МІНІСТЕРСТВО ОСВІТИ І НАУКИ УКРАЇНИ ДОНЕЦЬКИЙ НАЦІОНАЛЬНИЙ УНІВЕРСИТЕТ ІМЕНІ ВАСИЛЯ СТУСА

САПОЖНІК АЛІНА ОЛЕКСАНДРІВНА

Допускається до захисту:
в.о завідувача кафедри
політології та державного
управління
д.політ.н., професор
_____Чальцева О.М.
«____» _____2025 р.

ВПЛИВ ІНФОРМАЦІЙНОЇ ВІЙНИ НА НАЦІОНАЛЬНУ БЕЗПЕКУ В УКРАЇНІ

Спеціальність 052 Політологія
Бакалаврська робота

Науковий керівник:
Дубель М. В., старший викладач кафедри
політології та державного управління
д-р. філос. з м.е.в.

Оцінка: ____/ ____/ _____
(бали/за шкалою ЄКТS/за національною шкалою)
Голова ЕК:
_____
(підпис)

Вінниця – 2025

АНОТАЦІЯ

Сапожнік А.О. Вплив інформаційної війни на національну безпеку в Україні.

Кваліфікаційна робота на здобуття ступеня освіти «Бакалавр» за спеціальністю 052 «Політологія». Донецький національний університет імені Василя Стуса, Вінниця, 2025.

У кваліфікаційній (бакалаврській) роботі досліджено вплив інформаційної війни на національну безпеку України. Проаналізовано теоретико-методологічні основи поняття інформаційної війни, її основні інструменти та методи, а також історичні та сучасні приклади інформаційних операцій, зокрема в контексті російсько-українського повномасштабного вторгнення. Особливу увагу приділено ролі дезінформації, пропаганди, кібератак і психологічного впливу на громадську думку як засобів дестабілізації внутрішньої ситуації в державі. Визначено основні загрози, що виникають унаслідок інформаційних атак, та надано рекомендації щодо підвищення рівня інформаційної безпеки.

Ключові слова: інформаційна війна, національна безпека, дезінформація, пропаганда, кіберзагрози, Україна.

ABSTRACT

Sapozhnik A.O. The impact of information warfare on national security in Ukraine.

Qualification work for the degree of "Bachelor" in the specialty 0312 Political sciences and civics. Vasyl' Stus Donetsk National University, Vinnytsia, 2025.

The qualification (bachelor`s) work investigates the impact of information warfare on Ukraine’s national security. The theoretical and methodological foundations of the concept of information warfare, its key tools and methods, as well as historical and contemporary examples of information operations—particularly in the context of the full-

scale Russian-Ukrainian invasion—are analyzed. Special attention is given to the role of disinformation, propaganda, cyberattacks, and psychological influence on public opinion as means of destabilizing the internal situation in the state. The main threats resulting from information attacks are identified, and recommendations for enhancing information security are provided.

Keywords: information warfare, national security, disinformation, propaganda, cyber threats, Ukraine.

ЗМІСТ

ВСТУП

Актуальність теми дослідження. У сучасному глобалізованому світі інформація перетворилася на один із найпотужніших ресурсів, що здатен істотно впливати на політичні процеси, суспільну свідомість та рівень стабільності в державах. В умовах стрімкого розвитку інформаційно-комунікаційних технологій вона стала не лише засобом передачі знань чи засобом комунікації, а й потужною зброєю, яка у багатьох випадках виявляється не менш ефективною, ніж традиційні військові інструменти. Особливої актуальності проблема інформаційної війни набула в контексті сучасних гібридних конфліктів, де її роль дедалі частіше прирівнюється до класичних форм збройного протистояння.

Це твердження особливо справедливе для України, яка з 2014 року перебуває в умовах постійного інформаційного тиску з боку Російської Федерації. В інформаційному просторі ведеться систематична та багаторівнева агресія, що має на меті не лише викривлення об'єктивної реальності, а й формування альтернативного інформаційного порядку денного, здатного впливати на свідомість мільйонів громадян. Інформаційна війна у цьому контексті виступає як ключовий елемент гібридної стратегії, що охоплює широке коло заходів — від пропагандистських кампаній і поширення дезінформації до психологічних операцій та кібератак. Її головною метою є дестабілізація внутрішньополітичної ситуації, розкол суспільства, зниження рівня довіри до державних інституцій, а також підрив стратегічної стійкості держави загалом.

Актуальність дослідження зумовлюється тим, що інформаційна безпека стала невід'ємною складовою національної безпеки, а розуміння специфіки та наслідків інформаційного впливу — необхідною умовою для формування ефективної державної політики у сфері безпеки. Вивчення механізмів інформаційної війни, її інструментів і методів дозволяє не лише окреслити масштаби загрози, але й виявити найбільш уразливі ділянки інформаційного простору, які потребують посиленого

захисту. Крім того, воно відкриває можливості для розробки практичних заходів щодо запобігання дезінформаційним кампаніям та підвищення рівня медіаграмотності населення, що є надзвичайно важливим в умовах тривалої гібридної агресії.

Стан теоретичної розробки теми. Проблематика інформаційної війни, її сутності, механізмів та впливу на суспільство й державу викликає підвищену увагу як у зарубіжній, так і у вітчизняній науковій думці, особливо з огляду на виклики, з якими зіштовхується Україна з 2014 року. У центрі наукового дискурсу опинилися такі поняття, як інформаційна безпека, інформаційна агресія, гібридна війна, медіаманіпуляції та інформаційна зброя. Зокрема, після початку збройної агресії Російської Федерації проти України, вітчизняні дослідники зосередили увагу на вивченні специфіки ведення інформаційних атак, їх впливу на суспільну свідомість, державні інститути та міжнародний імідж держави.

Вагомий внесок у наукове осмислення цієї тематики зробили такі українські науковці, як Т.М. Варга, який досліджує інформаційну війну як ключовий елемент гібридної агресії Росії проти України, зосереджуючись на стратегіях дезінформації [1]. Д. О. Мельник у своїх працях аналізує інформаційну безпеку як складову національної безпеки та окреслює аналітичні підходи до її оцінки [13]. На особливості інформаційного середовища в умовах війни звертає увагу також Г. Маляр, яка розглядає ризики, пов’язані з функціонуванням українських медіа під тиском зовнішніх загроз [12].

Актуальність та складність проблеми також підкреслюється у працях М.О. Зінченко, О.Б. Плугова, О.В. Драглюк, які аналізують маніпулятивні медіатехнології та поширення дезінформації в соціальних мережах [6]. Значущим є внесок О. Виговської та Н. Бєлоусової, які окреслють сучасні виклики інформаційного характеру, що постають перед національною безпекою України [3]. В.В. Карлова комплексно аналізує механізми ведення інформаційної війни, її інструменти та наслідки для суспільної стабільності [9].

Таким чином, вітчизняна наукова думка активно розробляє проблему інформаційної війни, вказуючи на її багатовимірність, системність та глибокі наслідки для функціонування демократичного суспільства і державної безпеки. Однак попри значний обсяг досліджень, залишаються недостатньо вивченими питання довгострокового впливу інформаційних атак на громадську довіру до інституцій, формування стійкості до дезінформації, а також адаптація західного досвіду в умовах української реальності, що потребує подальшого аналізу в межах даної наукової роботи.

Зв'язок роботи з науковими програмами, планами, темами: Кваліфікаційна робота виконана в рамках тематичного плану НДР Донецького національного університету імені Василя Стуса – ініціативного фундаментального дослідження кафедри політології та державного управління: «Публічна політика і державне управління в умовах війни та повоєнного відновлення України» (реєстраційний номер 0123U101423).

Метою кваліфікаційної (бакалаврської) роботи є комплексне дослідження впливу інформаційної війни на національну безпеку України та виявлення шляхів їх подолання.

Завданнями дослідження є:

1. Розкрити поняття інформаційної війни, визначити її ключові характеристики та відмінності від суміжних явищ.
2. Проаналізувати основні інструменти та методи ведення інформаційної війни.
3. Визначити роль інформаційного елементу в системі національної безпеки України.
4. Здійснити класифікацію основних інформаційних атак на Україну з 2014 року до сьогодні.
5. Дослідити механізми та цифрові платформи поширення дезінформації.

6. Оцінити вплив російської пропаганди на суспільну думку в Україні та за її межами.

7. Проаналізувати державну політику України у сфері інформаційної безпеки.

8. Визначити роль громадянського суспільства, незалежних ЗМІ та фактчекінгових ініціатив у протидії дезінформації.

9. Дослідити міжнародний досвід боротьби з інформаційними війнами та можливості його застосування в Україні.

Об'єкт дослідження: національна безпека України в умовах інформаційної війни.

Предмет дослідження: інформаційні впливи та їхній вплив на політичну, соціальну та безпекову ситуацію в Україні.

Гіпотеза. Розвиток інформаційних технологій несе потенційну загрозу національній безпеці України, у зв'язку з тим, що зброя інформаційної війни розвивається швидше, ніж захисні механізми.

Методи дослідження:

• Системний метод застосовано для комплексного аналізу інформаційної війни як багатокомпонентного явища, що впливає на різні сфери національної безпеки. Цей методи дав змогу розглядати інформаційну безпеку не ізольовано, а як частину загальної безпекової системи держави, з урахуванням взаємозв'язку політичних, соціальних, військових та інформаційних чинників.

• Структурно-функціональний метод дозволив виявити ключові елементи інформаційної війни (засоби дезінформації, пропагандистські кампанії, кібератаки тощо) та проаналізувати їх функціональну роль у підриві стабільності державних інституцій. Завдяки цьому методу було визначено, як саме інформаційні загрози впливають на функціонування системи національної безпеки.

• Компаративний метод використано для порівняння впливу інформаційної війни на Україну з аналогічними випадками в інших державах (наприклад, країни

Балтії). Це дозволило виявити спільні риси та особливості інформаційних атак, а також специфіку реагування українських державних структур на ці виклики.

• Історичний метод допоміг проаналізувати еволюцію інформаційної війни проти України, зокрема її інтенсивність та форми у періоди активних військових дій (2014 рік, повномасштабне вторгнення у 2022 році). Завдяки цьому методу вдалося простежити динаміку змін інформаційного середовища.

• Контент-аналіз застосовано для дослідження змісту інформаційних повідомлень, поширюваних через медіа та соціальні мережі. Це дозволило виявити основні теми та наративи, які використовувалися у межах інформаційних операцій проти України, а також оцінити рівень їх впливу на громадську думку.

Теоретичне та практичне значення одержаних результатів полягає у поглибленні розуміння природи інформаційної війни як загрози національній безпеці, а також у визначенні ефективних механізмів її виявлення, аналізу та протидії. Результати дослідження можуть бути використані для формування державної інформаційної політики, вдосконалення системи інформаційної безпеки, підготовки фахівців у сфері національної безпеки та комунікацій.

Структура роботи. Бакалаврська робота складається з вступу, трьох розділів, висновків, списку використаних джерел з 42 найменувань. Обсяг роботи складає 65 сторінки, при цьому основний зміст роботи займає 60 сторінок.

РОЗДІЛ 1.
ТЕОРЕТИКО-МЕТОДОЛОГІЧНІ ЗАСАДИ ДОСЛІДЖЕННЯ РОЛІ ІНФОРМАЦІЙНОЇ ВІЙНИ ДЛЯ НАЦІОНАЛЬНОЇ БЕЗПЕКИ

1.1 Поняття інформаційної війни: визначення та основні характеристики

Розвиток людської цивілізації супроводжується безперервною та необхідною потребою у забезпеченні власної безпеки через протистояння різноманітним зовнішнім загрозам, знищення або підкорення потенційних супротивників, а також здобуття у важливих ресурсів. Війна, як одна з фундаментальних складових цього процесу, упродовж століть пройшла складний шлях еволюції, постійно адаптуючись до змінюваних умов та технологічних досягнень. Військові операції, невід'ємна частина цього процесу, продовжують активно розвиватися і нерідко набувають найбільш неочікуваних та інколи революційних форм, які часом здаються не передбачуваними для попередніх етапів людської історії. Ще кілька століть тому важко було уявити, що ключовим ресурсом у війнах майбутнього стане не лише зброя чи територія, а інформація. У сучасному світі особливого значення набуває інформаційна безпека, адже саме через інформаційні канали здійснюється вплив на громадську думку, ухвалення політичних рішень та дестабілізацію держав. Інформаційні технології стали не лише інструментом комунікації, а й засобом ведення конфліктів, здатним змінювати хід подій без застосування фізичної сили.

Паралельно, особливу роль у військових конфліктах відіграють сучасні інформаційно-психологічні операції, здатні істотно змінити ситуацію на полі бою, не застосовуючи при цьому безпосереднього фізичного насильства. Можливості таких операцій є вражаючими: вони можуть не лише сприяти підвищенню морального стану власних сил, але й змусити противника відчувати паніку та невпевненість, що у результаті здатне вплинути на перебіг війни. Крім того, інформаційно-психологічні методи здатні посіяти розбрат та недовіру серед

ворожих сил, змусити їх населення сумніватися у вірності один одному, водночас об’єднуючи власний народ навколо спільної мети та загальної ідеї. З цієї точки зору, перемога над супротивником – це лише частина стратегії, а здатність змусити його тікати чи капітулювати є справжнім мистецтвом, що потребує глибокого розуміння людської психології та ефективного використання інформаційних ресурсів.

Історія демонструє, що інформація завжди була потужним інструментом впливу: ще в давнину чутки чи скандали могли спричинити серйозні конфлікти. Попри примітивність перших інформаційних операцій, вони заклали основу для розвитку складніших стратегій, що згодом стали важливою складовою військових і політичних протистоянь [35].

Інформаційна війна — це складний і динамічний процес, що включає приховані маніпуляції, внаслідок яких супротивник не усвідомлює, що є об’єктом впливу. За класифікацією НАТО, це операція зі здобуття інформаційної переваги шляхом контролю власного інформаційного простору, захисту ресурсів та впливу на інформаційні системи ворога [36].

У межах дослідження впливу інформаційної війни на національну безпеку України було застосовано низку методів, які забезпечили всебічний та комплексний підхід до аналізу цього складного і багатовимірного явища. Зокрема, системний метод дозволив розглядати інформаційну війну не як ізольоване явище, а як елемент ширшої системи національної безпеки, що функціонує у взаємозв’язку з політичними, соціальними, економічними та військовими складовими. Такий метод сприяв глибшому розумінню механізмів взаємодії між окремими елементами безпекової системи держави в умовах інформаційного протистояння. Структурно-функціональний метод дав змогу детальніше проаналізувати внутрішню будову явища інформаційної війни, виокремити її основні компоненти — такі як засоби дезінформації, пропагандистські кампанії, кібератаки, інформаційні вкиди тощо — та дослідити специфіку їхнього функціонування в умовах гібридної агресії. Застосування цього методу також дозволило встановити, яким чином ці елементи

взаємодіють між собою і який вплив вони мають на ефективність функціонування інституцій національної безпеки.

Крім того, було використано компаративний метод, що став у пригоді при зіставленні українського досвіду протидії інформаційним загрозам із аналогічними кейсами в інших країнах, зокрема у державах Балтії. Такий порівняльний аналіз дав змогу виявити як загальні закономірності в інформаційній агресії, так і унікальні аспекти українського контексту, які зумовлені історичними, політичними та геополітичними факторами. Історичний метод, у свою чергу, забезпечив можливість проаналізувати динаміку розвитку інформаційної війни проти України з урахуванням ключових віх — початку агресії у 2014 році, ескалації у 2022 році та подальших трансформацій у формах і засобах інформаційного впливу. Це дало змогу простежити еволюцію стратегій ворога у медійному просторі та оцінити зміну рівня інформаційної загрози з плином часу.

Особливе значення в межах роботи мав контент-аналіз, за допомогою якого було здійснено вивчення змісту медійних повідомлень, поширюваних як через традиційні засоби масової інформації, так і через соціальні мережі, месенджери та інші цифрові платформи. Цей метод дав змогу виявити ключові теми, пропагандистські наративи та стратегії впливу, що використовуються у рамках інформаційної війни проти України, а також проаналізувати рівень їхнього проникнення у масову свідомість і потенційні наслідки для інформаційної безпеки держави.

У вітчизняному науковому просторі проблема інформаційної війни постає як надзвичайно актуальна у зв’язку з триваючим гібридним протистоянням, що охоплює всі сфери суспільного життя, зокрема інформаційний простір. В умовах зростаючої інтенсивності інформаційних загроз українські дослідники зосереджують увагу на вивченні ролі інформаційної безпеки як складової національної безпеки, аналізуючи як концептуальні, так і прикладні аспекти цього явища.

Зокрема, Ю. Горбань у своєму аналітичному дослідженні наголошує, що інформаційна безпека України є не лише елементом державної політики, а й ключовою умовою стабільного функціонування політичної системи в цілому. Він розглядає інформаційний простір як критично вразливу зону, що потребує постійного моніторингу, аналітичного оцінювання та стратегічного планування. На думку дослідника, головними викликами для національної безпеки є несанкціонований вплив на масову свідомість, підміна фактів, нав'язування ворожих наративів, а також внутрішня політична поляризація, яка стає зручним ґрунтом для зовнішніх маніпуляцій [4].

М. Зінченко, у свою чергу, акцентує увагу на гібридній природі російської агресії, в центрі якої — інтенсивна інформаційна експансія. Він підкреслює, що інформаційна війна проти України здійснюється через багатоканальні комунікаційні мережі із застосуванням як традиційних ЗМІ, так і цифрових платформ, що дозволяє Росії одночасно впливати на внутрішню аудиторію, міжнародну спільноту та українське суспільство. Дослідник розглядає інформаційні атаки як спробу формування альтернативної реальності, у якій викривлюються обставини збройного конфлікту, делегітимізуються українські інституції та нав'язуються проросійські погляди [6].

Хоча інформаційні війни не є абсолютно новим явищем, вони зазнали значних змін у зв'язку з технологічним розвитком і зростанням швидкості поширення інформації. Інновації, що виникли внаслідок розвитку сучасних інформаційних технологій, дозволяють значно швидше і ефективніше впливати на хід подій, обробляти більші обсяги даних і здійснювати маніпуляції на значно більших територіях. Використання інформаційної протидії дозволяє змінювати тактичне, оперативне та стратегічне становище на полі бою, здійснювати маскування переміщення та підготовки військових операцій, тим самим обманюючи противника. Важливим аспектом є здатність змусити ворога повірити

в те, що є вигідним для атакуючої сторони, таким чином перешкоджаючи його реальним діям.

Видатний китайський філософ Сунь-Цзи створив цілу низку трактатів, присвячених майстерності обману супротивника, серед яких найвідоміший – «Мистецтво війни». Цей твір, що став класикою військової стратегії, здобув всесвітнє визнання та до сьогодні є обов'язковим для вивчення в академічних військових закладах по всьому світу, а також серед китайських партійних функціонерів. Його ідеї, що відзначаються вишуканою точністю, логічною чіткістю та доступністю, дозволили цьому філософу передавати свої знання наступним поколінням на протязі століть. Принципи, викладені Сунь-Цзи, стали основою для розвитку стратегії не лише в Китаї, але й в інших культурах, зокрема в античному світі [20].

У ході Другої світової війни, спостерігаючи за неймовірним успіхом та вражаючим потенціалом інформаційних кампаній, які вели сили О Axis (які протягом тривалого часу домінували в інформаційному просторі Європи, сіючи паніку, страх і зневіру серед населення, а також переконуючи у повній безглуздості спротиву їх військовим силам), Великобританія вирішила створити спеціалізовану та надзвичайно важливу організацію, здатну протистояти такій потужній інформаційній атакі. Ця організація, відома як «London Controlling Section» (LCS), була заснована в 1941 році. На чолі з Олівером Стенлі, а пізніше під керівництвом Джона Бевана, який замінив Стенлі через його недостатньо високі управлінські здібності, LCS стала однією з ключових структур у рамках Британії, яка відповідала за організацію та координацію різноманітних інформаційно-психологічних операцій. Першопочатково організація діяла в умовах надзвичайної секретності, її існування залишалося таємницею аж до 1969 року, коли сер Рональд Вінгейт, один із найбільших дослідників історії Великої Британії, підтвердив її функціонування після закінчення Другої світової війни.

Основною метою створення LCS було забезпечення ефективного проведення інформаційно-психологічних операцій, спрямованих на введення ворога в оману та підготовку підґрунтя для здійснення військових операцій. Це включало не лише підготовку військових дій, але й нейтралізацію можливих стратегічних ініціатив супротивника. Успіх цих операцій міг мати вирішальний вплив на хід війни, адже від них часто залежали долі мільйонів людей, і правильне застосування інформаційних стратегій ставало питанням життя та смерті. Розуміння важливості інформаційної війни дозволило союзникам виділяти значні фінансові ресурси для забезпечення діяльності LCS, що в свою чергу відкривало нові можливості для досягнення стратегічних переваг [35].

Таким чином, завданням LCS було відвести увагу від реального місця висадки союзних військ, приховати точну кількість та розташування бойових з'єднань, щоб забезпечити максимальну ефективність основної операції та обдурити ворога, змусивши його зосередити всі свої сили на менш важливому напрямку. Цей підхід став одним із основних елементів інформаційної стратегії, що дозволила союзникам здобути вирішальну перевагу в плануванні та виконанні висадки в Нормандії [35].

Після закінчення Другої світової війни, хоча LCS була розпущена, її досвід і методи не зникли безслідно. Багато з технологій та стратегій, розроблених і застосованих цією організацією, були успішно використані в рамках спецоперацій під час Холодної війни, що підтверджує їх безсмертну цінність у контексті ведення інформаційно-психологічної боротьби на глобальному рівні.

Отже, аналіз поняття та витоків інформаційної війни засвідчує, що вона є результатом еволюції військових стратегій, в яких дедалі вагомішу роль починає відігравати не стільки фізичне протистояння, скільки боротьба за домінування в інформаційному просторі. Історичні приклади – від Сунь-Цзи до Другої світової війни – підтверджують, що інформаційна компонента завжди була важливим елементом конфліктів, хоча її роль значно зросла з розвитком технологій. У сучасному контексті інформаційна війна виступає як системна діяльність, що

охоплює вплив на масову свідомість, деморалізацію ворога, створення викривленої реальності. Вона базується на маніпуляції, дезінформації, психологічному тиску, а її стратегічна мета полягає у здобутті контролю над інформаційним полем супротивника.

1.2 Інструменти та методи інформаційної війни

Інформаційна війна – це новий, динамічний та складний компонент сучасних конфліктів, що ґрунтується на технологічних революціях у сфері зв'язку та обробки даних. За визначенням RAND, інформаційна війна є «швидко еволюційним і поки що нечітко визначеним полем», яке активно цікавить стратегів та військових планувальників. Ідеться про те, що як держави, так і недержавні актори прагнуть використати глобальну інформаційну інфраструктуру (інтернет, мобільний зв'язок, соціальні мережі тощо) у військових цілях. Головна суть інформаційної війни полягає не стільки у прямому знищенні супротивника зброєю, скільки у впливі на свідомість і рішення людей – насамперед солдатів, політиків і цивільного населення. Засоби та технології цієї боротьби – пропаганда, дезінформація, кібератаки, психологічні операції – тісно взаємопов'язані.

За концепцією НАТО, інформаційна війна розглядається як складова гібридної війни, де «використовуються військові та невійськові, а також приховані й відкриті засоби (включно з дезінформацією, кібератаками тощо) для розмивання меж між війною та миром і підриву суспільної стабільності». Іншими словами, вона одночасно використовує політичні, економічні, технологічні та інформаційні важелі. Розробники стратегії оборони США у 1990-х роках акцентували увагу на тому, що інформаційна війна виникла під впливом «інформаційної революції» та стрімкого зростання значення кіберпростору. Аналіз цих змін показав, що нові можливості можуть як надати військовим переваги, так і створити значні вразливості, зокрема якщо противник активно «спотворює» інформаційну

реальність за допомогою сучасних технологій (штучного інтелекту, глибинних підробок тощо) [35].

Головною метою інформаційної війни є маніпулювання свідомістю та поведінкою суспільства. Агресор прагне підірвати довіру до влади, посіяти паніку та знизити міжнародну підтримку. За даними СБУ та ГУР, Росія з 2014 року системно реалізує такі напрями: дискредитація керівництва України, зрив мобілізації й допомоги партнерів, дестабілізація ситуації в країні. Аналітики наголошують, що ця діяльність є злочином проти миру й має каратися [7].

Згідно з конструктивістським підходом у політичній науці, інформаційна війна розглядається не лише як інструмент прямого впливу на суб'єкти міжнародних відносин, але й як засіб формування соціальної реальності шляхом маніпулювання символами, смислами та ідентичностями. У межах цієї методології ключову увагу приділено не матеріальним аспектам сили, а здатності акторів впливати на уявлення, переконання та світогляд цільових груп через комунікативні практики.

Інформаційна війна в такому розумінні постає як процес активного конструювання політичних і соціальних наративів, за допомогою яких формуються установки громадськості, делегітимізуються інститути влади, підривається довіра до держави та створюються сприятливі умови для досягнення стратегічних цілей агресора. Таким чином, конструктивістський підхід дозволяє розглядати інформаційну війну не лише як технологічний чи комунікаційний феномен, а як політичну практику боротьби за контроль над смислами у глобальному та національному інформаційному просторі.

Крім того, Служба безпеки України (СБУ) зазначає, що за підтримки партнерів Україні доводиться одночасно протистояти двом основним фронтам інформаційної агресії: внутрішньому та зовнішньому. Внутрішній полягає у підриві єдності та морального духу українського суспільства, а зовнішній – у дискредитації України у світі. Така подвійна стратегія спрямована на те, щоб з одного боку

деморалізувати громадян і відірвати їх від реальних дій, а з іншого – викликати сумніви в підтримці України серед іноземних партнерів. У розумінні фахівців НАТО, інформаційні загрози розривають «тканину, що тримає суспільства разом», стимулюючи «сумніви, страхи та упередження» і «розділяючи людей, щоб послабити суспільну згуртованість». Використання цих методів потенційно може спричинити реальний хаос і насильство, оскільки посіяні міфи та зневіра мають наслідки, співмірні з військовими втратами [10].

Класичним інструментом інформаційної війни є пропаганда — цілеспрямоване поширення ідеологічних наративів через контрольовані медіа. У XXI столітті її доповнює дезінформація — свідоме викривлення фактів, створення фейків і маніпулятивний добір новин. Під час війни проти України Росія активно використовує наративи про «денацифікацію», «захист російськомовних» і «штучність української державності». Ці міфи поширюються як усередині РФ, так і за кордоном через підконтрольні ЗМІ, псевдоекспертів і соціальні мережі [39].

У контексті посилення інформаційного протистояння в умовах гібридної війни, наукове осмислення феномену інформаційної агресії проти України набуває особливої важливості. Вітчизняні дослідники акцентують увагу на стратегічному значенні інформаційного чинника для забезпечення національної безпеки. Зокрема, у працях Т. Варга інформаційна безпека розглядається як системоутворювальний елемент безпекової політики держави, що перебуває у постійній взаємодії з політичною, військовою та економічною складовими. Автор наголошує на тому, що ефективна інформаційна політика має ґрунтуватися на аналітичному прогнозуванні загроз, своєчасному реагуванні на інформаційні атаки та розвитку державної антикризової комунікації [1].

У свою чергу, Г. Маляр зосереджується на технологіях маніпулятивного впливу в українському медіапросторі. Авторка досліджує мовно-дискурсивні та психологічні методи, що використовуються у процесі поширення дезінформації, зокрема через заголовки, емоційно забарвлену лексику, візуальні символи та

підміну фактів. Маляр підкреслює, що маніпулятивний контент має здатність створювати спотворену соціальну реальність, що особливо небезпечно в умовах війни. Особливу роль вона відводить формуванню критичного мислення, медіаграмотності та культури фактчекінгу як основі захисту суспільства від інформаційних загроз [12].

У сучасній інформаційній війні соціальні медіа є ключовим інструментом, що дозволяє швидко та цілеспрямовано поширювати контент. Під час війни 2022 року вони перетворилися на поле бою, де за допомогою хештегів, мемів та відеороликів, часто поширюваних скоординованими мережами ботів, впливали на настрої населення. Нерідко використовувалася тактика розповсюдження суперечливих новин серед прихильників та противників конфлікту одночасно, щоб викликати розгубленість та підірвати довіру до джерел інформації.

Окремої уваги заслуговують новітні технологічні засоби. Глибинні підробки (deepfake) — це синтетичні аудіо- і відео-матеріали, створені штучним інтелектом, що імітують зовнішність та голос конкретних осіб. У березні 2022 року з'явилося імітоване відео Президента України Володимира Зеленського із закликом до солдатів здатися. Попри низьку якість, відео викликало резонанс і було розкритиковане як «погано змонтований deepfake». ЗМІ пов'язали його з гібридними атаками РФ. Reuters зазначило, що цей «недосконалий фейк» міг бути провісником складніших обманів. Deepfake-відео можуть одночасно поширюватися у соцмережах і навіть з'являтися на телебаченні в окупованих регіонах. Експерти попереджають: з розвитком технологій такі підробки стають дедалі реалістичнішими, що робить їх небезпечним інструментом інформаційної війни. [26].

До методів інформаційної війни належать і кібероперації — навмисні атаки на інформаційні та критичні інфраструктури супротивника для створення хаосу та інформаційних перешкод. НАТО прямо відносить «кібератаки» до гібридних засобів дестабілізації. Приклад — атака у грудні 2015 року на українську

енергомережу, яка залишила без світла понад 200 тисяч споживачів. Розслідування міжнародних фахівців (CISA) вказує на російських агентів. Мета — не лише вивести з ладу мережу, а й посіяти почуття вразливості — типовий елемент комбінованого впливу. Такі операції можуть включати шкідливе ПЗ, DDoS-атаки, перехоплення або блокування сигналів, створюючи інформаційну «туманність» і занурюючи суспільство в стан паніки [35].

Крім усього, інформаційні операції поєднують технічні й психологічні заходи. Наприклад, разом з кібератакою на мережу може йти штучний «флуд» – одночасне розсилання десятків тисяч фейкових повідомлень від імені зламаних акаунтів, щоб завалити стрічки новин у соцмережах. Такі скоординовані атаки змушують звичайних користувачів втрачати довіру до онлайн-платформ – у якийсь момент стає важко відрізнити правду від пропаганди. Як наголошує Альянс, інформаційні загрози навмисно викликають «конфуз та плутанину, щоб люди не могли відрізнити факти від вигадок». Водночас це може призвести до двох типових реакцій серед населення: або люди починають поширювати і вірувати у малодоказові сенсації, або ж, розчарувавшись, повністю дистанціюються від інформаційного простору – що також корисно агресору, адже знижує стійкість суспільства.

У реальних подіях інформаційна війна часто поєднується із класичними військовими діями. У випадку повномасштабного вторгнення РФ в Україну було задокументовано численні тактики. Зокрема, про використання deepfake-технологій уже згадувалося – відео з «присягаючим» Зеленським розповсюджували передусім на проросійських платформах, одночасно з’являючись і на зламаному українському сайті. В Україну також надходили лавини повідомлень про уявні «тенденції зречення влади» чи «диверсії в тилу», що створювали атмосферу недовіри навіть серед військових підрозділів. Навіть світові соцмережі були втягнуті: наприклад, у березні 2022-го фейкове повідомлення про капітуляцію Зеленського мало понад 5 мільйонів переглядів у Telegram, доки модератори не позначили його як брехню.

Такі випадки ілюструють, наскільки швидко хибна інформація може розлітатися в епоху цифрових комунікацій.

Отже, сучасна інформаційна війна є комплексним явищем, у якому синтезовано кіберзасоби, класичну пропаганду, соціальні мережі, маніпуляції на історичному ґрунті, а також новітні інструменти, як-от deepfake та таргетована дезінформація. Ворог, використовуючи алгоритми соціальних медіа та штучний інтелект, здатен не лише атакувати інфраструктуру, але й трансформувати уявлення людей про реальність. Основна небезпека полягає в тому, що така війна часто не фіксується як акт агресії, але при цьому створює передумови для політичної та соціальної дестабілізації. Український досвід боротьби з російською інформаційною агресією засвідчує важливість стійкості держави в умовах гібридних загроз, де ключову роль відіграє не тільки військова готовність, а й інформаційна просвіта, технологічна спроможність та міжнародна підтримка.

1.3 Інформаційний елемент системи національної безпеки

У сучасних умовах стрімкої еволюції інформаційних технологій питання забезпечення інформаційної безпеки набуває визначального значення для стійкості держави, її політичної, економічної та соціальної стабільності. Інформаційна сфера перетворилася на арену глобального протистояння, де національні інтереси захищаються не лише військовою силою чи дипломатією, а й через активні заходи в інформаційному просторі. Особливо актуальним це питання є для України, яка з 2014 року стала об'єктом масштабної гібридної агресії з боку Російської Федерації, у межах якої інформаційні операції виступають одним із ключових інструментів досягнення стратегічних цілей агресора.

У контексті повномасштабної агресії Російської Федерації проти України, що розпочалася у 2022 році, поняття інформаційної безпеки набуло нового змісту, відображеного в Стратегії інформаційної безпеки України, затвердженій Указом Президента №685/2021 від 28 грудня 2021 року. Згідно з цим документом,

інформаційна безпека розглядається як комплексна система заходів, спрямованих на захист національного інформаційного простору від внутрішніх і зовнішніх загроз, включаючи дезінформацію, пропаганду, інформаційно-психологічні операції та інші форми інформаційної агресії, що підривають державний суверенітет, територіальну цілісність, демократичний конституційний лад і права громадян. Стратегія передбачає створення ефективної системи взаємодії між органами державної влади, місцевого самоврядування та суспільством, а також розвиток міжнародної співпраці у сфері інформаційної безпеки на засадах партнерства та взаємної підтримки [8].

У контексті повномасштабної збройної агресії Російської Федерації проти України з 2022 року особливої актуальності набуло питання адаптації державної інформаційної політики до нових викликів гібридної війни. Відповіддю на ці виклики стало ухвалення низки стратегічних документів, що визначають сучасний підхід до забезпечення інформаційної безпеки держави.

Зокрема, 28 грудня 2021 року було затверджено Стратегію інформаційної безпеки України (Указ Президента України №685/2021), у якій сформульовано основні принципи, завдання та напрями державної політики у сфері інформаційної безпеки [16]. Стратегія передбачає комплекс заходів із протидії дезінформації, інформаційним впливам з боку держави-агресора, а також із посилення стійкості інформаційного середовища України. Для практичного втілення її положень Кабінет Міністрів України 30 березня 2023 року затвердив План заходів з реалізації Стратегії на період до 2025 року (розпорядження №272-р) [8].

Ключовими напрямами державної інформаційної політики в умовах війни стали:

– розбудова системи протидії інформаційним операціям і деструктивному впливу ворожих наративів;

– підвищення рівня медіаграмотності населення як елементу інформаційної стійкості;

– розвиток стратегічних комунікацій між державою та громадянами;

– захист критичної інформаційної інфраструктури та інформаційних ресурсів. [10].

Таким чином, сучасна стратегія інформаційної безпеки України демонструє перехід від пасивної оборони до активної інформаційної політики, спрямованої на зміцнення національної єдності, протидію інформаційній агресії та інтеграцію у загальноєвропейську систему колективної безпеки.

У науковій літературі підкреслюється, що інформаційна безпека має багатовимірний характер і охоплює технічний, політичний, соціальний та психологічний аспекти. Наприклад, Гаврилюк А. І. наголошує на тому, що в умовах гібридної війни класичні форми збройного протистояння поступово доповнюються інформаційними кампаніями, спрямованими на підрив національної ідентичності, деморалізацію населення та створення альтернативної картини реальності в суспільній свідомості [30].

Аналіз практики інформаційної війни проти України засвідчує використання широкого спектра інструментів впливу: від класичної пропаганди через мас-медіа до кібератак на критичну інфраструктуру. Зокрема, ще у 2014 році російські телеканали розгорнули масовану кампанію дискредитації подій Революції Гідності, нав’язуючи наративи про «державний переворот», «неонацизм» та «зовнішнє управління». Через такі повідомлення формувалася викривлена інтерпретація реальності, що була спрямована як на внутрішню російську аудиторію, так і на міжнародне співтовариство.

Особливу роль в інформаційній війні відіграють соціальні мережі, які стали простором для миттєвого поширення як достовірної, так і маніпулятивної інформації. Бот-мережі, фабрики тролів, фейкові акаунти активно використовуються для створення ілюзії суспільного консенсусу щодо певних тез або для нагнітання панічних настроїв. Відомим прикладом є діяльність так званої «фабрики тролів» у Санкт-Петербурзі, яка ще у 2016–2018 роках проводила

операції не лише в контексті США та Європи, а й активно працювала на українському напрямку, зокрема під час виборчих кампаній.

Згідно з аналітичною доповіддю Центру стратегічних комунікацій та інформаційної безпеки 2022 року, лише 32% українських громадян можуть самостійно розпізнавати дезінформацію. Це свідчить про нагальну потребу в розвитку цифрової грамотності та критичного мислення серед населення. Інформаційна безпека не може забезпечуватися виключно через діяльність спеціальних органів — вона повинна стати складовою культури громадянського суспільства [25].

У цьому контексті особливої ваги набувають медіа-освітні ініціативи, спрямовані на навчання громадян навичкам перевірки інформації, розпізнавання маніпуляцій та усвідомленого споживання медіаконтенту. Важливою є діяльність проєктів, таких як «StopFake», що здійснюють перевірку фактів і розвінчують фейки, а також освітні програми з медіаграмотності, впроваджені Міністерством освіти і науки України.

Міжнародний досвід також демонструє важливість комплексного підходу до інформаційної безпеки. Зокрема, країни Балтії (Латвія, Литва, Естонія) після набуття незалежності активно працювали над побудовою національної системи стратегічних комунікацій, інтеграцією інформаційного компоненту в оборонну політику, розвитком партнерства між державними структурами, громадським сектором і медіа. Створення спеціалізованих центрів, як-от Латвійський центр стратегічних комунікацій, стало ефективною відповіддю на інформаційні загрози.

Важливо зазначити і роль міжнародних організацій. Програми Європейського Союзу, такі як EUvsDisinfo, активно моніторять випадки дезінформації, спрямованої проти України, та надають аналітичну підтримку у протидії таким кампаніям. НАТО, у свою чергу, надає технічну допомогу в зміцненні кіберзахисту, підтримує обмін досвідом і розвиток національних стратегічних комунікацій [30].

Отже, інформаційна безпека є надзвичайно складним, багатовимірним явищем, що охоплює технічні, соціальні, політичні та психологічні аспекти. В умовах сучасних гібридних загроз ефективне забезпечення інформаційної безпеки вимагає інтегрованого підходу: поєднання технологічних рішень, законодавчого регулювання, розвитку медіаграмотності, підтримки громадянського суспільства та міжнародного співробітництва. Від здатності держави протистояти інформаційним загрозам залежить не лише її внутрішня стабільність, а й сама перспектива збереження державного суверенітету та національної ідентичності.

Підсумовуючи теоретичні основи, розглянуті у першому розділі, можна зробити висновок, що інформаційна війна – це нова форма глобального протистояння, що об'єднує технічні, психологічні та ідеологічні виміри. Вона глибоко інтегрована в сучасну безпекову парадигму і має системний вплив на політичну, соціальну та військову сфери. Інформаційна агресія стала постійною загрозою в умовах цифрової епохи, особливо вразливими до якої є демократичні суспільства. Сучасні інструменти інформаційної війни дають змогу противнику діяти непомітно, підривати довіру до інституцій, послаблювати моральну стійкість та трансформувати ідентичність націй. У цьому контексті інформаційна безпека набуває ключового значення у системі національної безпеки, оскільки від її ефективності залежить не лише обороноздатність, а й стійкість самої державності. Український досвід є показовим у цьому плані: лише через комплексне осмислення природи інформаційної загрози, системну політику й освітній підхід можна вибудувати дієву модель протидії на рівні держави, суспільства та кожного громадянина.

РОЗДІЛ 2.
ДОСЛІДЖЕННЯ ВПЛИВУ ІНФОРМАЦІЙНОЇ ВІЙНИ НА НАЦІОНАЛЬНУ БЕЗПЕКУ УКРАЇНИ

2.1 Аналіз основних інформаційних атак на Україну з 2014 року

Із початком Революції Гідності у 2013–2014 роках Україна стала об’єктом системної інформаційної агресії з боку Російської Федерації. Цей тип агресії є ключовим елементом гібридної війни, що має на меті вплинути на суспільну свідомість, посіяти недовіру до влади, дискредитувати українські інституції та послабити внутрішню єдність держави. Інформаційні атаки, що здійснювалися впродовж останнього десятиліття, еволюціонували від примітивної пропаганди до високотехнологічних кампаній, які використовують алгоритми штучного інтелекту, бот-мережі, deepfake-технології та інші інструменти цифрової війни.

Першою масштабною інформаційною операцією стала кампанія із легітимізації анексії Криму у 2014 році. Російські ЗМІ поширювали наративи про «захист російськомовного населення», «переворот у Києві», «націоналістичну загрозу», що нібито виходила від нової української влади. Ці меседжі активно транслювалися як на внутрішній російській аудиторії, так і на міжнародній арені, з метою створення хибного образу громадянського конфлікту замість збройної агресії [27].

Варто зазначити, що однією з форм тривалого інформаційного впливу стало нав’язування Україні образу «failed state» — держави, яка нібито не здатна функціонувати самостійно без зовнішнього управління. Через дезінформаційні кампанії послідовно просуваються наративи про тотальну корупцію, неефективність органів влади, внутрішню політичну боротьбу, розпад економіки та зневіру населення. Такі повідомлення спрямовані на деморалізацію не лише українців, а й іноземної аудиторії, зокрема західних союзників, для послаблення міжнародної підтримки України на фоні затяжного конфлікту [9].

Ще одним важливим інструментом є використання інфлюенсерів, блогерів та псевдоекспертів, які виступають у ролі «нейтральних» чи «альтернативних» джерел інформації. Через такі канали Росія намагається маскувати свої меседжі під «об'єктивну думку» або «голос народу». Такі особи можуть мати українське походження, володіти відповідною мовною та культурною компетенцією, що підвищує довіру аудиторії. Особливо активно ці методи застосовуються у TikTok, YouTube та Telegram, де публікуються «розслідування», «документальні» відео та живі трансляції, покликані сіяти сумніви, недовіру до офіційної інформації та створювати альтернативну реальність [7].

Зростає також кількість так званих «сірого» контенту — напівправдивої інформації, яка змішує факти з домислами або недомовками. Цей метод є особливо небезпечним, оскільки ускладнює ідентифікацію фейків навіть для обізнаного користувача. Наприклад, інформаційні вкиди можуть базуватись на реальних подіях, але спотворювати їх контекст, акценти або причинно-наслідкові зв'язки. Завдяки цьому створюється ефект достовірності, який важко спростувати звичайними фактчекінговими методами, особливо в умовах інформаційного перевантаження [34].

Окремо слід наголосити на кібератаках як складовій інформаційної агресії. Відомими є випадки атак на інформаційну інфраструктуру державних органів України, зокрема на сайти уряду, ЦВК, обласних адміністрацій, що супроводжувались розміщенням дезінформаційних повідомлень. Наприклад, перед початком вторгнення у 2022 році на низці державних вебресурсів з'явилися повідомлення про «злиття персональних даних», «викриття урядових змов», що мали на меті дестабілізацію ситуації. Подібні акції також супроводжувалися DDOS-атаками та спробами зламу інформаційних систем [35].

Значну роль у забезпеченні інформаційної безпеки відіграє система протидії дезінформації, яка формується в Україні у співпраці з партнерами. Зокрема, у 2021 році було створено Центр протидії дезінформації при РНБО, що координує

діяльність органів влади, аналітичних центрів та громадських ініціатив. У відповідь на deepfake-атаки та відеоманіпуляції держава запровадила алгоритми верифікації офіційної інформації, оперативно реагуючи на спроби маніпуляцій. Це сприяє зменшенню впливу ворожих інформаційних хвиль, зокрема в кризові моменти [27].

З початком бойових дій на сході України у 2014–2015 роках РФ активізувала дезінформаційні кампанії, спрямовані на делегітимацію української армії та створення образу «громадянської війни». Приклади таких атак включають фейки про «розіп'ятого хлопчика в Слов'янську», «звірства українських військових», «таємничі каральні батальйони» тощо. Сюжети та фальшиві свідчення поширювалися через федеральні телеканали РФ та проросійські онлайн-ресурси, а також через мережу ботів у соціальних медіа [27].

У 2016–2019 роках відбувається активне перенесення інформаційної війни в цифровий простір. Російська «фабрика тролів» (IRA) створювала тисячі акаунтів у Facebook, Twitter, YouTube, що мімікрували під українських користувачів, просуваючи деструктивні наративи. Особливий акцент робився на темах корупції, зради інтересів, "зовнішнього управління", розчарування в реформах та євроінтеграції. Аналітики фіксували координацію таких кампаній із внутрішніми протестними настроями та важливими політичними подіями [28].

У 2022 році, із початком повномасштабного вторгнення, інформаційна агресія вийшла на новий рівень. У перші дні війни російські ресурси активно поширювали повідомлення про «здачу Києва», «знищення інфраструктури», «втечу керівництва», «масові жертви», що супроводжувалися фотомонтажами, відеофейками та бот-розсилками в Telegram. Основними цілями були деморалізація цивільного населення та дестабілізація тилу [33].

У 2023–2024 роках РФ активізувала використання deepfake-технологій — з'явилися фальшиві відеозаписи з "виступами" українських лідерів, у яких вони нібито визнають поразку або закликають до капітуляції. Такі відео швидко ширилися через TikTok, Telegram, Instagram, часто — під виглядом «зливів

зсередини». Супровідний текст підсилював недовіру до держави, армії та західних партнерів [40].

Також у цей період посилюється атака на внутрішню єдність українського суспільства. Через псевдоаналітичні канали просуваються наративи про конфлікти між переселенцями та місцевим населенням, між військовими та цивільними, релігійні суперечності тощо. Наприклад, у 2024 році було виявлено декілька інформаційних хвиль, спрямованих на створення уявного конфлікту між військовими та волонтерами, з фокусом на «недоотриману допомогу», «крадіжки» або «неправильний розподіл ресурсів» [40].

У 2024 році особливо помітним стало поширення дезінформації через месенджери - Telegram, Viber, WhatsApp. Під виглядом «ексклюзивної інформації» надсилалися анонімні повідомлення про «повну мобілізацію», «закриття кордонів», «втрату територій» тощо. Ці повідомлення запускали паніку, спричиняли хвилі відтоку людей та тиснули на психіку населення в прифронтових регіонах.

У 2025 році, в контексті наближення до виборчих процесів, інформаційні атаки набули електорального спрямування. Противник активно створює та просуває фейки про «зміну Конституції», «скасування виборів», «втручання Заходу», «списки зрадників», «антиукраїнських кандидатів». Ці інформаційні вкиди спрямовані на дестабілізацію політичної ситуації, зниження явки виборців та делегітимацію результатів [40].

Ще одним напрямом є інформаційна атака на культуру та мову. Російські ресурси системно поширюють меседжі про «насильницьку українізацію», «переслідування православних», «заборону російської культури», створюючи штучну картину внутрішньої культурної війни. У 2022–2025 роках особливо активно поширювалися фейки щодо УПЦ (МП), з метою підірвати міжконфесійну злагоду.

Крім того, РФ продовжує використовувати штучний інтелект для автоматизованого створення великої кількості фейкових новин, дописів,

коментарів. Це значно ускладнює розпізнавання правдивої інформації, а також посилює потребу в медіаграмотності громадян. Розвиток нейромереж типу GPT, Midjourney, DALL·E дозволяє противнику продукувати сотні "реалістичних" картинок і текстів щоденно.

У відповідь на зростаючу дезінформаційну загрозу, Україна посилила координацію з міжнародними партнерами: створено платформи обміну даними між Центром стратегічних комунікацій, СБУ, НАТО StratCom COE, аналітичними структурами ЄС. На національному рівні важливу роль відіграють незалежні фактчекінгові організації (StopFake, VoxCheck), а також інформаційні кампанії Мінцифри щодо цифрової безпеки [40].

Отже, з 2014 року інформаційний простір України став ареною цілеспрямованого та багатовекторного впливу з боку Російської Федерації, що охоплює як традиційні канали масової комунікації, так і новітні цифрові технології. Інформаційні атаки еволюціонували від простих фейкових повідомлень до комплексних операцій із застосуванням бот-мереж, глибоких фейків, автоматизованого генеративного контенту та психологічного тиску. Їх головною метою є підрив національної єдності, деморалізація суспільства, делегітимація державних інституцій, розпалювання паніки, послаблення бойового духу та вплив на політичні процеси.

Особливої інтенсивності дезінформаційні кампанії набули в період повномасштабної збройної агресії у 2022–2025 роках. Спостерігається підвищення рівня технічної складності атак, що вимагає від держави постійного вдосконалення систем інформаційної безпеки, розвитку медіаграмотності громадян, міжнародної співпраці та підтримки незалежних інституцій фактчекінгу.

Аналіз основних інформаційних атак дозволяє зробити висновок, що інформаційна війна не є лише фоновим явищем, а виступає ключовим інструментом сучасного гібридного конфлікту. Україна, як форпост європейської демократії, щоденно стикається з інформаційними викликами, які формують нову реальність

національної безпеки. Адекватне реагування на ці виклики потребує системного аналізу, проактивної комунікації з громадянами, міжвідомчої координації та посилення кібер- і комунікаційної стійкості.

2.2 Механізми та платформи розповсюдження дезінформації

У сучасних умовах російсько-української війни інформаційна складова набуває особливої ваги, перетворюючись на окремий фронт протистояння. Дезінформація як один із ключових інструментів інформаційної війни стала основою численних кампаній, спрямованих на послаблення державного управління, підрив суспільної довіри до інституцій, а також на маніпулювання громадською думкою як в Україні, так і за її межами. З 2014 року Російська Федерація систематично розгортає багаторівневі дезінформаційні операції, зокрема із використанням традиційних та цифрових платформ. Ці дії мають ознаки гібридної війни, в якій інформаційний вплив доповнює воєнні дії, дозволяючи досягати стратегічних цілей без прямого зіткнення.

Механізми поширення дезінформації включають цілий комплекс комунікативних і технологічних прийомів. Насамперед ідеться про використання маніпулятивних наративів, які цілеспрямовано формуються в межах пропагандистського дискурсу. Типовими прикладами таких наративів є твердження про нібито «громадянську війну» в Україні, «неонацистський режим», «утиски російськомовного населення» або «штучність української державності». Ці конструкції повторюються в різних форматах та каналах, що забезпечує їх глибоке закріплення в масовій свідомості. Ще одним поширеним механізмом є створення та трансляція фейкових новин. Такі матеріали мають вигляд офіційних повідомлень або журналістських розслідувань, однак подають спотворені, вигадані або перекручені факти. Фейкові новини часто апелюють до емоцій — страху, гніву, співчуття — що дозволяє підсилити психологічний вплив на аудиторію [21].

Важливою складовою дезінформаційної діяльності є застосування бот-мереж та інтернет-тролів. Створені масово фейкові акаунти в соціальних мережах і месенджерах поширюють заздалегідь підготовлені повідомлення, створюючи ілюзію масштабного суспільного обговорення чи підтримки певної позиції. Така діяльність також дозволяє штучно підвищувати охоплення дезінформаційного контенту та здійснювати тиск на інформаційне середовище. Окрім того, дезінформація легітимується через залучення псевдоекспертів, підставних аналітичних центрів, фейкових «наукових» публікацій, які створюють ілюзію об'єктивності та глибини дослідження. У контексті технологічного розвитку зростає роль цифрових фальсифікацій, зокрема відео- та аудіоматеріалів, створених за допомогою deepfake. У 2022 році прикладом такого інструменту стало фальшиве відео з «виступом» Президента України, у якому він нібито закликає здатися. Попри швидке спростування, відео встигло поширитися на багатьох ресурсах і викликати суспільний резонанс [26].

Платформи розповсюдження дезінформації охоплюють як традиційні ЗМІ, так і новітні цифрові інструменти. Російські державні телеканали, зокрема RT, «Россия 24», «Первый канал», відіграють провідну роль у трансляції пропагандистських повідомлень на внутрішню й міжнародну аудиторію. Через супутникове мовлення та інтернет-трансляції ці канали доступні навіть у тих регіонах, де їхній контент формально заборонено. Значну роль у дезінформаційному впливі відіграють інтернет-ЗМІ та агрегатори новин, зокрема сайти NewsFront, SouthFront, Sputnik, які подають маніпулятивну інформацію у формі «аналітичних» або «експертних» матеріалів. Соціальні мережі, зокрема Facebook, Twitter (нині X), Telegram і ВКонтакте, стали головним середовищем для оперативного поширення фейків. Через анонімні або підставні акаунти поширюються маніпулятивні повідомлення, які миттєво ретранслюються через різні цифрові канали, набуваючи вірусного характеру. Telegram, зокрема, набув значної популярності серед проросійських інформаційних джерел. Анонімні канали

поширюють фейкові новини про мобілізацію, втрати ЗСУ, ситуацію в тилу, намагаючись викликати паніку серед населення. Інструментом легітимації дезінформаційного контенту слугують також відеоплатформи, такі як YouTube, де під виглядом документалістики або журналістських розслідувань публікуються матеріали, що містять антиукраїнську риторику. Окрему нішу займають форуми й сайти конспірологічного спрямування, які виконують роль «інкубаторів» для формування нових дезінформаційних меседжів, що згодом потрапляють до мейнстримових ресурсів [26].

Особливістю дезінформаційних кампаній після 24 лютого 2022 року стало їх масштабування і глобалізація. Російська Федерація активізувала поширення повідомлень багатьма мовами, включаючи англійську, французьку, іспанську, намагаючись сформувати альтернативну версію подій серед світової аудиторії. В інформаційному просторі поширювалися меседжі про «захист Донбасу», «боротьбу з неонацизмом», «наявність біолабораторій США в Україні», що мали на меті викликати сумніви в легітимності українського спротиву. Додатково дезінформація використовувалася як інструмент дискредитації партнерів України в Європі та США. Таким чином, дезінформаційна діяльність Російської Федерації у контексті війни проти України є багатовимірною, технологічно розвиненою та інтегрованою в загальну стратегію гібридної агресії. Її ефективність забезпечується поєднанням традиційних пропагандистських методів із новітніми цифровими технологіями та використанням широкого спектра інформаційних платформ. Протидія таким загрозам потребує не лише технічних рішень, а й інформаційної грамотності суспільства, ефективної комунікаційної політики держави, міжнародної співпраці та постійного моніторингу медіапростору [26].

Окремим вектором дезінформаційної діяльності стала мілітаризація історичної пам’яті та перекручення фактів минулого. Російська пропаганда активно використовує тематику Другої світової війни, репрезентуючи себе як єдиного спадкоємця «перемоги над нацизмом», водночас приписуючи Україні

«неонацистські» тенденції. Така історична інверсія не лише виконує ідеологічну функцію, але й апелює до емоційної складової сприйняття, особливо серед старших поколінь у пострадянських країнах. Використання цього дискурсу дозволяє Росії формувати морально-політичне виправдання агресивних дій, зокрема серед внутрішньої аудиторії та частини міжнародної спільноти.

Крім того, дезінформація виконує стратегічну функцію в контексті деморалізації противника. Поширення фейків про нібито поразки Збройних Сил України, масові втрати, зраду у вищому військовому командуванні або соціальні конфлікти всередині країни спрямоване на підрив бойового духу та довіри до державних інституцій. Такі кампанії активізуються під час ключових військових подій, наприклад, під час оборони Маріуполя чи контрнаступів на півдні. Психологічний ефект посилюється через координацію між анонімними каналами, бот-мережами та проросійськими медіа, що забезпечує синхронізованість та масштабність дезінформаційних хвиль.

Отже, аналіз механізмів і платформ поширення дезінформації в контексті російсько-української війни засвідчив, що інформаційна складова є ключовим елементом сучасної гібридної агресії. Російська Федерація активно застосовує широкий спектр інструментів інформаційного впливу — від традиційної пропаганди й фейкових новин до складних технологічних рішень на основі штучного інтелекту. Основні механізми, зокрема маніпулятивні наративи, використання бот-мереж, трансляція фейкових повідомлень та залучення псевдоекспертів, забезпечують широке охоплення аудиторії та формують спотворену картину дійсності. Соціальні мережі, месенджери, проросійські ЗМІ та відеоплатформи стали основними каналами поширення дезінформації, що дозволяє агресору здійснювати інформаційний тиск як на українське суспільство, так і на міжнародну спільноту.

Особливу небезпеку становить здатність дезінформаційних кампаній до швидкої адаптації та масштабування, що ускладнює їх виявлення й нейтралізацію.

Досвід останніх років свідчить, що ефективна протидія дезінформації можлива лише за умови комплексного підходу, який включає розвиток медіаграмотності, інституційну протидію інформаційним загрозам, активну позицію громадянського суспільства та міжнародну співпрацю. Урахування цих чинників є критично важливим для забезпечення інформаційної безпеки України в умовах триваючої війни.

2.3. Вплив російської пропаганди на суспільну думку в Україні та за кордоном

У сучасних умовах гібридної війни, що триває між Російською Федерацією та Україною з 2014 року і особливо загострилася після початку повномасштабного вторгнення у 2022 році, інформаційна складова набула винятково важливого значення. Російська пропаганда стала системним і багатоаспектним інструментом впливу на суспільну думку як всередині України, так і за її межами. Її метою є не лише поширення дезінформації, а й формування викривленої картини реальності, яка слугує досягненню політичних, військових і стратегічних інтересів Кремля. Пропагандистські зусилля мають на меті посіяти розбрат, підважити довіру до демократичних інституцій, зруйнувати міжнародну підтримку України та створити позитивний імідж РФ на зовнішній арені [26].

У межах українського інформаційного простору російська пропаганда спрямована передусім на підрив національної єдності, дестабілізацію суспільно-політичної ситуації та послаблення бойового духу населення. Основні методи включають масове поширення фейкових новин, емоційно забарвлених маніпуляцій, використання напівправди та фабрикації подій. Наприклад, у періоди загострення бойових дій регулярно поширювалися повідомлення про уявні масові жертви серед мирного населення, «злочини» Збройних Сил України або гуманітарні катастрофи, які нібито замовчувалися офіційною владою. Такі інформаційні атаки створювали атмосферу паніки, сприяли деморалізації та посиленню недовіри до офіційних

джерел. Особливо вразливими до таких впливів є соціальні групи, що мають обмежений доступ до альтернативної інформації або критичне ставлення до державних інституцій.

Окрему увагу варто приділити російському інформаційному впливу за межами України. На міжнародному рівні російська пропаганда діє з метою дискредитації української держави, зниження рівня підтримки України серед країн-партнерів, а також створення привабливого образу Росії як жертви міжнародної змови або захисника традиційних цінностей. У цьому контексті активно використовується поширення спотворених наративів про нібито «громадянський конфлікт» в Україні, «утиски російськомовного населення», «зростання неонацистських настроїв» та «зовнішнє управління» українською політикою. Такі меседжі особливо активно транслюються в країнах Європейського Союзу, США, Латинської Америки та на пострадянському просторі через мережу міжнародних телеканалів, інформаційних агентств, псевдонаукових видань та підконтрольних «експертів» [32].

Найбільш небезпечним інструментом розповсюдження дезінформації стали цифрові платформи, зокрема соціальні мережі. Швидкість циркуляції інформації, можливість цільового впливу та низький рівень перевірки фактів у цих середовищах створюють сприятливе підґрунтя для реалізації інформаційних атак. Російські структури активно використовують фейкові акаунти, мережі ботів, тролів та «фабрики контенту» для створення ілюзії масової підтримки певних тез, деструктивної поляризації дискусій, атак на опозиційні голоси та поширення фейкових новин. У результаті виникає ефект «інформаційної ілюзії більшості», який здатен суттєво впливати на політичні вподобання, наративи громадської думки та виборчу поведінку, особливо серед молоді, яка значною мірою споживає новини саме через цифрові платформи.

Важливу роль у впливі російської пропаганди відіграє експлуатація історичних та культурних наративів. Постійне апелювання до спільного минулого,

зокрема періоду Другої світової війни, героїзація Радянського Союзу та ностальгія за «слов'янською єдністю» — це типові інструменти, які сприяють нав'язуванню ідеї «братніх народів», що нібито виправдовує поточну агресію. Також широко використовується риторика про «історичну несправедливість», «штучність української державності» та «захист російськомовного населення» — усі ці наративи знаходять резонанс серед аудиторій, які недостатньо обізнані з українською історією або схильні до авторитарного стилю мислення.

Ключовим чинником, що визначає ефективність російської пропаганди, є рівень медіаграмотності населення та доступ до незалежних джерел інформації. Дослідження показують, що у суспільствах із розвиненими критичним мисленням, освітою та високим рівнем довіри до авторитетних медіа вплив дезінформації суттєво зменшується. Натомість у регіонах, де домінують емоційне сприйняття, інформаційна ізоляція або де державна політика недостатньо підтримує незалежні медіа, пропаганда може мати глибокий і тривалий вплив. У контексті України важливою складовою протидії стали державні ініціативи з підвищення медіаграмотності, включення теми дезінформації у шкільну та університетську освіту, а також розвиток незалежних фактчекінгових платформ [42].

Від 2014 року і особливо з 2022 року інформаційна агресія РФ трансформувалася у масштабний, системно організований фронт гібридної війни. Дезінформаційні кампанії стали більш скоординованими, технічно складними та адаптивними до змін політичного контексту. Росія застосовує широкий спектр інструментів – від кібератак і «зливу» підроблених документів до створення фейкових «розслідувань», «аналітики» та маніпулювання результатами соціологічних досліджень. Ці кампанії охоплюють не лише територію України, а й міжнародні інформаційні платформи, що підтверджує стратегічний характер інформаційної війни як складової загального плану агресії.

У відповідь на такі виклики Україна послідовно формує політику інформаційної безпеки, яка включає правові, технічні, освітні та комунікаційні

компоненти. Серед ключових заходів — запровадження санкцій проти медіа-структур і фізичних осіб, причетних до поширення дезінформації, розвиток системи інформаційного моніторингу, створення Центру протидії дезінформації при РНБО, підтримка незалежних журналістських розслідувань, співпраця з міжнародними партнерами та технологічними платформами (Facebook, YouTube, Twitter/X). Також важливими є активна участь громадянського суспільства та волонтерських ініціатив, які здійснюють щоденний аналіз, спростування фейків та роз'яснювальну роботу серед населення [24].

Узагальнюючи викладене, слід підкреслити, що російська пропаганда є надзвичайно потужним та адаптивним інструментом інформаційної агресії, що відіграє ключову роль у реалізації гібридної стратегії РФ. Вона здійснює багатовимірний вплив на суспільну думку як в Україні, так і на міжнародному рівні, використовуючи емоційні, культурні, соціальні та технологічні механізми. Її ефективність залежить від сприйнятливості цільової аудиторії, рівня критичного мислення, доступу до незалежної інформації та здатності держави й суспільства вчасно реагувати на загрози.

Отже, для забезпечення національної інформаційної безпеки в умовах гібридної війни Україна потребує системного, міждисциплінарного та стратегічного підходу, який передбачає не лише технічні засоби захисту, а й формування критичного мислення, розвиток медіаосвіти, підтримку незалежних медіа та активну міжнародну співпрацю. Тільки у разі ефективної координації дій усіх зацікавлених сторін — держави, громадянського суспільства, медіаспільноти та міжнародних партнерів — можливо протистояти деструктивному інформаційному впливу Російської Федерації та зберегти стабільність демократичного інформаційного простору.

Отже узагальнюючи весь розділ, можна сказати, що, аналіз механізмів, платформ і впливів російської дезінформації свідчить, що інформаційна війна стала невід'ємною складовою сучасної гібридної агресії проти України. З 2014 року і

особливо в умовах повномасштабного вторгнення у 2022–2025 роках, інформаційний простір України зазнав безпрецедентного тиску з боку Російської Федерації, яка активно використовує як традиційні ЗМІ, так і новітні цифрові технології — від бот-мереж до штучного інтелекту й deepfake. Основними цілями цих дезінформаційних кампаній є деморалізація населення, підрив довіри до державних інституцій, розпалювання панічних настроїв, вплив на внутрішньополітичні процеси та дискредитація України на міжнародній арені.

Соціальні мережі, месенджери, відеоплатформи та проросійські медіа стали ключовими каналами поширення спотвореної інформації, що ускладнює виявлення та нейтралізацію загроз через швидкість і гнучкість таких атак. У цьому контексті інформаційна війна перестає бути лише супутнім явищем бойових дій, а виступає стратегічним інструментом формування нової архітектури безпеки.

Особливої уваги заслуговує використання Росією культурно-історичних наративів та маніпуляцій зі значущими для цільової аудиторії темами, такими як «братні народи», «боротьба з нацизмом» або «захист російськомовного населення». Такі меседжі не лише апелюють до емоційного сприйняття, але й формують спотворене уявлення про причини конфлікту, виправдовують агресію і легітимізують дії Російської Федерації як на території України, так і в очах міжнародної аудиторії. Таким чином, пропаганда не обмежується інформуванням, а слугує інструментом ідеологічного тиску й дестабілізації.

У свою чергу, важливим чинником протидії інформаційній агресії є розвиток критичного мислення, медіаграмотності та інформаційної культури громадян. Досвід останніх років показує, що зростання обізнаності населення щодо технік маніпуляції, розширення доступу до перевірених джерел, підтримка незалежної журналістики та фактчекінгових ініціатив сприяють зниженню ефективності ворожих інформаційних впливів. Іншими словами, саме підвищення інформаційної самосвідомості є одним з ключових елементів національної безпеки в умовах гібридної війни.

Для ефективної протидії цим загрозам Україна потребує комплексного, міждисциплінарного та стратегічного підходу, що включає технічні засоби захисту, розвиток критичного мислення та медіаграмотності, підтримку незалежних медіа і фактчекінгових платформ, міжвідомчу координацію та міжнародну співпрацю. Лише за умов скоординованих дій держави, громадянського суспільства, медіаспільноти й міжнародних партнерів можливо забезпечити стійкість до деструктивного інформаційного впливу та зберегти демократичні засади українського інформаційного простору.

РОЗДІЛ 3.
ПЕРСПЕКТИВИ ПРОТИДІЇ ІНФОРМАЦІЙНИМ ЗАГРОЗАМ В УКРАЇНІ

3.1 Державна політика у сфері інформаційної безпеки

З початку гібридної агресії Російської Федерації проти України, питання інформаційної безпеки на державному рівні набуло виняткової актуальності. Інформаційний фронт став не менш важливим за військовий, а отже — формування ефективної державної політики у цій сфері стало пріоритетом національної безпеки. В умовах постійної інформаційної загрози з боку зовнішніх (насамперед — російських) акторів, держава Україна змушена оперативно адаптувати законодавство, модернізувати інституційні механізми, впроваджувати стратегії інформаційної протидії та зміцнювати співпрацю з міжнародними партнерами.

Одним із ключових напрямів інформаційної безпеки є кібербезпека. У 2016 році ухвалено Закон України «Про основні засади забезпечення кібербезпеки України», що визначив правові та організаційні засади захисту кіберпростору. Держава послідовно зміцнює систему кіберзахисту, створюючи національні комунікаційно-інформаційні системи, системи реагування на інциденти, інститути обміну інформацією. У 2022–2024 роках Україна зазнала численних кібератак на урядові портали, банківську сферу та критичну інфраструктуру, що підкреслило необхідність подальшого посилення кіберзахисту [18].

Україна активно співпрацює у сфері інформаційної безпеки з міжнародними партнерами. Вона є учасницею Центру передових технологій НАТО у галузі кібероборони (CCDCOE), бере участь у проектах Європейського Союзу з протидії дезінформації, зокрема у програмі EU vs Disinfo. У 2023 році Україна провела низку спільних кібернавчань із країнами НАТО, спрямованих на відпрацювання реагування на масштабні кібератаки. Така співпраця зміцнює спроможності держави у сфері інформаційної оборони.

Першим вагомим кроком стало прийняття Доктрини інформаційної безпеки України 2017 року, яка визначила основні засади державної політики у сфері захисту національного інформаційного простору. Доктрина передбачає забезпечення інформаційного суверенітету України, недопущення використання інформації з метою підриву конституційного ладу, суверенітету та територіальної цілісності держави (Указ Президента України №47/2017). У цьому документі також наголошується на важливості стратегічних комунікацій, сприяння розвитку незалежних медіа, підвищення рівня медіаграмотності населення та протидії ворожим інформаційним впливам [10].

На реалізацію положень Доктрини було спрямовано створення та зміцнення профільних інституцій, зокрема Центру стратегічних комунікацій та інформаційної безпеки при Міністерстві культури та інформаційної політики України. Центр забезпечує інформаційну підтримку державної політики, проводить оперативний аналіз дезінформаційних кампаній, а також координує міжвідомчу співпрацю в цій сфері. Крім того, функціонують структури при Службі безпеки України, Міністерстві оборони, Національній раді з питань телебачення і радіомовлення та інших органах, які здійснюють заходи з моніторингу, блокування та нейтралізації інформаційних загроз.

Окремим напрямом державної політики стала медіаосвіта та медіаграмотність населення. З 2020 року в Україні реалізується проєкт «Фільтр», що включає освітні програми, тренінги, онлайн-курси для молоді, державних службовців та журналістів. Такі ініціативи сприяють розвитку критичного мислення, вміння аналізувати джерела інформації та протидіяти маніпулятивному впливу. Важливо, що елементи медіаосвіти інтегруються у шкільні програми, вищу освіту та систему підвищення кваліфікації.

Незважаючи на певні досягнення, політика держави у сфері інформаційної безпеки стикається з низкою проблем. Насамперед це фрагментованість міжвідомчої взаємодії, недостатнє фінансування, а також кадровий дефіцит у сфері

кіберзахисту та аналітики. Окремі інформаційні ініціативи залишаються малоефективними через відсутність довгострокового планування або моніторингу результатів. Також існує потреба в оновленні стратегічних документів з урахуванням сучасних викликів, зокрема поширення штучного інтелекту, deepfake-технологій та автоматизованих систем впливу.

У майбутньому державна політика має бути більш інтегрованою, системною та адаптивною до нових загроз. Варто розробити єдину національну платформу моніторингу інформаційних атак, зміцнити аналітичні центри, які займаються дослідженням інформаційних ризиків, запровадити регулярні аудити інформаційної безпеки в державних установах.

У відповідь на повномасштабне вторгнення Росії у 2022 році, держава активізувала зусилля з протидії ворожим інформаційним впливам. Зокрема, в умовах воєнного стану набули чинності нові законодавчі ініціативи щодо заборони проросійських медіа, обмеження трансляції контенту, що може бути використаним у шкоду національній безпеці, а також впровадження єдиного телемарафону "Єдині новини" як механізму централізованого інформування населення. Хоча цей підхід має як позитивні (протидія паніці, єдність інформаційного простору), так і дискусійні наслідки (обмеження медіаплюралізму), його ефективність у кризовий період визнається багатьма аналітиками [36]. Окрему увагу приділено співпраці з міжнародними партнерами. Україна бере участь у програмах НАТО з розвитку стратегічних комунікацій та кібербезпеки, а також у проектах ЄС щодо боротьби з дезінформацією, зокрема в межах ініціативи East StratCom Task Force та EUvsDisinfo. Такі партнерства дозволяють Україні отримувати експертну підтримку, обмінюватися досвідом і адаптувати передові практики до національного контексту. Згідно з дослідженням Київського безпекового форуму 2023 року, міжнародна підтримка відіграє ключову роль у забезпеченні інформаційної стійкості України в умовах війни.

Детальніше ознайомитися з дервною політикою України у сфері інформаціної безпеки можа у таблиці 3.1.

Таблиця 3.1. Державна політика України у сфері інформаційної безпеки: заходи, досягнення, виклики та перспективи (2016–2024)

Напрям	Ключові заходи / інституції	Досягнення / результати	Проблеми / виклики	Пропозиції / перспективи
Кібербезпека	Закон «Про кібербезпеку» (2016), реагування на інциденти, національні системи захисту	Захист критичної інфраструктури, участь у навчаннях НАТО, зміцнення технічної спроможності	Часті кібератаки, кадровий дефіцит, потреба в оновленні законодавства	Розвиток державно-приватного партнерства, аудити кіберзахисту, оновлення технічної бази
Інституційна підтримка	Центр стратегічних комунікацій, структури при СБУ, РНБО, Нацрада з ТБ та РМ	Оперативний моніторинг, міжвідомча співпраця, створення координаційного механізму	Фрагментованість міжвідомчої взаємодії, нестача ресурсів	Формування єдиної платформи реагування на інформаційні загрози, посилення координації
Доктринальні основи	Доктрина інформаційної безпеки (2017), укази Президента	Визначення стратегії, пріоритетів, підтримка незалежних ЗМІ, наголос на медіаграмотності	Застарілість підходів, потреба в адаптації до новітніх загроз (deepfake, ШІ)	Оновлення доктринальних документів, впровадження цифрової дипломатії
Медіаосвіта і просвітництво	Проєкт «Фільтр», співпраця з IREX, Internews, «Детектор медіа»	Тренінги, онлайн-курси, інтеграція в освіту; +30% до навичок розпізнавання фейків серед молоді	Обмежене фінансування, нерівний доступ до програм	Ширше охоплення аудиторій, закріплення в освітніх стандартах, розвиток критичного мислення
Інформаційне реагування (2022+)	Телемарафон «Єдині новини», заборона проросійських медіа, централізована комунікація	Єдність інформаційного простору в умовах війни, зменшення паніки	Ризики надмірної централізації, обмеження медіаплюралізму	Баланс між безпекою і свободою слова, прозора інформаційна політика
Міжнародна співпраця	Участь у NATO StratCom, CCDCOE, EUvsDisinfo, East StratCom, підтримка від ЄС, ОБСЄ, G7	Обмін досвідом, зміцнення спроможностей, адаптація кращих практик	Залежність від зовнішньої підтримки, потреба в інституціоналізації досвіду	Інтеграція до європейської системи колективної інформаційної безпеки, розширення цифрової дипломатії
Регуляторні заходи (санкції)	Санкції проти пропагандистських ЗМІ, заборона трансляцій, обмеження проросійського контенту	Блокування джерел дезінформації, очищення медіаполя	Можливі звинувачення у цензурі, втрати довіри до держінформації	Прозорість критеріїв блокування, залучення громадськості до моніторингу
Цифрові виклики (нові загрози)	Використання deepfake, штучного інтелекту, бот-мереж, автоматизованих систем впливу	Усвідомлення загроз, початок аналітичної роботи	Відсутність готових інструментів реагування, технологічна відсталість	Інвестиції у нові технології, створення інноваційних аналітичних центрів

У сфері освіти та просвітництва держава також реалізує політику підвищення інформаційної обізнаності громадян. У партнерстві з неурядовими організаціями, такими як StopFake, Internews Ukraine, IREX, впроваджуються програми з медіаграмотності для школярів, студентів, держслужбовців та журналістів. За даними дослідження ГО "Детектор медіа", рівень базових навичок розпізнавання фейкових новин зріс серед молоді на 30% у порівнянні з 2020 роком [26].

На міжнародному рівні, політика інформаційної безпеки дедалі більше інтегрується у загальноєвропейську систему колективної безпеки. Наприклад, у 2022 році Європейський Союз започаткував механізми санкцій за поширення дезінформації, які було застосовано до низки російських державних пропагандистських ресурсів. Подібні ініціативи мають важливе значення для створення спільного фронту боротьби з ворожими інформаційними впливами.

Водночас державна політика в інформаційній сфері стикається з низкою викликів. Зокрема, постає проблема збереження балансу між безпекою та свободою слова, а також забезпечення відкритості комунікації в умовах інформаційної централізації. Експерти наголошують на потребі переходу від реактивної до проактивної моделі інформаційної політики, яка передбачає системне прогнозування ризиків, розвиток нових форм цифрової дипломатії та ефективну присутність держави в соціальному медіасередовищі.

Отже, державна політика України у сфері інформаційної безпеки є динамічною та багатовекторною. Вона включає правові, інституційні, технічні, просвітницькі та міжнародні компоненти, що спільно спрямовані на нейтралізацію інформаційних загроз і забезпечення стійкості національного інформаційного простору. Зміцнення цієї політики є необхідною умовою для збереження демократичного ладу, національного суверенітету та ефективної протидії гібридним впливам в умовах тривалої війни та глобальної нестабільності.

3.2 Роль громадянського суспільства та незалежних ЗМІ у протидії дезінформації

Значення громадянського суспільства та незалежних засобів масової інформації у боротьбі з дезінформацією в Україні й світі набуло особливої актуальності у зв'язку з ескалацією гібридної війни, частиною якої є інформаційна агресія. У контексті постійної зовнішньої дестабілізації, інформаційних атак та кампаній з маніпулювання громадською думкою, саме активна позиція громадянського сектору й медіа стала важливим чинником формування стійкості суспільства до зовнішнього інформаційного тиску. Цей процес охоплює різноманітні сфери: від фактчекінгу й медіаграмотності до мобілізації локальних ініціатив та міжнародного партнерства.

Громадянське суспільство — це сукупність організацій та об'єднань, що функціонують незалежно від державної влади та діють у сфері захисту прав і свобод громадян, у тому числі в інформаційному просторі. В умовах гібридної війни в Україні, громадянські ініціативи стали активними учасниками процесу ідентифікації, нейтралізації та попередження інформаційних загроз. Однією з провідних ініціатив у цій сфері є проєкт StopFake, заснований у 2014 році. Його місією стало виявлення, спростування та систематизація неправдивої інформації, що розповсюджується щодо України, зокрема у контексті анексії Криму та збройного конфлікту на Донбасі. За роки роботи платформа верифікувала й спростувала понад 5000 фейкових повідомлень, а її діяльність вийшла за межі внутрішнього інформаційного простору завдяки багатомовним випускам новин (у т.ч. англійською, іспанською, російською), що дозволило активно протидіяти поширенню дезінформації на міжнародному рівні.

Іншою важливою ініціативою є VoxCheck — фактчекінгова платформа, яка аналізує правдивість публічних заяв, новин та політичних наративів. У відповідь на повномасштабне вторгнення Росії у 2022 році, VoxCheck запустив окремий проєкт «VoxCheck Military», який зосереджується на перевірці військової дезінформації.

Зокрема, організація активно моніторить соціальні мережі, виявляє фейкові акаунти, спростовує наративи щодо «покинутих позицій ЗСУ», «зради влади» та інші деструктивні інформаційні вкиди. У 2023 році, у співпраці з технологічними платформами, було заблоковано понад 100 акаунтів, пов'язаних із системною дезінформацією в українському сегменті мережі [42].

Значну аналітичну роботу проводить також Detector Media, який фокусується на моніторингу як українського, так і російського медіаполя. Організація у 2022–2023 роках публікувала щоденні аналітичні дайджести «Маніпуляції дня», у яких систематизувала маніпулятивні техніки, зокрема використання фальсифікованих цитат, підміни понять, контекстних викривлень тощо. Було ідентифіковано понад 200 ключових наративів кремлівської пропаганди, що циркулювали в українських медіа та соцмережах [27].

Освітній компонент у протидії дезінформації також має надзвичайне значення. Програма «Вивчай та розрізняй», реалізована міжнародною організацією IREX, з 2015 року здійснює системну медіаосвітню роботу в українських школах. Лише у 2022–2023 роках програму пройшли понад 38 000 школярів і 2500 педагогів, а результати оцінювання продемонстрували зростання здатності розпізнавати маніпуляції до 85% серед учасників після тренінгів [35].

На міжнародному рівні важливу роль у виявленні та спростуванні дезінформаційних кампаній Росії відіграє проєкт EUvsDisinfo, заснований Європейською службою зовнішніх дій. Його база даних містить понад 15 000 прикладів кремлівської дезінформації, зокрема щодо війни в Україні, наративів про «неіснуючі біолабораторії» або «нацифікацію» української влади. EUvsDisinfo тісно співпрацює з українськими громадськими організаціями, надаючи аналітичну підтримку та сприяючи просуванню правди у міжнародному медіапросторі [30].

Організація Internews Ukraine також активно працює в напрямі підтримки незалежної журналістики, фактчекінгу та створення освітнього контенту для широкої аудиторії. У 2022–2023 роках було проведено понад 200 тренінгів для

журналістів з теми медіаосвіти, а також створено кампанії у соціальних мережах для молоді, спрямовані на підвищення стійкості до фейкової інформації. Internews також підтримала створення та функціонування понад 30 локальних незалежних ЗМІ в регіонах, де інформаційний вплив ворога був особливо потужним [34].

Незалежні ЗМІ також відіграють фундаментальну роль у забезпеченні прозорості інформаційного простору. У контексті війни вони не лише виконують інформаційну функцію, але й беруть участь у формуванні національного наративу, що протистоїть пропагандистським конструкціям агресора. Показовим є приклад Суспільного мовлення України, яке, попри обмежені ресурси, демонструє високий рівень професіоналізму та редакційної незалежності, надаючи перевірену та збалансовану інформацію. Згідно з дослідженням Рейтер Інституту журналістики, рівень довіри до Суспільного у 2023 році зріс до 48 %, що є одним із найвищих показників серед українських медіа.

Крім безпосереднього фактчекінгу та аналітики, важливим напрямом діяльності громадянського суспільства є розвиток медіаграмотності населення. У партнерстві з міжнародними організаціями, такими як IREX, Internews та DW Akademie, в Україні реалізується низка освітніх програм, спрямованих на формування критичного мислення, здатності ідентифікувати фейки, аналізувати джерела інформації та уникати емоційної маніпуляції. Зокрема, програма «Вивчай та розрізняй: інфо-медійна грамотність» охопила понад 15 000 учнів і студентів у 23 областях України з 2020 до 2023 року. Такі ініціативи мають довгостроковий ефект, сприяючи зміцненню демократичного суспільства та формуванню стійкої до пропаганди молоді [35].

Особливо важливою є синергія між громадянськими ініціативами, журналістами та державними структурами. В умовах війни, коли існує потреба у швидкому реагуванні на загрози, ефективна взаємодія між Міністерством культури та інформаційної політики, Центром стратегічних комунікацій, СБУ та незалежними фактчекінговими платформами дає змогу оперативно локалізовувати

ворожі інформаційні кампанії. Наприклад, у 2022–2024 роках під час атак на об'єкти критичної інфраструктури Росія активно поширювала панічні повідомлення через цифрові канали. Швидка реакція громадських ініціатив — з перевіркою та спростуванням цих наративів — запобігла масовій дестабілізації у великих містах.

Однак попри очевидні досягнення, сектор незалежних медіа й громадських організацій в Україні стикається з низкою викликів: недостатнім фінансуванням, ризиком політичного тиску, інформаційною втомою споживачів, а також технологічною еволюцією маніпулятивних інструментів (deepfake, автоматизовані мережі ботів тощо). Крім того, зростає важливість міжнародної солідарності — як у сфері фінансової підтримки, так і на рівні стандартизації підходів до боротьби з дезінформацією. Український досвід поступово інтегрується у глобальний контекст інформаційної безпеки, стаючи прикладом стійкості в умовах тотальної гібридної агресії.

З огляду на динамічний розвиток інформаційного простору та постійні виклики, пов’язані з гібридною агресією проти України, роль громадянського суспільства у протидії дезінформації має тенденцію до посилення. У найближчій перспективі очікується зростання впливу неурядових організацій, ініціативних груп, фактчекінгових проєктів та медіаосвітніх платформ на формування критичного мислення в суспільстві. Зокрема, діяльність таких структур, як VoxCheck, StopFake, «Фільтр», сприятиме подальшому інституційному укріпленню інфраструктури протидії інформаційним загрозам.

Прогнозується, що громадянське суспільство виконуватиме не лише функцію верифікації інформації, а й активно впливатиме на державну політику в сфері інформаційної безпеки через експертизу, аналітику та громадський контроль. Посилення горизонтальних комунікацій між громадськими структурами та освітніми закладами, а також включення питань медіаграмотності до навчальних програм різних рівнів освіти, дозволить сформувати більш стійке до маніпуляцій інформаційне середовище. За умови належної підтримки з боку держави та

міжнародних партнерів, громадянське суспільство України зможе стати ключовим елементом у побудові ефективної, адаптивної та демократично орієнтованої системи інформаційної безпеки.

Детальніше ознайомитися з ролями та інструментами громадянського суспільства у таблиці 3.2.

Таблиця 3.2. Роль та інструменти громадянського суспільства України у протидії дезінформації (2022–2024)

Організація / Ініціатива	Основні напрямки діяльності	Досягнення / Результати
StopFake	Виявлення, спростування та архівація фейків про Україну	>5000 спростованих фейків; багатомовні випуски; міжнародне охоплення
VoxCheck / VoxCheck Military	Фактчек політичних заяв, протидія військовій дезінформації, моніторинг соцмереж	>100 заблокованих фейкових акаунтів; системна перевірка ворожих наративів
Detector Media	Аналітика медіаполя України та РФ, виявлення маніпуляцій і пропагандистських наративів	Ідентифіковано >200 кремлівських наративів; щоденні дайджести «Маніпуляції дня»
IREX — «Вивчай та розрізняй»	Медіаосвіта у школах, тренінги з критичного мислення для учнів і педагогів	38 000 школярів і 2500 вчителів охоплено (2022–2023); зростання розпізнавання фейків до 85%
EUvsDisinfo (спільно з Україною)	Аналіз дезінформаційних кампаній РФ, співпраця з українськими НУО	>15 000 задокументованих фейків; просування правди у міжнародному медіапросторі
Internews Ukraine	Освітні кампанії, підтримка локальних медіа, тренінги для журналістів	>200 тренінгів; підтримка 30+ незалежних регіональних ЗМІ
Суспільне мовлення	Незалежне інформування, формування національного наративу	Рівень довіри у 2023 р. — 48% (один з найвищих в Україні)
«Фільтр» та партнерські платформи	Медіаосвітні ініціативи у співпраці з державою та міжнародними донорами	Охоплено >15 000 учнів і студентів у 23 областях (2020–2023)
Співпраця з державою (МКІП, СБУ, РНБО)	Скоординоване реагування на ворожі інформаційні атаки	Успішне локалізування фейків під час атак на критичну інфраструктуру (2022–2024)
Перспективні напрями	Використання ШІ, розвиток цифрових платформ, інтеграція медіаграмотності в освіту	Прогнозується посилення впливу НУО на держполітику, зростання цифрової мобілізації

У контексті подальшої цифровізації суспільства та зростання ролі соціальних мереж громадянське суспільство матиме можливість більш оперативно реагувати на виклики інформаційної безпеки. Активізація цифрових платформ, розвиток спільнот, які займаються моніторингом інформаційного простору, а також впровадження інноваційних технологій на кшталт штучного інтелекту для

виявлення фейкових новин створять нові інструменти для швидкого виявлення та нейтралізації дезінформаційних кампаній. Проте успіх цих зусиль буде значною мірою залежати від рівня довіри громадян до громадських ініціатив та незалежних ЗМІ, а також від здатності цих інститутів підтримувати високі стандарти професійної етики та об’єктивності в інформаційному полі [25].

Отже, роль громадянського суспільства та незалежних медіа у протидії дезінформації є стратегічною. Їхня діяльність забезпечує не лише оперативне виявлення загроз, а й формує довгострокову інформаційну культуру, що ґрунтується на достовірності, відкритості та критичному мисленні. Посилення взаємодії між цими секторами, державою та міжнародними партнерами є запорукою ефективної інформаційної оборони України.

3.3 Міжнародний досвід боротьби з інформаційними війнами та перспективи його застосування в Україні

У сучасному глобалізованому світі інформаційні війни стали невід'ємною складовою міждержавної конкуренції та гібридних конфліктів. Багато держав, зіткнувшись із зовнішніми інформаційними загрозами, виробили власні стратегії реагування на дезінформацію, пропаганду, кібератаки та маніпуляції у цифровому середовищі. Аналіз міжнародного досвіду у цій сфері є надзвичайно важливим для України, яка перебуває на передовій інформаційного фронту в умовах повномасштабної агресії Російської Федерації.

Однією з найпоширеніших практик західних країн є створення спеціалізованих інституцій, які займаються виявленням і протидією дезінформаційним кампаніям. Наприклад, у 2015 році в Європейському Союзі було створено підрозділ East StratCom Task Force при Європейській службі зовнішньої дії (EEAS), головним завданням якого стало моніторинг і спростування дезінформаційних наративів, насамперед пов’язаних з російською пропагандою. Цей підрозділ щотижнево публікує аналітику про фейки, маніпуляції та

інформаційні атаки, а також співпрацює з аналітичними центрами, журналістами та урядами країн-членів ЄС [230].

У США боротьба з інформаційними загрозами набуває міжвідомчого характеру. Зокрема, Міністерство внутрішньої безпеки США (DHS) у співпраці з Федеральним бюро розслідувань та Міністерством оборони координує зусилля щодо кіберзахисту, виявлення впливу іноземних держав на внутрішню політику через цифрові платформи, зокрема під час виборів. На додаток, у 2021 році було запущено програму щодо покращення медіаграмотності серед громадян, а також розширено співпрацю з провідними технологічними компаніями з метою обмеження поширення фейкової інформації [30].

Країни Балтії, особливо Литва, Латвія та Естонія, завдяки історичному досвіду радянської окупації та геополітичній близькості до Росії, активно впроваджують законодавчі та комунікаційні інструменти протидії пропаганді. У Литві діє Центр стратегічних комунікацій при Міністерстві оборони, який системно аналізує наративи російських ЗМІ, проводить просвітницькі кампанії та реалізує проєкти з підвищення стійкості суспільства до дезінформації. Латвія запровадила законодавчі обмеження на ретрансляцію російських телеканалів, а також активно залучає громадянське суспільство до верифікації фактів.

Ефективним елементом міжнародного досвіду є інтеграція державних структур із незалежними фактчекінговими платформами. Наприклад, у Швеції за підтримки уряду діє кампанія «Психологічний захист» (Myndigheten för psykologiskt försvar), яка спрямована на підвищення критичного мислення, виявлення інформаційних впливів та навчання громадян розпізнавати спроби маніпуляцій. У межах цієї кампанії уряд Швеції тісно співпрацює з освітніми установами, громадськими організаціями та ЗМІ.

Канада, як одна з країн, що активно підтримує Україну, зосереджує увагу на інформаційній безпеці в контексті кіберзагроз та впливу іноземних акторів на внутрішній політичний порядок. У 2019 році канадський уряд створив програму

"Critical Election Incident Public Protocol", яка дозволяє оперативно реагувати на спроби втручання у виборчі процеси. Також, у межах міжнародної співпраці Канада підтримує українські інституції у сфері цифрової безпеки та медіаграмотності.

У межах НАТО діє Центр передового досвіду зі стратегічних комунікацій у Ризі (NATO StratCom COE), який розробляє методології аналізу інформаційних кампаній, проводить тренінги для фахівців країн-членів та публікує регулярні звіти щодо новітніх форм інформаційного впливу. Україна, маючи статус партнера НАТО, активно співпрацює з цим Центром, що дозволяє адаптувати євроатлантичні практики до національного контексту [38].

Особливої уваги заслуговує досвід Фінляндії, яка зробила медіаосвіту частиною національної політики ще на початку 2000-х років. У країні впроваджено міждисциплінарні програми з критичного мислення для школярів та студентів, організовано державну підтримку незалежних медіа, а також забезпечено правове регулювання протидії зовнішнім впливам на інформаційне середовище. Цей досвід визнається одним з найуспішніших у світі, оскільки поєднує системну державну політику з активною участю громадянського суспільства.

Україна, враховуючи зазначені приклади, поступово імплементує кращі міжнародні практики у сфері боротьби з дезінформацією. Зокрема, одним із кроків стало створення Центру протидії дезінформації при Раді національної безпеки і оборони України, який займається моніторингом, аналізом та оперативним інформуванням про загрози у сфері комунікації. Окрім того, активно розвиваються партнерства з міжнародними фактчекінговими організаціями, такими як StopFake, Bellingcat, EU DisinfoLab та інші.

Інший важливий напрям — розвиток медіаграмотності, який підтримується міжнародними донорами та інституціями, зокрема Посольством Великої Британії в Україні, Представництвом ЄС, Internews та Deutsche Welle Akademie. Ці організації реалізують проєкти, що охоплюють навчання вчителів, підготовку підручників, створення інтерактивних платформ для молоді та журналістів.

Не менш важливою є співпраця України з міжнародними інституціями, зокрема ОБСЄ, яка постійно моніторить ситуацію у сфері свободи медіа та реагує на загрози інформаційного характеру. Крім того, Україна є учасником Глобального форуму з кіберекономіки та інформаційної безпеки (GFCIS), де обговорюються виклики цифрової епохи та виробляються спільні рекомендації.

Успішна реалізація міжнародного досвіду вимагає не лише нормативної адаптації, але й внутрішньої політичної волі, інституційної спроможності та підтримки громадянського суспільства. Важливим фактором залишається прозорість комунікації держави з суспільством, а також забезпечення доступу до правдивої, перевіреної інформації у кризові моменти.

Досвід країн Європейського Союзу, США, Канади, Ізраїлю та Балтійського регіону у сфері боротьби з інформаційними війнами демонструє важливість комплексного підходу, що поєднує державну стратегію, розвиток медіаосвіти, підтримку незалежних ЗМІ та активну взаємодію з громадянським суспільством. Одним із найбільш ефективних прикладів є діяльність Європейської служби зовнішніх дій (EEAS), зокрема її підрозділу East StratCom Task Force, що здійснює моніторинг дезінформаційних наративів і веде портал EUvsDisinfo. Цей приклад демонструє доцільність створення подібної структури в Україні з розширеними аналітичними й комунікаційними повноваженнями, інтегрованої до системи національної безпеки [35].

Для України доцільно адаптувати кращі міжнародні практики, враховуючи особливості власного інформаційного середовища. Зокрема, ефективним є досвід Фінляндії щодо інтеграції курсів з медіаграмотності до шкільної освіти, що в перспективі сприяє формуванню суспільства, стійкого до впливу фейків та маніпуляцій. Крім того, позитивний приклад Естонії у створенні державного кіберцентру, що забезпечує захист критичної інформаційної інфраструктури, може стати моделлю для посилення українських спроможностей у сфері кіберзахисту. Варто також активізувати участь України у міжнародних ініціативах, спрямованих

на боротьбу з дезінформацією, зокрема шляхом розширення співпраці з НАТО, ЄС та Глобальною коаліцією з протидії інформаційним загрозам [35].

Підсумовуючи викладене, міжнародна практика боротьби з інформаційними загрозами свідчить про необхідність комплексного підходу, що поєднує технічні, правові, освітні та комунікаційні інструменти. Ефективна модель інформаційної безпеки повинна включати не лише захист інформаційного простору, а й формування критично мислячого громадянина, який здатен розпізнати маніпуляцію та протистояти інформаційній агресії. Для України, яка є мішенню постійних інформаційних атак, запозичення та адаптація міжнародного досвіду має стати одним із ключових векторів державної політики у сфері національної безпеки.

Тому, державна політика України в сфері інформаційної безпеки та протидії інформаційним загрозам є ключовим елементом національної безпеки країни в умовах сучасних гібридних загроз. Вона охоплює широкий спектр заходів, що включають правові, технічні, інформаційно-просвітницькі та міжнародні стратегії для забезпечення стійкості інформаційного простору. Створення відповідної інфраструктури для боротьби з дезінформацією та інформаційними атаками є необхідним для збереження суверенітету, а також для запобігання підриву національної єдності та безпеки.

Особливу роль у протидії інформаційним загрозам відіграють громадянське суспільство та незалежні медіа. Вони не тільки активно реагують на поточні загрози, але й формують довгострокову стратегію інформаційної безпеки, сприяючи розвитку критичного мислення та медіаграмотності серед громадян. Завдяки таким організаціям формується здатність суспільства протистояти маніпуляціям, фальсифікаціям та дезінформації.

Міжнародний досвід боротьби з інформаційними загрозами підтверджує необхідність комплексного підходу, що включає законодавчі, технічні, освітні та комунікаційні інструменти. Для України важливо адаптувати ці моделі до специфічних умов, враховуючи поточний воєнний стан та геополітичні реалії.

Запозичення успішних практик міжнародних партнерів, інтеграція з міжнародними структурами та постійна адаптація національної політики є важливими складовими ефективної протидії інформаційним загрозам.

Таким чином, забезпечення інформаційної безпеки вимагає постійної координації зусиль між державними органами, громадянським суспільством, медіа та міжнародними партнерами. Тільки так можна сформувати стійкий, ефективний механізм протидії зовнішнім і внутрішнім інформаційним атакам, що забезпечить надійний захист національних інтересів України.

ВИСНОВКИ

У результаті проведеного комплексного дослідження встановлено, що інформаційна війна є не лише похідною сучасних технологій чи окремою формою конфлікту, а системним і стратегічним викликом для національної безпеки, що пронизує політичну, соціальну, економічну, культурну та військову сфери. Поняття інформаційної війни, окреслене у першому розділі роботи, підтвердило свою міждисциплінарну природу, оскільки поєднує в собі інструменти психологічного впливу, технології маніпулювання свідомістю, дезінформаційні кампанії, кібератаки та пропаганду. Її ключовими характеристиками є невидимість, швидкість розповсюдження, здатність викривляти реальність і трансформувати систему сприйняття соціальних та політичних явищ у масовій свідомості.

Розкриття інструментарію ведення інформаційної війни продемонструвало, що сучасні агресивні практики використовують широке коло платформ: від класичних мас-медіа до соціальних мереж, а також алгоритмізованих систем, бот-мереж, технологій deepfake і штучного інтелекту. Особливу небезпеку становить гібридна взаємодія цих засобів, яка дозволяє агресору водночас проникати у приватний, суспільний та державний виміри. Ці методи спрямовані на створення постправди, деморалізацію громадян, делегітимацію державної влади, ослаблення довіри до інститутів та стимулювання внутрішніх конфліктів. Такий підхід дозволяє супротивнику досягати стратегічних цілей без відкритого військового втручання, водночас створюючи умови для політичної дестабілізації та втрати державної суб’єктності.

У другому розділі було здійснено системну класифікацію основних інформаційних атак на Україну з 2014 року. Проаналізовані приклади — анексія Криму, вторгнення на Донбас, інформаційне супроводження повномасштабної війни з 2022 року — засвідчили, що РФ реалізує довгострокову, багаторівневу стратегію підриву України як держави. Інформаційні кампанії Росії поєднують такі

ключові елементи, як нав'язування альтернативного порядку денного, імітація внутрішнього розколу в українському суспільстві, делегітимація міжнародної підтримки України, маніпулювання темами національної ідентичності, мови, історичної пам'яті. Основними платформами для реалізації ворожих наративів виступають телеканали, Telegram-канали, YouTube, TikTok, месенджери, а також дезінформаційні сайти, що видають себе за локальні українські медіа.

Аналіз механізмів поширення дезінформації дозволив ідентифікувати чіткі технологічні й організаційні моделі її функціонування. Йдеться про централізоване планування кампаній з боку державних структур РФ, їх подальшу реалізацію через мережі псевдомедіа, а також поширення через органічний та платний контент у соціальних мережах. Маніпулятивні матеріали часто маскуються під новини, експертні думки або позиції «незалежних журналістів», що істотно ускладнює процес їх викриття. Інформаційне середовище України характеризується високим ступенем фрагментації, що у поєднанні з низьким рівнем медіаграмотності окремих категорій громадян підвищує ефективність інформаційних атак.

Оцінка впливу російської пропаганди на суспільну думку в Україні засвідчила неоднорідність її наслідків. У регіонах, де переважає доступ до незалежних джерел, наявна критична медіаосвіта і розвинуте громадянське суспільство, вплив дезінформації мінімальний. Натомість у середовищах з обмеженим доступом до перевірених ЗМІ, високою емоційною напругою та інформаційною втомою, сприйняття ворожих наративів значно вище. У цьому контексті особливо важливою є підтримка фактчекінгових ініціатив, просвітницьких кампаній та інформаційних проєктів, орієнтованих на формування культури критичного мислення. Такий підхід не лише знижує ефективність пропаганди, а й формує довгострокову стійкість до маніпулятивного впливу.

Третій розділ кваліфікаційної роботи дозволив оцінити політичні, інституційні та громадські механізми протидії інформаційній війні. Увагу було зосереджено на державній політиці, яка реалізується через Стратегію

інформаційної безпеки, діяльність Центру протидії дезінформації, Національної ради з питань телебачення і радіомовлення, МКІП та інших структур. Встановлено, що, попри помітні зрушення у напрямі консолідації державної політики у сфері інформаційної безпеки, система протидії залишається фрагментарною та залежною від зовнішньої підтримки. Основними проблемами є брак сталої координації між органами влади, нестача технічних і людських ресурсів, а також затримка у впровадженні сучасних цифрових інструментів.

Особливу роль у забезпеченні інформаційної безпеки відіграють незалежні ЗМІ, фактчекінгові ініціативи (StopFake, VoxCheck, Detector Media), освітні проєкти (IREX, «Фільтр», Internews) та інші неурядові організації, які в умовах обмежених ресурсів ефективно заповнюють прогалини в державній системі реагування. Встановлено, що діяльність цих структур сприяє підвищенню рівня довіри громадян до об'єктивної інформації, проте вони потребують інституційної підтримки, зокрема фінансової стабільності, юридичних гарантій і розширення повноважень щодо співпраці з державою.

Досвід зарубіжних країн, проаналізований у межах дослідження, дозволив виділити низку практик, які можуть бути ефективно адаптовані в Україні. Йдеться про централізовану інформаційну координацію (Фінляндія, Литва), інтеграцію медіаосвіти в шкільну програму (Фінляндія, США), законодавче обмеження ворожого контенту (Латвія, Естонія), а також розвиток національних стратегічних комунікацій (Велика Британія, НАТО StratCom). Україна вже почала застосовувати частину з цих підходів, однак для досягнення системної ефективності необхідна міжгалузева узгодженість, оновлення нормативної бази, а також укріплення міжнародного партнерства.

Таким чином, результати дослідження підтвердили гіпотезу про те, що в умовах сучасної повномасштабної війни інформаційна безпека є критичним елементом національної безпеки. Ефективна протидія інформаційній агресії передбачає не лише оборонну політику, а й проактивну позицію держави,

суспільства та медіаінституцій. Формування інформаційної стійкості громадян, інституційна координація, цифровізація засобів реагування, розвиток медіаосвіти та міжнародна інтеграція є ключовими векторами, здатними забезпечити довгострокову безпеку держави у сфері інформації. Розроблені у роботі висновки й рекомендації можуть бути використані для вдосконалення національної політики, освітніх програм і стратегічних комунікацій, що є необхідною передумовою збереження суверенітету та стійкості демократичного устрою України в умовах інформаційного тиску.

СПИСОК ВИКОРИСТАНИХ ДЖЕРЕЛ І ЛІТЕРАТУРИ

1. Варга Т. М. Дезінформація та пропаганда як інструменти ведення гібридної війни росії проти України. *Аналітично-порівняльне правознавство*. 2024. №6. С. 526-531

2. Виговська О., Бєлоусова Н. Інформаційна складова національної безпеки України. 2017. 168 с.

3. Війна і фейки: як Росія веде інформаційну війну проти України. URL: https://texty.org.ua (дата звернення 29.04.2025)

4. Горбань Ю.О. Інформаційна війна проти України та засоби її ведення. *Вісник Національної академії державного управління при Президентові України*. 2015. № 1. С. 136–141.

5. Гріцак Я. Подолати минуле: глобальна історія України. Київ : Yakaboo Publishing, 2022. 448 с.

6. Зінченко М.О., Плугова О.Б, Драглюк О.В. Інформаційна війна, засоби реалізації та протидії. *Інформаційний вимір гібридної війни*: досвід України: матеріали міжнародної науково-практичної конференції. Київ : НУОУ, 2017. С. 38–40.

7. Золотухін Д. Протидія інформаційній агресії Росії на рівні законодавчих актів: Резолюція Європарламенту. URL: http://bit.ly/2mVqxzW (дата звернення 18.04.2025)

8. Кабінет Міністрів України. Розпорядження №272-р «Про затвердження плану заходів з реалізації Стратегії інформаційної безпеки України на період до 2025 року», 2023. URL: https://zakon.rada.gov.ua/go/272-2023-р (дата звернення 17.04.2025)

9. Карлова В. В. Вплив засобів масової інформації на формування української національної свідомості. *Державне управління: теорія та практика*. 2007. № 2 (6). URL: http://academy.gov.ua/ej/ej6/txts/07kvvunc.htm

10. Концепція національної безпеки України : Указ Президента України від 26 травня 2015 р. № 287/2015, URL: https://zakon.rada.gov.ua/laws/show/287/2015 (дата звернення 08.04.2025)

11. Малик Я. Й. Інформаційна війна і Україна. *Демократичне врядування*. 2015. Вип. 15. С. 45–49.

12. Маляр Г.: Перше правило інформаційної безпеки під час війни - не вір джерелам інформації ворога. URL: https://www.kmu.gov.ua/news/gannamalyar-pershe-pravilo-informacijnoyi-bezpeki-pid-chas-vijni-ne-vir-dzherelaminformaciyi-voroga. (дата звернення 06.03.2025)

13. Мельник Д.С. Актуальні загрози національній безпеці України в інформаційній сфері: питання визначення та протидії. *Інформаційна безпека людини, суспільства, держави*. 2021. № 1–3 (31–33). С. 16-27.

14. Міжнародний досвід протидії гібридним загрозам: законодавче регулювання та організації з питань стратегічних комунікацій. URL: http://euinfocenter.rada.gov.ua/uploads/documents/29377.pdf (дата звернення 30.04.2025)

15. Пархоменко-Куцевіл О. Проблеми забезпечення національної безпеки в умовах воєнного часу. *Науковий вісник Вінницької академії безперервної освіти. Серія «Екологія. Публічне управління та адміністрування»*. 2023. Вип. 3. С. 143–150.

16. Президент України. Указ №685/2021 «Про Стратегію інформаційної безпеки України», 2021. URL: https://www.president.gov.ua/documents/6852021-41069 (дата звернення 20.04.2025)

17. Російське іномовлення як інструмент маніпулювання громадською думкою у трансатлантичному просторі. НІСД. URL: http://www.niss.gov.ua/articles/1834/

18. Світова гібридна війна: український фронт / за ред. В. П. Горбуліна. URL: http://www.niss.gov.ua/articles/2431/

19. Сунь-цзи. Мистецтво війни., пер. з кит. В. М. Шекера., вступ. ст., комент. та ред. С. Капранова., Київ : Знання, 2017., 192 с.

20. Ткаченко, В. В., Паливода, В. В. Загрози інформаційній безпеці України як проблематика національної безпеки. *Юридичний науковий електронний журнал*. 2022. №10. С. 496–498.

21. Український кризовий медіа-центр. Війна і дезінформація. URL: https://uacrisis.org/uk/ (дата звернення 20.03.2025)

22. Центр демократії та верховенства права. Медіаграмотність та спротив дезінформації в Україні, 2023. URL: https://cedem.org.ua (дата звернення 11.04.2025)

23. Центр протидії дезінформації при РНБО України. Аналітика і звіти. URL: https://cpd.gov.ua (дата звернення 06.03.2025)

24. Центр стратегічних комунікацій та інформаційної безпеки. Як захищати себе від інформаційної агресії. Аналітична доповідь., Київ, 2022. URL: https://spravdi.gov.ua (дата звернення 06.04.2025)

25. Detector Media. Аналітика дезінформації в українському медіапросторі, 2024. URL: https://detector.media/infospace/article/230408/2024-08-02-z-pochatkom-velykoi-viyny-ukrainski-media-zaynyalysya-temoyu-mediagramotnosti-ta-protydii-dezinformatsii-analityka-uimk/ (дата звернення 15.04.2025)

26. DW Akademie. Media Development Projects in Ukraine, 2023. URL: https://akademie.dw.com/ru/dw-akademie-v-ukraine/a-68419550 (дата звернення 17.04.2025)

27. EUvsDisinfo. Disinformation Cases Database, 2024. URL: https://euvsdisinfo.eu/disinformation-is-not-potatoes/ (дата звернення 27.04.2025)

28. EUvsDisinfo. Fighting disinformation. URL: https://euvsdisinfo.eu/fighting-the-disinformation-virus-georgia-edition/ (дата звернення 27.04.20250

29. EUvsDisinfo. Russian Disinformation Tactics. – European External Action Service, 2024. URL: https://euvsdisinfo.eu/kremlin-disinformation-attacking-the-legitimacy-of-ukrainian-authorities/ (дата звернення 27.04.2025)

30. Gavryliuk A. I. Інформаційна безпека держави в умовах гібридних загроз : монографія. Київ : НАДУ, 2021. 240 с.

31. International Fact-Checking Network (IFCN). Verified Signatories & Principles, 2023. URL: https://ifcncodeofprinciples.poynter.org (дата звернення 18.04.2025)

32. Internews Ukraine. Програми медіаграмотності та підтримки незалежних медіа, 2023. URL: https://internews.ua (дата звернення 10.04.2025)

33. IREX. Проєкт “Вивчай та розрізняй: інфо-медійна грамотність”, 2023. URL: https://academia.vinnica.ua/index.php/uk/news/1121-uprovadzhennya-proektu-irex-vivchaj-ta-rozriznyaj-info-medijna-gramotnist-v-osvitnij-protses-profesijnogo-rozvitku-vchiteliv-slovesnosti-v-sistemi-pislyadiplomnoji-pedagogichnoji-osviti (дата звернення 01.05.2025)

34. NATO Cooperative Cyber Defence Centre of Excellence. About, URL: https://ccdcoe.org (дата звернення 05.04.2025)

35. Pomerantsev, P. This is Not Propaganda: Adventures in the War Against Reality. London : Faber & Faber, 2019. – 256 p.

36. Reuters Institute for the Study of Journalism. Digital News Report 2023: Ukraine URL: https://reutersinstitute.politics.ox.ac.uk/digital-news-report/2023 (дата звернення 26.04.2025)

37. Shekhovtsov A. Russian influence operations in the West: assessing propaganda and disinformation. London : Routledge, 2020. 198 p.

38. StopFake. Аналітичні звіти про російську дезінформацію, URL: https://www.stopfake.org/uk/category/doslidzhennya/ (дата зверненя 18.04.2025)

39. StopFake. Щотижневі огляди дезінформації, 2024. URL: https://www.stopfake.org/uk/golovna/ (дата звернення 30.04.2025)

40. Texty.org.ua. Бази фейків і бот-мереж, 2023. URL: https://texty.org.ua/articles/113512/shcho-rozpoviv-ahent-fbr-pro-rosiysku-dezinformatsiyu-v-ssha/ (дата звернення 07.04.2025)

41. Texty.org.ua. Війна і фейки: як Росія веде інформаційну війну проти України, 2023. URL: https://texty.org.ua/fragments/112415/rosiya-vyhraye-hlobalnu-informacijnu-vijnu-rusi/ (дата зверненн 01.04.2025)

42. VoxCheck. Моніторинг заяв українських політиків та медіа URL: https://voxukraine.org/stali-naratyvy-minlyvi-fejky-doslidzhennya-voxcheck-pro-rosijsku-brehnyu-v-yevropi (дата звернення 30.04.2025)