

Міністерство освіти і науки України
Національний університет «Острозька академія»
Навчально-науковий інститут міжнародних відносин та національної безпеки
Кафедра міжнародних відносин

Кваліфікаційна робота
на здобуття освітнього ступеня магістр

на тему: «Основні інструменти інформаційної війни рф в Україні у період
повномасштабної війни»

Виконала студентка 2 курсу, групи ММВ-21 спеціальності 291
«Міжнародні відносини, суспільні комунікації та регіональні студії»,
освітньо-професійної програми
«Міжнародні відносини»
Митюк Анастасія Вадимівна

Науковий керівник: Близняк Ольга Анатоліївна
кандидат політичних наук, старший викладач
Рецензент: Шаправський Сергій Анатолійович
кандидат історичних наук

Робота допущена до захисту
(протокол №____ засідання кафедри
міжнародних відносин

від_____20__року

Завідувач кафедри міжнародних відносин:

Острог – 2025

ЗМІСТ

ВСТУП.....	3
РОЗДІЛ 1. ТЕОРЕТИКО-МЕТОДОЛОГІЧНІ ЗАСАДИ ДОСЛІДЖЕННЯ ІНФОРМАЦІЙНОЇ ВІЙНИ	9
1.1.Поняття та ознаки інформаційної війни	9
1.2. Теоретичні підходи до класифікації інструментів інформаційної війни	16
1.3. Світовий досвід ведення інформаційних війн у XX–XXI століттях	25
Висновки до розділу 1.....	31
РОЗДІЛ 2. ІНФОРМАЦІЙНА ВІЙНА РФ ПРОТИ УКРАЇНИ ЕТАПИ ТА ОСОБЛИВОСТІ У ПЕРІОД ПОВНОМАСШТАБНОГО ВТОРГНЕННЯ	33
2.1. Основні характеристики інформаційної війни РФ в просторі України	33
2.2. Основні цілі та наративи російської пропаганди у період повномасштабного вторгнення	42
2.3. Пропагандистські платформи РФ та їх вплив на інформаційний український простір.....	49
Висновки до розділу 2.....	53
РОЗДІЛ 3. ПЕРСПЕКТИВИ ВПРОВАДЖЕННЯ РЕКОМЕНДАЦІЙ ЩОДО ІНСТРУМЕНТІВ ІНФОРМАЦІЙНОЇ ВІЙНИ РФ В УКРАЇНІ.....	54
3.1. Інформаційно-психологічні та кібероперації як інструменти стратегічного впливу російської федерації	54
3.2. Вплив російських інформаційних атак у соціальних мережах та шляхи їхньої нейтралізації	60
3.3. Перспективи формування цифрової оборони в Україні: стратегічні пріоритети та безпекові виклики.....	68
Висновки до розділу 3.....	76
ВИСНОВКИ	78
СПИСОК ВИКОРИСТАНОЇ ЛІТЕРАТУРИ.....	82

Актуальність теми дослідження зумовлена трансформацією міждержавних конфліктів у межах якої інформаційний компонент стає стратегічним ресурсом, співмірним із військовою силою. російська федерація з 24 лютого 2022 року реалізує масштабну інформаційно-психологічну операцію проти України. За даними Центру протидії дезінформації РНБО, щомісяця фіксується понад 300 тисяч випадків поширення фейків. Науково-практичне значення обраної проблематики визначається необхідністю формування ефективної системи національної інформаційної безпеки в умовах, коли традиційні моделі протидії пропаганді виявляються недостатніми перед обличчям технологічно вдосконалених методів маніпулювання громадською думкою.

Досвід України у протистоянні російській інформаційній агресії становить унікальний емпіричний матеріал для теоретичного узагальнення, оскільки країна фактично виступає полігоном випробування новітніх технологій когнітивної війни. Відтак дослідження інформаційної війни російської федерації набуває як академічної цінності, так і прикладного значення для вдосконалення державної політики у сфері стратегічних комунікацій, медіаграмотності населення та міжнародної координації зусиль із протидії авторитарній дезінформації.

Стан наукової розробки проблематики. Збройна агресія російської федерації проти України, що розпочалася 24 лютого 2022 року, стала одним із найбільших викликів для системи міжнародної безпеки у XXI столітті. Поряд із безпосередніми бойовими діями світ став свідком масштабної інформаційної війни, що охопила глобальний інформаційний простір. О. А. Близняк та К. М. Гуменна справедливо зазначають, що інструменти інформаційної війни росії проти України під час повномасштабного вторгнення 2022-2025 років набули принципово нового характеру, поєднуючи традиційні пропагандистські методи з новітніми технологіями дезінформації [4].

Інформаційний вимір збройного протистояння став невід’ємною складовою гібридної стратегії агресора, спрямованої на підрив обороноздатності України та руйнування міжнародної підтримки нашої держави. Актуальність зумовлена тим, що інформаційні операції стали ключовим елементом сучасних збройних конфліктів. Г. Гребньов підкреслює системний характер застосування дезінформації, маніпуляцій та психологічного тиску для досягнення стратегічних цілей агресора [12]. В. В. Белімов з колегами фіксують постійну еволюцію методів інформаційного впливу за період із жовтня по грудень 2023 року [45]. І. П. Шевель відзначає, що інформаційний компонент конфлікту став інструментом впливу на міжнародну спільноту та формування образу України на глобальній арені [51].

Наукова розробленість проблематики активно розвивається останніми роками. В. І. Старжець з колегами досліджують основні тренди інформаційної кампанії російської федерації на початку 2023 року [41]. О. Фролова та А. Дарницький аналізують інформаційно-психологічні загрози, акцентуючи увагу на механізмах впливу на свідомість громадян [54]. В. В. Макарчук розглядають інформаційні операції як інструмент економічної дестабілізації [32]. Г. П. Зірчак розкриває системний характер інформаційного складника гібридної війни [17]. Теоретико-методологічні засади дослідження базуються на міждисциплінарному підході. В. О. Шведун пропонує комплексний підхід до протидії інформаційним загрозам [49]. О. М. Венгер виявляє механізми маніпулятивного впливу на суспільну думку [6]. О. Карпенко, О. Свйонтик та Р. Терещенко систематизують наукові напрацювання у цій галузі [21]. О. О. Гордійчук показує еволюцію форм збройного протистояння [11]. А. С. Волох демонструє широкий спектр наслідків інформаційних операцій для різних сфер суспільного життя [8].

Метою дослідження є всебічне дослідження основних інструментів інформаційної війни, які використовує російська федерація проти України у період повномасштабної агресії (2022–2025 рр.), для виявлення їх впливу на політичну свідомість громадян та інформаційний простір держави. Досягнення

поставленої мети зумовлює необхідність виконати наступні **завдання дослідження:**

1. Розкрити теоретико-методологічні засади дослідження інформаційної війни, визначити поняття, ознаки та систематизувати класифікації інструментів інформаційного протиборства.

2. Проаналізувати світовий досвід ведення інформаційних війн у ХХ–ХХІ століттях з акцентом на механізми дезінформації та пропаганди. 3. Дослідити стратегію, етапи та основні інструменти інформаційної війни РФ проти України в умовах повномасштабного вторгнення. 4. Обґрунтувати напрями та перспективи розбудови системи цифрової оборони України в контексті протидії гібридній агресії. **Об’єктом дослідження** виступає інформаційна політика російської федерації в контексті гібридної війни проти України у період повномасштабного вторгнення.

Предметом дослідження є структура, зміст, форми та засоби інформаційного впливу росії, зокрема механізми дезінформації, пропаганди, когнітивних операцій, кібератак та інших інструментів, спрямованих на маніпуляцію громадською думкою, підрив державної стабільності та дискредитацію України на міжнародному рівні.

Методологія дослідження ґрунтується на міждисциплінарному підході, що поєднує знання соціальних комунікацій, політології, безпекознавства та інформаційних технологій. Теоретико-методологічною основою стали концепції інформаційної війни, гібридних конфліктів та праці провідних науковців у галузі дослідження пропаганди й дезінформації. Системний підхід дозволив розглядати інформаційну війну як цілісне явище з елементами стратегічного планування, засобами комунікаційного впливу та цільовими аудиторіями. Структурно-функціональний підхід застосовано для аналізу медіаплатформ, наративів та інструментів впливу.

Порівняльно-історичний метод використано для аналізу етапів розвитку

інформаційних війн у світі та виявлення специфіки російсько-українського протистояння. Метод періодизації дозволив виокремити основні етапи російської інформаційної агресії проти України. Метод систематизації та узагальнення застосовувався для класифікації інструментів інформаційної війни за технологічним, функціональним, структурним та психологічним критеріями. Описово-аналітичний метод використано для характеристики механізмів функціонування російських пропагандистських платформ, виявлення цілей і наративів російської пропаганди. Метод аналізу документів дозволив опрацювати стратегічні документи у сфері національної безпеки, звіти міжнародних організацій, наукові публікації та матеріали фактчекінгових організацій. Метод синтезу забезпечив формулювання практичних рекомендацій щодо зміцнення цифрової оборони України та протидії російським інформаційним загрозам.

Джерельна база дослідження спирається на актуальні наукові праці, присвячені аналізу інструментів і методів інформаційної війни російської федерації в контексті повномасштабної агресії проти України. Вивчення питання ґрунтується на міждисциплінарному підході, що охоплює політологічний, інформаційний, безпековий та соціально-психологічний виміри. О. А. Близняк та К. М. Гуменна у статті «Інструменти інформаційної війни росії проти України під час повномасштабного вторгнення 2022–2024 рр.» досліджують стратегічні напрямки інформаційної агресії, зокрема поширення дезінформації та використання цифрових інструментів впливу.

О. О. Гордійчук аналізує взаємозв'язок інформаційної, гібридної та конвенційної війни, характеризуючи механізми адаптації російської інформаційної тактики. Г. Гребньов акцентує на значенні пропагандистських наративів та соціотехнічних маніпуляцій як способів дестабілізації українського суспільства. О. Маслій та А. Буряк аналізують трансформацію загроз економічній і інформаційній безпеці України у воєнних умовах, що

дозволяє оцінити інформаційну війну як складову комплексного впливу на

стратегічну стабільність держави. О. А. Близняк та К. М. Гуменна у праці «Український досвід протидії інформаційній війні РФ» розкривають особливості державного і громадянського спротиву, акцентуючи на практиках виявлення та нейтралізації ворожих операцій. О. М. Венгер розглядає вплив інформаційної війни на трансформацію політичної свідомості населення України. Сукупність зазначених джерел становить комплексну наукову основу для системного аналізу інформаційної війни як інструменту гібридної агресії, її механізмів, масштабів та наслідків для українського суспільства.

Практичне значення дослідження полягає у формуванні науково обґрунтованої основи для розробки ефективних стратегій протидії інформаційній війні російської федерації проти України в умовах повномасштабного вторгнення 2022–2025 років. Аналіз сучасних інструментів інформаційного впливу, засобів дезінформації та методів когнітивного тиску дозволяє впроваджувати механізми інформаційного захисту на державному, громадському та інституційному рівнях. Результати дослідження сприятимуть вдосконаленню системи національної безпеки України у сфері інформаційної та кібербезпеки. Вони можуть бути застосовані державними органами, що займаються комунікаційною політикою, інформаційною безпекою та національною обороною. Дослідження має цінність для фахівців у сфері медіа, журналістики та цифрових технологій, які можуть використовувати його напрацювання для ідентифікації фейків, протидії пропаганді та попередження впливу деструктивних наративів на громадську думку.

Наукова новизна полягає в комплексному міждисциплінарному аналізі феномену інформаційної війни російської федерації проти України в умовах повномасштабної збройної агресії, здійсненому з позицій сучасних підходів до вивчення гібридних конфліктів та безпекових студій. Обґрунтовано теоретико-методологічні засади дослідження інформаційної війни як явища, що поєднує інструменти інформаційного, психологічного та кібернетичного

впливу для досягнення стратегічних геополітичних цілей агресора.

Конкретизовано класифікацію інструментів інформаційної агресії з урахуванням розвитку цифрових технологій та соціальних медіа. Систематизовано основні пропагандистські платформи російської федерації та проаналізовано їхній вплив на інформаційний простір України.

Структура роботи. Кваліфікаційна робота складається зі вступу, трьох розділів, висновків та списку використаної літератури. У першому розділі розглянуто теоретико-методологічні засади дослідження інформаційної війни, визначено поняття, ознаки та систематизовано класифікації інструментів інформаційного протиборства, проаналізовано світовий досвід ведення інформаційних війн у XX–XXI століттях. Другий розділ присвячено аналізу інформаційної війни російської федерації проти України в умовах повномасштабного вторгнення, її етапам, основним характеристикам, цілям і пропагандистським наративам. У третьому розділі досліджено інформаційно психологічні та кібероперації як інструменти стратегічного впливу, проаналізовано вплив російських інформаційних атак у соціальних мережах, визначено перспективи формування цифрової оборони України. Загальний обсяг роботи становить 92 сторінки, з них основного тексту – 79 сторінок. Список використаної літератури налічує 76 джерел.

9

РОЗДІЛ 1. ТЕОРЕТИКО-МЕТОДОЛОГІЧНІ ЗАСАДИ ДОСЛІДЖЕННЯ ІНФОРМАЦІЙНОЇ ВІЙНИ

1.1. Поняття та ознаки інформаційної війни

Сучасні збройні конфлікти дедалі більше характеризуються активним використанням інформаційних технологій як інструменту досягнення стратегічних цілей. Повномасштабна збройна агресія російської федерації проти України засвідчила трансформацію традиційних форм ведення війни, де інформаційний простір став таким самим полем бою, як і фізична територія держави. Якщо раніше військові операції переважно обмежувалися фізичним знищенням противника та захопленням територій, то сьогодні вони невід’ємно

супроводжуються масовими інформаційними атаками, спрямованими на свідомість як безпосередніх учасників конфлікту, так і цивільного населення. У зв'язку з цим актуалізується необхідність теоретичного осмислення феномену інформаційної війни, визначення її сутнісних характеристик та особливостей прояву в умовах сучасних гібридних конфліктів.

Розуміння природи інформаційної війни є важливим для розробки ефективних механізмів протидії інформаційним загрозам та забезпечення національної безпеки держави в інформаційній сфері. Дослідження інформаційної війни потребує насамперед чіткого понятійного апарату, оскільки термінологічна невизначеність унеможливорює адекватний аналіз явища та розробку практичних рекомендацій щодо протидії інформаційним загрозам. У науковій літературі спостерігається множинність підходів до визначення змісту цього явища, що зумовлено міждисциплінарним характером проблематики та динамічним розвитком інформаційних технологій. О. А. Близняк та К. М. Гуменна визначають інформаційну війну як комплексну систему заходів, спрямованих на досягнення інформаційної переваги шляхом впливу на інформаційні системи противника при одночасному захисті власних інформаційних ресурсів [4]. Таке розуміння акцентує увагу на двосторонньому

10

характері інформаційного протиборства, де важливими є як наступальні, так і оборонні дії. Автори підкреслюють, що інформаційна війна охоплює широкий спектр дій: від технічних кібератак на критичну інфраструктуру до психологічних операцій, спрямованих на деморалізацію населення та підрив довіри до органів державної влади.

Важливим є те, що інформаційна війна передбачає систематичний та скоординований характер дій, а не окремі епізодичні заходи інформаційного впливу. Г. Гребньов розглядає інформаційну війну як складову гібридної війни. Вчений наголошує, що інформаційна війна може розгортатися як у мирний час, так і супроводжувати традиційні військові дії, посилюючи їхню ефективність через психологічний вплив на противника. Зазначається, що інформаційна

складова гібридної війни часто випереджає фізичні військові дії, створюючи сприятливі умови для подальшої агресії шляхом формування відповідних суспільних настроїв, поширення паніки та дезінформації. Г. Гребньов також підкреслює, що інформаційна війна характеризується прихованістю джерел інформаційного впливу, використанням підставних осіб та організацій, створенням ілюзії спонтанних суспільних процесів там, де насправді відбувається керована ззовні маніпуляція. О. О. Гордійчук аналізує інформаційну війну російської федерації проти України через призму основних аспектів протистояння, виокремлюючи декілька етапів її розгортання [11]. Дослідниця стверджує, що інформаційна агресія російської федерації розпочалася задовго до повномасштабного вторгнення 2022 року та мала системний характер.

Вже з 2014 року спостерігалось масове поширення антиукраїнських наративів, спрямованих на делегітимізацію української державності, применшення української культурної ідентичності, створення образу України як неспроможної держави. О. О. Гордійчук детально описує еволюцію російських інформаційних стратегій: якщо на початковому етапі акцент робився на заперечення самого факту агресії та приписування відповідальності за конфлікт

11

українській стороні, то з часом риторика трансформувалася у відверте виправдання військових дій під приводом «денацифікації» та «демілітаризації». Науковиця наголошує, що інформаційна війна РФ характеризується багатоканальністю поширення дезінформації, використанням як традиційних медіа, так і соціальних мереж, блогосфери, месенджерів для охоплення максимально широкої аудиторії.

В. В. Белімов та його колектив у дослідженні хронік інформаційної війни за період з жовтня по грудень 2023 року систематизували основні інформаційні події та проаналізували динаміку інформаційного протиборства [45]. Науковці виявили, що інформаційна війна характеризується високою інтенсивністю та різноманітністю форм прояву. Зокрема, за досліджуваний період було

зафіксовано сотні випадків поширення фейкових новин, спрямованих на підрив міжнародної підтримки України, дискредитацію Збройних Сил України, провокування панічних настроїв серед цивільного населення. В. В. Белімов та співавтори звертають увагу на те, що російська інформаційна машина адаптується до контрзаходів української сторони, постійно змінюючи тактику, створюючи нові канали поширення дезінформації, використовуючи складніші технології маніпуляції, включаючи штучний інтелект для генерування фейкових зображень та відео. Вчені підкреслюють, що ефективна протидія інформаційній війні вимагає постійного моніторингу інформаційного простору, швидкого реагування на дезінформаційні кампанії та координації зусиль різних державних і недержавних акторів.

О. М. Венгер досліджує вплив інформаційної війни на формування політичної свідомості в умовах повномасштабної російсько-української війни [6]. У роботі аргументується, що інформаційна війна безпосередньо впливає на політичні орієнтації громадян, їхнє ставлення до влади, розуміння причин та перебігу конфлікту. Виокремлено декілька механізмів впливу інформаційної війни на політичну свідомість: по-перше, через створення альтернативної реальності, де факти замінюються вигаданими наративами; по-друге, через

12

емоційну маніпуляцію, що апелює до страхів, образ, історичних травм; по-третє, через підрив довіри до офіційних джерел інформації та створення атмосфери тотальної підозри. Підкреслюється, що особливо вразливими до інформаційних маніпуляцій є групи населення з низьким рівнем медіаграмотності, обмеженим доступом до альтернативних джерел інформації, а також особи похилого віку, які звикли довіряти телебаченню як основному джерелу новин. Звертається увага на те, що інформаційна війна має довгострокові наслідки для суспільної свідомості, оскільки навіть після спростування дезінформації залишаються психологічні сліди, що впливають на подальше сприйняття подій.

О. Маслій та А. Буряк [73] розглядають трансформацію загроз економічній безпеці та безпеці інформаційного середовища України в умовах

повномасштабної війни. Інформаційна війна стала невід'ємною складовою економічної агресії, оскільки спрямована на підриз довіри інвесторів, дестабілізацію фінансових ринків, створення панічних настроїв серед населення щодо економічних перспектив держави. У роботі детально описано, як російська пропаганда використовує економічну тематику для інформаційних атак: поширюються фейки про нібито неминучий дефолт України, колапс банківської системи, масове безробіття, голод. Такі інформаційні атаки мають конкретну мету – спровокувати панічний вивід коштів з банків, масовий продаж гривні, зупинку інвестиційних процесів. Дослідження доводить взаємозв'язок між безпекою інформаційного середовища та загальною національною безпекою: захист інформаційного простору є передумовою забезпечення економічної, політичної, військової безпеки держави. О. Маслій та А. Буряк обґрунтовують необхідність комплексного підходу до забезпечення інформаційної безпеки, що передбачає як технічні заходи захисту інформаційних систем, так і розвиток критичного мислення населення, підвищення рівня медіаграмотності.

О. А. Близняк та К. М. Гуменна [5] систематизували практики боротьби з дезінформацією на основі українського досвіду протидії інформаційній війні рф в умовах повномасштабної війни. У дослідженні виокремлено декілька напрямів

13

протидії: розвиток системи стратегічних комунікацій, створення спеціалізованих структур з виявлення та спростування фейків, міжнародна співпраця у сфері інформаційної безпеки, медіаосвіта населення. Автори детально аналізують ефективність різних інструментів протидії: від законодавчих заборон російського контенту до добровільних ініціатив громадянського суспільства з фактчекінгу. Дослідження підтверджує, що найбільш ефективною є багаторівнева система протидії, яка поєднує державні, громадські та міжнародні зусилля. Автори звертають увагу на помилки та прорахунки у протидії інформаційній агресії на різних етапах конфлікту, підкреслюючи необхідність постійного вдосконалення механізмів захисту інформаційного простору.

Для повноцінного розуміння сутності інформаційної війни необхідно

виокремити її основні ознаки, які дозволяють відрізнити інформаційну війну від інших форм інформаційного впливу. На основі аналізу наукової літератури можна виділити декілька фундаментальних характеристик інформаційної війни. По-перше, це цілеспрямованість та систематичність дій. Інформаційна війна передбачає наявність чітко визначених стратегічних цілей та координацію різноманітних заходів інформаційного впливу для їх досягнення. На відміну від спонтанного поширення неправдивої інформації або окремих випадків маніпуляції, інформаційна війна характеризується плановістю, послідовністю, використанням значних ресурсів. По-друге, це багатоканальність поширення інформації. Інформаційна війна використовує всі доступні канали комунікації: традиційні засоби масової інформації, соціальні мережі, месенджери, блоги, форуми, відеохостинги. Така різноманітність каналів забезпечує охоплення різних сегментів аудиторії та ускладнює протидію інформаційним атакам.

По-третє, інформаційна війна характеризується маскуванню справжніх джерел інформації. Для підвищення довіри до дезінформації використовуються підставні організації, фейкові експертні середовища, анонімні акаунти в соціальних мережах, боти. Приховування справжнього джерела інформації ускладнює її верифікацію та дозволяє уникнути відповідальності за поширення

14

неправдивих відомостей. По-четверте, це адаптивність та еволюція тактик. Інформаційна війна постійно змінюється у відповідь на контрзаходи противника, використовує нові технології, експериментує з різними формами подачі інформації, шукає вразливості в інформаційному захисті опонента. По-п'яте, інформаційна війна передбачає поєднання правдивої інформації з маніпуляціями та відвертою брехнею. Дезінформація часто будується на реальних фактах, які вириваються з контексту, доповнюються вигаданими деталями, інтерпретуються у потрібному агресору ключі. Важливою ознакою інформаційної війни є її спрямованість на емоційну сферу реципієнтів. Інформаційні атаки часто апелюють до базових емоцій людини: страху, гніву, обурення, жалю.

Емоційно забарвлена інформація краще запам'ятовується, активніше

поширюється в соціальних мережах, менш критично сприймається аудиторією. Інформаційна агресія проти України активно використовує емоційні маніпуляції, зокрема поширення жахливих, але неправдивих історій про нібито злочини української сторони, створення віктимізованого образу російськомовного населення України, апеляцію до історичних травм та фобій. Ще однією характерною ознакою інформаційної війни є створення паралельної інформаційної реальності. Замість простого спростування певних фактів інформаційна війна прагне побудувати цілісну альтернативну картину світу, в якій чорне стає білим, жертва перетворюється на агресора, справедливість на несправедливість. Така паралельна реальність має внутрішню логіку, пояснює події минулого та прогнозує майбутнє, пропонує готові інтерпретаційні схеми для розуміння складних явищ.

Інформаційна війна також характеризується використанням принципу інформаційного перевантаження. Замість замовчування певних подій застосовується протилежна тактика: поширення величезної кількості суперечливих, неперевіраних, відверто фейкових повідомлень про одну й ту саму подію. У такому інформаційному шумі людина втрачає здатність відрізнити правду від брехні, що призводить до інформаційної апатії, цинізму, недовіри до

15

будь-яких джерел інформації. Ворожа пропаганда активно використовує цю тактику, створюючи десятки різних версій одних і тих самих подій, кожна з яких претендує на істинність. Результатом стає ситуація, коли людина просто відмовляється від спроб зрозуміти, що насправді відбувається, і починає керуватися емоціями або попередніми переконаннями замість раціонального аналізу інформації.

Характерною рисою сучасної інформаційної війни є використання штучного інтелекту та алгоритмічних систем для створення та поширення дезінформації. Технології глибинного навчання дозволяють генерувати надзвичайно реалістичні фейкові зображення, відео, аудіозаписи, які практично неможливо відрізнити від справжніх без спеціального технічного аналізу. Боти в

соціальних мережах імітують поведінку реальних користувачів, створюючи ілюзію масової підтримки певних ідей або політиків. Алгоритми таргетованої реклами використовуються для точного націлювання дезінформації на найбільш вразливі до неї групи населення. Усе це робить сучасну інформаційну війну значно більш небезпечною та ефективною порівняно з традиційною пропагандою минулого.

Інформаційна війна характеризується також транскордонним характером та глобальним охопленням. На відміну від традиційних військових дій, які обмежені географічними кордонами, інформаційні атаки можуть здійснюватися з будь-якої точки світу та спрямовуватися на аудиторію в будь-якій країні. Інтернет та супутникове телебачення знищили географічні бар'єри для поширення інформації, що дозволяє агресору впливати одночасно на населення безпосередньо атакованої держави, її союзників, нейтральних країн, навіть власного населення. Інформаційна війна проти України не обмежується територією України, а спрямована також на громадську думку в Європі та США з метою підриву міжнародної підтримки України та послаблення санкційного тиску на росію. Важливо відзначити, що інформаційна війна може вестися як окремо, так і у поєднанні з іншими формами агресії. У випадку

16

повномасштабного вторгнення росії в Україну інформаційна війна супроводжує військові дії, доповнює їх, підвищує їхню ефективність. Водночас інформаційна війна може розгортатися і в мирний час, готуючи ґрунт для майбутньої агресії, послаблюючи противника зсередини, створюючи внутрішні протиріччя в суспільстві. Так, російська інформаційна агресія проти України розпочалася задовго до 2014 року і мала на меті поступове відчуження України від європейського цивілізаційного вибору, збереження її в орбіті російського впливу, формування негативного ставлення до української мови та культури навіть серед самих українців.

Підсумовуючи характеристику ознак інформаційної війни, можна стверджувати, що вона є комплексним, багатовимірним явищем, яке поєднує

технологічні, психологічні, соціальні, політичні аспекти. Інформаційна війна використовує найсучасніші досягнення інформаційних технологій, глибоке розуміння психології масової свідомості, знання соціальних процесів та політичних механізмів. Ефективна протидія інформаційній війні вимагає не менш комплексного підходу, який би враховував усі виміри цього явища та використовував адекватні інструменти захисту інформаційного простору. Розуміння сутності та ознак інформаційної війни є необхідною передумовою для розробки ефективної стратегії забезпечення інформаційної безпеки держави та суспільства в умовах гібридних загроз сучасності.

1.2. Теоретичні підходи до класифікації інструментів інформаційної війни

У науковому дискурсі існує декілька концептуальних моделей класифікації інструментів інформаційного протиборства, кожна з яких розкриває певні грані досліджуваного феномену та дозволяє глибше зрозуміти механізми ведення інформаційних війн. О. А. Близняк та К. М. Гуменна виділяють технологічний підхід, згідно з яким інструменти поділяються за способом їх реалізації та каналами поширення [4]. В умовах повномасштабного вторгнення

17

2022-2025 років спостерігається трансформація традиційних засобів інформаційного впливу та поява нових форм маніпулятивних практик. Активно використовуються цифрові платформи, соціальні мережі, месенджери та традиційні медіа для формування потрібних наративів. Технологічна еволюція суттєво розширила можливості ведення інформаційної війни, дозволяючи охоплювати мільйонні аудиторії за лічені години та персоналізувати повідомлення відповідно до характеристик кожного реципієнта.

Г. Гребньов пропонує функціональну класифікацію, яка базується на цілях застосування конкретних інструментів [12]. За такого підходу виділяються засоби дезінформації, спрямовані на спотворення фактичної інформації; інструменти пропаганди, що формують потрібні смисли та інтерпретації подій;

механізми цензури, які обмежують доступ до альтернативних джерел інформації; технології маніпуляції, що впливають на емоційний стан аудиторії. Кожна з категорій має власну специфіку застосування та передбачає використання відповідних методів впливу на аудиторію. Функціональний підхід дозволяє аналізувати інструменти через призму завдань, які вони покликані вирішувати в межах загальної стратегії інформаційного протиборства. О. О. Гордійчук акцентує увагу на структурному підході до систематизації інструментів інформаційної війни [11]. Вчена виокремлює три основні рівні інструментарію: стратегічний, операційний та тактичний. Стратегічний рівень включає довгострокові кампанії з формування негативного образу противника, створення альтернативних історичних наративів, підрив довіри до державних інституцій. Операційний рівень охоплює середньострокові заходи, спрямовані на дискредитацію конкретних політичних рішень, посилення соціальної напруги, створення інформаційних приводів для міжнародної спільноти. Тактичний рівень передбачає короткострокові акції: поширення фейкових новин, організацію ботоферм, проведення DdoS-атак на інформаційні ресурси. Така ієрархічна структура відображає комплексність інформаційної війни та необхідність координації дій на різних рівнях для досягнення стратегічних цілей.

18

В. В. Белімов та співавтори у своєму аналітичному огляді інформаційних подій пропонують хронологічний підхід до класифікації інструментів [45]. У дослідженні відстежується еволюція засобів інформаційного впливу протягом жовтня-грудня 2023 року, що демонструє, як змінюються пріоритети та методи ведення інформаційної боротьби залежно від розвитку подій на фронті.

Така класифікація дозволяє виявити закономірності використання певних інструментів у конкретних ситуаціях та прогнозувати можливі сценарії розвитку інформаційних кампаній. Хронологічний аналіз розкриває адаптивний характер інформаційної війни, де арсенал засобів впливу постійно оновлюється відповідно до змін у воєнно-політичній ситуації та ефективності попередніх операцій. О. Маслій та А. Буряк розробили класифікацію на основі об'єктів

впливу [73]. Виділено інструменти, спрямовані на внутрішню аудиторію агресора, населення країни-жертви, міжнародну спільноту та союзників.

Кожна цільова група потребує специфічних підходів та використання відповідних каналів комунікації. Для внутрішньої аудиторії застосовуються переважно пропагандистські методи з метою підтримки воєнних дій та мобілізації суспільства. Щодо населення країни-жертви використовуються технології психологічного тиску, залякування, деморалізації. Міжнародна спільнота стає об'єктом впливу через створення альтернативних пояснень подій, виправдання агресії, формування образу жертви як агресора.

А. К. Дубень у дослідженні теоретико-методологічних основ інформаційної безпеки пропонує структурувати інструменти за сферами їх застосування [62]. Виділено політичну, економічну, соціальну, культурну, військову сфери, в кожній з яких використовуються специфічні засоби інформаційного впливу. Політична сфера стає об'єктом впливу через дискредитацію владних інституцій, підриг довіри до демократичних процедур, створення образу неефективної влади. Економічна сфера зазнає впливу через поширення панічних настроїв щодо фінансової стабільності, прогнозів економічного колапсу, інформації про корупційні схеми. Соціальна сфера

19

піддається маніпуляціям через загострення міжгрупових конфліктів, етнічних та мовних суперечностей, поглиблення соціального розколу. Культурна сфера стає ареною боротьби за історичну пам'ять, культурні символи, мовну ідентичність.

Військова сфера зазнає інформаційного впливу через дезінформацію про бойові дії, втрати, ефективність збройних сил. Д. Боянич у теоретико-методологічному аналізі викликів, ризиків та загроз у сучасній теорії національної безпеки звертає увагу на необхідність розрізнення інструментів за їхнім потенційним впливом на державну безпеку [57,58]. У роботі запропоновано класифікацію, що враховує масштаб можливих наслідків застосування конкретних засобів інформаційного впливу. До інструментів критичного рівня належать ті, що можуть призвести до дестабілізації державної

системи, масових заворушень, порушення територіальної цілісності. Інструменти високого рівня загрози здатні спричинити значні соціальні потрясіння, економічні втрати, підрив міжнародного авторитету держави.

Технологічна класифікація інструментів інформаційної війни передбачає їх поділ за способами реалізації. До традиційних засобів належать друковані видання, телебачення, радіо, кінематограф. Цифрові інструменти включають соціальні мережі, відеохостинги, новинні портали, месенджери, подкасти. Кібернетичні засоби охоплюють хакерські атаки, створення ботнетів, поширення вірусів та шкідливого програмного забезпечення. Кожна технологічна платформа має власні особливості використання, охоплення аудиторії, швидкості поширення інформації. Еволюція технологій постійно розширює арсенал доступних інструментів, створюючи нові можливості для ведення інформаційного протиборства та водночас породжуючи нові виклики для систем захисту інформаційного простору. Соціальні мережі стали одним із найпотужніших інструментів ведення інформаційної війни. Їхня ефективність зумовлена можливістю швидкого поширення контенту, таргетування аудиторії за демографічними та психографічними характеристиками, створення ефекту вірусності. Російська пропагандистська машина активно використовує Facebook,

20

Twitter, Telegram, TikTok для просування своїх наративів. Створюються фейкові акаунти, організовуються координовані кампанії з поширення дезінформації, проводиться таргетована реклама пропагандистського контенту.

Месенджери набули особливого значення як канал поширення оперативної інформації та чуток. Telegram зокрема став платформою для розповсюдження фейків про обстріли, гуманітарну ситуацію, дії збройних сил. Анонімність та швидкість поширення повідомлень у месенджерах ускладнюють верифікацію інформації та дозволяють ефективно проводити операції психологічного впливу. В умовах активних бойових дій месенджери використовуються для дезорієнтації населення, створення паніки, підриву довіри до офіційних джерел інформації. Приватний характер комунікації в месенджерах створює ілюзію довіри до

отриманої інформації, адже люди схильні більше вірити повідомленням, отриманим від знайомих або у закритих групах, навіть якщо джерело початкової інформації є сумнівним або відверто пропагандистським. Традиційні медіа зберігають своє значення як інструменти інформаційної війни, особливо для впливу на старше покоління та населення регіонів з обмеженим доступом до інтернету. Телебачення використовується для трансляції масштабних пропагандистських наративів, створення потрібного емоційного фону, формування образу ворога.

Кіберінструменти інформаційної війни включають широкий спектр технічних засобів. DdoS-атаки спрямовані на виведення з ладу критичних інформаційних ресурсів, урядових порталів, медіа. Фішингові кампанії використовуються для отримання доступу до конфіденційної інформації, облікових записів посадових осіб, баз даних. Шкідливе програмне забезпечення дозволяє перехоплювати комунікації, викрадати дані, порушувати роботу систем. Кібернетичний вимір інформаційної війни стає дедалі важливішим у міру зростання залежності суспільства від цифрових технологій та інформаційних систем, а межа між кібератаками та традиційними воєнними діями поступово стирається. Класифікація за методами впливу виділяє

21

раціональні, емоційні та підсвідомі інструменти. Раціональні засоби апелюють до логіки, фактів, аргументів, хоча часто базуються на маніпуляції статистикою, вирваних з контексту цитатах, псевдонаукових дослідженнях. Емоційні інструменти використовують страх, гнів, обурення, співчуття для формування потрібної реакції. Підсвідомі механізми включають використання архетипів, символів, повторення, якорування для створення стійких асоціацій та установок.

Поширення панічних настроїв щодо економічної ситуації, прогнозів дефолту, краху банківської системи призводить до реальних негативних наслідків: відтоку капіталу, зниження інвестиційної привабливості, девальвації національної валюти. Інформаційна війна в економічній сфері використовує як традиційні медіа, так і соціальні мережі для поширення негативних прогнозів та

дискредитації економічної політики держави. Економічний вимір інформаційної війни демонструє, як маніпуляція інформацією може призводити до матеріальних втрат та реальних економічних криз, перетворюючи інформаційний вплив на потужну зброю економічного тиску. Інституційна класифікація інструментів виділяє державні, квазідержавні та недержавні структури, що беруть участь у веденні інформаційної війни. Державні інструменти включають офіційні медіа, урядові структури з питань інформаційної політики, спецслужби. Квазідержавні організації формально незалежні, але фактично контролюються та фінансуються державою. Недержавні суб'єкти включають пропагандистські медіа, тролінгові фабрики, хакерські групи, блогерів-пропагандистів.

Комплексні інформаційні операції передбачають одночасне застосування традиційних медіа, соціальних мереж, кіберзасобів для досягнення максимального ефекту. Синхронізація повідомлень через різні канали, взаємопосилення наративів, створення інформаційного резонансу підвищують результативність впливу на цільову аудиторію. Оркестрована природа сучасних інформаційних кампаній свідчить про високий рівень планування та координації,

22

де кожен інструмент відіграє певну роль у загальній стратегії, а їхня взаємодія створює кумулятивний ефект, що значно перевищує суму окремих впливів. Географічна класифікація виділяє інструменти, спрямовані на різні регіони та країни. Для пострадянського простору використовуються специфічні наративи про спільну історію, мову, культуру. Європейська аудиторія стає об'єктом впливу через теми біженців, енергетичної безпеки, економічних втрат від санкцій. Для країн Глобального Півдня розробляються наративи про колоніалізм, неоімперіалізм Заходу, подвійні стандарти.

Оперативні засоби використовуються для швидкого реагування на події, поширення термінових фейків, організації флешмобів. Тактичні інструменти застосовуються для середньострокових кампаній тривалістю від тижнів до місяців. Стратегічні механізми спрямовані на довгострокову трансформацію

свідомості, зміну історичної пам'яті, перекодування культурних смислів. Часова стратифікація інструментів інформаційної війни демонструє багаторівневність інформаційного протиборства, де короткострокові тактичні операції служать досягненню довгострокових стратегічних цілей, а миттєве реагування на події поєднується з планомірною роботою з трансформації колективних уявлень. Класифікація за формою подачі інформації включає текстові, аудіовізуальні, мультимедійні інструменти. Текстові засоби охоплюють статті, пости, коментарі, меми з текстом. Аудіовізуальні інструменти включають фото, відео, аудіозаписи, інфографіку. Мультимедійні формати поєднують різні типи контенту для посилення впливу.

Ревізія історії, створення альтернативних історичних наративів, присвоєння культурної спадщини, заперечення окремої ідентичності народу становлять довгострокову стратегію інформаційного впливу. Фільми, книги, виставки, освітні програми використовуються для просування потрібної версії історичних подій та формування спільної ідентичності. Культурно-історичний вимір інформаційної війни спрямований на підрив фундаментальних основ національної ідентичності через деконструкцію історичної пам'яті та

23

культурних символів, що робить його особливо небезпечним для довгострокового існування нації як окремої спільноти. Класифікація за рівнем складності виділяє прості та складні інструменти інформаційної війни. Прості засоби включають поширення окремих фейків, публікацію провокаційних коментарів, створення одиночних пропагандистських матеріалів. Складні інструменти передбачають організацію масштабних інформаційних кампаній, координацію дій різних суб'єктів, використання штучного інтелекту для генерації контенту, створення дипфейків. Використання технологій штучного інтелекту для створення фальшивих фото та відео, автоматизація генерації пропагандистського контенту, персоналізація повідомлень на основі даних користувачів підвищують ефективність інформаційних операцій.

Ізольований аналіз окремих засобів впливу не дозволяє побачити

системний характер інформаційних операцій. Взаємозв'язок різних інструментів, їхня координація та синергія створюють кумулятивний ефект, що значно перевищує суму впливів окремих елементів. Тому ефективна протидія інформаційній війні потребує розуміння всієї системи інструментів та механізмів їх застосування. Системний характер інформаційної війни вимагає відповідного системного підходу до аналізу та протидії, де враховуються всі рівні, форми та методи інформаційного впливу у їхній взаємодії та взаємному посиленні. Етична класифікація розрізняє інструменти за мірою їхньої моральної прийнятності. Маніпуляція, обман, підбурювання до ненависті, заклики до насильства становлять неетичні інструменти інформаційної війни. Проте агресор часто не керується етичними обмеженнями, використовуючи найцинічніші методи впливу.

Класифікація за результатами впливу виділяє інструменти формування думок, зміни поведінки, управління діями. Формування думок передбачає створення та закріплення певних переконань, оцінок, установок. Зміна поведінки включає стимулювання або блокування конкретних дій: участі у протестах, міграції, споживчих рішень. Управління діями означає досягнення повного

24

контролю над вибором людини через тотальну маніпуляцію інформаційним полем. Систематичний інформаційний тиск призводить до трансформації ціннісних орієнтацій, політичних переконань, громадянської ідентичності. Інструменти інформаційної війни використовуються для підриву національної єдності, деморалізації суспільства, створення розколу між різними групами населення. Водночас спостерігається формування стійкості до інформаційних маніпуляцій через набуття досвіду розпізнавання пропаганди, що свідчить про адаптивність суспільства до умов інформаційної війни. Інноваційна класифікація звертає увагу на нові інструменти інформаційної війни, що з'являються завдяки технологічному розвитку. Метавсесвіти створюють нові простори для інформаційного впливу. Нейромережі дозволяють генерувати реалістичний контент у промислових масштабах. Блокчейн-технології використовуються для

створення децентралізованих пропагандистських платформ.

Доповнена та віртуальна реальність відкривають можливості для створення імерсивних пропагандистських наративів. Аналіз класифікацій інструментів інформаційної війни виявляє багатоаспектність феномену, де технологічний критерій відображає еволюцію від традиційних медіа до цифрових платформ, функціональний демонструє різноманітність цілей від дезінформації до психологічного тиску, а структурний розкриває багаторівневість планування від стратегічних кампаній до тактичних акцій. Психологічна систематизація виявляє механізми впливу на когнітивну, емоційну та поведінкову сфери, класифікація за об'єктами впливу підкреслює багатовекторність роботи з цільовими аудиторіями, а розмежування легальних і нелегальних інструментів має значення для міжнародно-правової оцінки дій агресора. Багатовимірність підходів свідчить про системність явища, тому комплексне застосування різних класифікаційних схем забезпечує найповніше розуміння феномену та дозволяє розробляти ефективні стратегії протидії інформаційним загрозам.

25

1.3. Світовий досвід ведення інформаційних війн у XX–XXI століттях

Історичний аналіз інформаційних протиборств демонструє їхню трансформацію від класичної пропаганди до багаторівневих кампаній у цифровому просторі. Упродовж XX століття інформаційна війна еволюціонувала разом із технологічним прогресом, набуваючи дедалі складніших форм і методів впливу на суспільну свідомість.

Розуміння історичного контексту інформаційних війн є необхідним для аналізу сучасних загроз і розробки ефективних стратегій протидії. Перша світова війна стала переломним моментом у розвитку систематичної інформаційної боротьби. Країни, що брали участь у війні, створили спеціалізовані пропагандистські структури, спрямовані на деморалізацію противника та зміцнення власного тилу. Британський Департамент пропаганди ворожим

країнам і Комітет громадської інформації США розробили комплексні кампанії, що охоплювали друковані видання, кінематограф і публічні виступи. Німеччина застосовувала схожі методи через Центральне бюро закордонної служби. Досвід цього періоду продемонстрував, що координована інформаційна робота може суттєво впливати на моральний стан як військових, так і цивільного населення.

Міжвоєнний період характеризувався становленням тоталітарних режимів, які довели пропаганду до рівня державної ідеології. Радянський Союз створив розгалужену систему агітації та пропаганди (Агітпроп), яка контролювала всі аспекти інформаційного простору. Нацистська Німеччина під керівництвом Міністерства народної освіти та пропаганди розробила досконалі технології маніпулювання масовою свідомістю, використовуючи радіо, кіно та друковану продукцію. Фашистська Італія запровадила Міністерство преси та пропаганди, що здійснювало тотальний контроль над засобами масової інформації.

Друга світова війна вивела інформаційне протиборство на якісно новий рівень. Союзники створили Управління стратегічних служб США та Виконавчий комітет політичної боротьби Великої Британії, що координували психологічні

26

операції на всіх напрямках бойових дій. Радіопередачі транслювалися ворожим військам і населенню окупованих територій, листівки масово розповсюджувалися з літаків, а агенти впливу поширювали дезінформацію в тилу противника. Німеччина відповідала власними пропагандистськими кампаніями через Міністерство Геббельса та Іноземний відділ Верховного командування вермахту.

Холодна війна трансформувала інформаційне протиборство в безперервний глобальний процес. Сполучені Штати заснували Інформаційне агентство США, що здійснювало культурну та інформаційну експансію через радіостанції «Голос Америки», «Радіо Свобода» та «Вільна Європа». СРСР створив систему міжнародного мовлення через «Радіо Москва» та використовував заходи активних дій через КДБ для поширення дезінформації на Заході. В'єтнамська війна стала першим великим конфліктом, де телебачення

відіграло вирішальну роль у формуванні громадської думки, продемонструвавши вразливість демократичних суспільств до візуального контенту з театру бойових дій.

Розпад Радянського Союзу відкрив нову еру регіональних конфліктів із потужним інформаційним супроводом. Війна в Перській затоці 1991 року вперше продемонструвала вплив інформаційних телеканалів, що працюють цілодобово, на сприйняття воєнних подій у реальному часі. Балканські війни 1990-х років характеризувалися інтенсивним використанням етнічної пропаганди та дезінформації для розпалювання ворожнечі між народами. НАТО використовувало інформаційні операції під час бомбардувань Югославії 1999 року, намагаючись виправдати військове втручання перед міжнародною спільнотою.

Терористичні атаки 11 вересня 2001 року і наступна «Війна з тероризмом» ознаменували початок епохи асиметричних інформаційних конфліктів. Терористичні організації почали активно використовувати Інтернет для рекрутингу, поширення пропаганди та координації дій. «Аль-Каїда» та пізніше

27

«Ісламська держава» створили професійні медіацентри, що продукували якісний пропагандистський контент різними мовами. США і союзники відповіли створенням Глобального центру взаємодії для протидії радикальній ідеології. Цей період продемонстрував здатність недержавних учасників проводити ефективні інформаційні кампанії проти значно потужніших супротивників. Арабська весна 2010–2012 років виявила революційний потенціал соціальних мереж в організації масових протестів і поширенні інформації. Facebook, Twitter, YouTube стали платформами для мобілізації населення та обходу державної цензури в Тунісі, Єгипті, Лівії та Сирії. Події Арабської весни показали вразливість авторитарних режимів до низових інформаційних кампаній, організованих через цифрові платформи. Водночас ті самі інструменти почали активно використовуватися державами для маніпулювання громадською думкою та придушення опозиції.

Агресія росії проти України з 2014 року започаткувала еру гібридних війн із домінуванням інформаційної складової. Анексія Криму та конфлікт на Донбасі супроводжувалися масштабною дезінформаційною кампанією, спрямованою на виправдання військової агресії. Противник використовував державні медіа, інтернет-тролів, ботів у соціальних мережах і хакерські атаки для просування власних наративів. Стратегія полягала у створенні альтернативної інформаційної реальності, де агресор постає жертвою, а справжня жертва зображується агресором.

Повномасштабне вторгнення росії в Україну 24 лютого 2022 року стало кульмінацією російської інформаційної війни. Напередодні вторгнення росія намагалася сформувати сприятливий інформаційний фон через поширення наративів про «геноцид» на Донбасі та «неминучість» військової операції [11]. Україна продемонструвала вражаючу стійкість у протидії російській пропаганді завдяки скоординованим зусиллям державних органів, громадянського суспільства та міжнародних партнерів.

28

Міжнародний досвід протидії інформаційним війнам демонструє різноманітність підходів. Європейський Союз створив East StratCom Task Force (Оперативну групу зі стратегічних комунікацій на Сході) для моніторингу та спростування російської дезінформації. Сполучені Штати Америки заснували Global Engagement Center (Глобальний центр взаємодії) для координації міжвідомчих зусиль проти ворожих пропагандистських кампаній. Країни Балтії, маючи досвід радянської окупації, розвинули комплексні системи інформаційної безпеки, що включають медіаосвіту, законодавчі обмеження та міжнародну співпрацю.

Г. Гребньов зазначає, що найуспішніші стратегії поєднують превентивні заходи з оперативним реагуванням на загрози [12]. Ізраїль виробив власну модель протидії інформаційним атакам, зосередившись на швидкому спростуванні фальшивої інформації та активній комунікації з міжнародною аудиторією. Південна Корея розвинула потужні цифрові технології для

виявлення та нейтралізації північнокорейської пропаганди. Тайвань запровадив інноваційні підходи до боротьби з дезінформацією, залучаючи громадянське суспільство та використовуючи гумор як інструмент дискредитації фейків.

Сучасні інформаційні війни характеризуються використанням штучного інтелекту, алгоритмічного таргетування та синтетичних медіа. Дипфейки, автоматизовані бот-мережі та мікротаргетована дезінформація створюють нові виклики для суспільств і держав.

Г. Гребньов стверджує, що майбутні інформаційні конфлікти вимагатимуть інтеграції технологічних рішень із гуманітарними підходами для захисту демократичних цінностей [12] (детальніше див. Таблицю 1.2). *Таблиця 1.2.*

Еволюція методів ведення інформаційних війн у XX–XXI століттях

Період	Основні учасники	Провідні технології	Характерні методи	Історичні приклади
Перша світова війна (1914–1918)	Держави учасниці конфлікту	Друковані видання, плакати, кінематограф	Патріотична пропаганда, демонізація противника, цензура	Британський Департамент пропаганди, Комітет громадської інформації США
Міжвоєнний період (1918–1939)	Тоталітарні режими	Радіо, масові заходи, кінохроніка	Ідеологічна індоктринація, культ особи, контроль медіа	Агітпроп СРСР, Міністерство пропаганди Німеччини
Друга світова війна (1939–1945)	Держави воєнної коаліції	Радіомовлення, листівки, підпільна преса	Психологічні операції, дезінформація, підривна діяльність	«Чорна пропаганда» союзників, німецьке радіо для СРСР
Холодна війна (1947–1991)	США та СРСР	Міжнародне радіо, телебачення, друковані медіа	Ідеологічне протистояння, культурна дипломатія, активні заходи	«Голос Америки», «Радіо Свобода», «Радіо

				Москва», операції КДБ
Пост-холод на війна (1991– 2001)	Держави та коаліції	Супутникове телебачення, ранній Інтернет	Медійний супровід конфліктів, інформаційні операції	Війна в Перській затоці, операція НАТО в Югославії
Війна з тероризмом (2001–2010)	Держави та терористич ні групи	Інтернет-форум и, відеохостинги, мобільний зв'язок	Онлайн рекрутинг, медіа джихад, контрпропаганда	Пропаганда «Аль-Каїди», американські інформаційні центри
Епоха соціальних мереж (2010– 2014)	Держави, активісти, корпорації	Facebook, Twitter, YouTube, смартфони	Мобілізація протестів, вірусний контент, цифрова цензура	Арабська весна, революція Євромайдану
Гібридні війни (2014–2022)	росія проти України та Заходу	Боти, тролі, державні медіа (RT і Sputnik), хакерські атаки	Дезінформація , фейкові новини, кібератаки, маніпуляція виборами	Анексія Криму, втручання у вибори США 2016 року, конфлікт на Донбасі

30

Повномасшта бна агресія (2022– дотепер)	росія проти України	Штучний інтелект, дипфейки, Telegram, координовані мережі	Синтетичні медіа, автоматизована дезінформація, цифрова стійкість	російське вторгнення в Україну, українська інформацій на оборона
--	---------------------------	--	---	---

Складено автором на основі джерел [4, 5, 6, 11, 12, 45, 58, 62, 73, 75].

Аналіз історичного досвіду інформаційних війн виявляє декілька стійких тенденцій. Інформаційне протиборство завжди йде в ногу з технологічним розвитком, використовуючи найсучасніші канали комунікації для досягнення цілей. Кожна нова комунікаційна технологія неодмінно ставала знаряддям

інформаційної боротьби. Держави постійно вдосконалюють організаційні структури для ведення інформаційних операцій, створюючи спеціалізовані відомства та координаційні механізми. Інституціоналізація інформаційної боротьби є характерною рисою сучасних держав. Інформаційні війни дедалі більше інтегруються з військовими діями, утворюючи єдиний комплекс впливу на противника. Розмежування між інформаційними та військовими операціями поступово зникає, оскільки обидва компоненти стають взаємозалежними. По четверте, роль недержавних учасників в інформаційних конфліктах постійно зростає, що ускладнює визначення джерел атак і розробку відповідних контрзаходів. По-п'яте, демократичні суспільства виявляються особливо вразливими до інформаційних атак через відкритість медіапростору та захист свободи слова. О. М. Венгер відзначає парадоксальну ситуацію, коли демократичні цінності стають інструментом їхнього власного підриву в руках авторитарних режимів [6]. По-шосте, ефективність інформаційних операцій залежить не лише від технологічної досконалості, а й від культурного контексту, довіри населення до інституцій і рівня медіаграмотності.

Аналіз світового досвіду ведення інформаційних війн засвідчує безперервну еволюцію методів і технологій впливу на суспільну свідомість. Розуміння історичних закономірностей інформаційних протиборств є

31

необхідною передумовою для розробки ефективних стратегій захисту національних інтересів у сучасному інформаційному просторі. Український досвід протидії російській інформаційній агресії вже став цінним внеском у світову практику інформаційної безпеки. Майбутнє інформаційних конфліктів вимагатиме інтеграції технологічних інновацій з гуманітарними знаннями для забезпечення стійкості демократичних суспільств.

Висновки до розділу 1

Теоретико-методологічний аналіз феномену інформаційної війни дозволяє сформулювати низку принципових висновків щодо природи, механізмів і

історичного розвитку цього явища. Інформаційна війна є комплексною системою цілеспрямованих дій у інформаційному просторі, спрямованих на досягнення стратегічних цілей через вплив на свідомість, поведінку та прийняття рішень цільовими аудиторіями. На відміну від традиційних форм пропаганди, сучасна інформаційна війна характеризується багатовекторністю, використанням передових технологій і координацією різноманітних каналів впливу. В. В. Белімов та інші дослідники обґрунтовують необхідність міждисциплінарного підходу, що синтезує військово-стратегічні, комунікаційні, психологічні та технологічні аспекти, О. О. Гордійчук підкреслює важливість розрізнення між інформаційною війною як стратегічним феноменом і окремими інформаційними операціями як тактичними інструментами, а Г. Гребньов наголошує на трансформації інформаційної війни з допоміжного елемента збройного конфлікту в самостійну форму стратегічного протиборства.

Класифікація інструментів інформаційної війни демонструє їхню різноманітність і взаємодоповнюваність. О. А. Близняк і К. М. Гуменна виокремлюють технологічні, контентні, організаційні та психологічні інструменти, що формують інтегровану систему впливу, О. Маслій і А. Буряк обґрунтовують розмежування між наступальними та оборонними інструментами

32

інформаційної боротьби, а О. М. Венгер підкреслює зростання ролі цифрових технологій у розширенні арсеналу інформаційних впливів.

Історичний аналіз інформаційних війн XX–XXI століть виявив еволюцію від централізованої державної пропаганди до децентралізованих мережевих кампаній у цифровому просторі, де Перша і Друга світові війни започаткували систематичне використання пропаганди як елемента державної стратегії, Холодна війна інституціоналізувала інформаційне протиборство як безперервний глобальний процес, а російська агресія проти України з 2014 року ознаменувала перехід до гібридних форм інформаційної війни, що інтегрують військові, дипломатичні, економічні та інформаційні інструменти впливу.

Аналіз світового досвіду виявив стійкі закономірності: інформаційні

технології відповідають рівню розвитку комунікаційних засобів; держави постійно вдосконалюють інституційні механізми координації операцій; демократичні суспільства виявляються особливо вразливими через відкритість медіапростору; ефективність протидії залежить від медіаграмотності населення та швидкості реагування на дезінформацію. Міжнародний досвід засвідчує важливість комплексного підходу, що поєднує законодавче регулювання, технологічні рішення, медіаосвіту та міжнародну співпрацю. Країни Балтії, Ізраїль, Тайвань, Південна Корея, Європейський Союз і Сполучені Штати виробили власні моделі інформаційної безпеки, а український досвід протидії російській агресії додав нові практики до світового арсеналу стратегій інформаційної стійкості. Теоретико-методологічні засади дослідження інформаційної війни формують концептуальну основу для подальшого аналізу російської інформаційної агресії проти України, оскільки розуміння природи, інструментів і історичного контексту є необхідною передумовою для об'єктивної оцінки масштабів, методів і наслідків російської інформаційної кампанії.

33

РОЗДІЛ 2. ІНФОРМАЦІЙНА ВІЙНА РФ ПРОТИ УКРАЇНИ ЕТАПИ ТА ОСОБЛИВОСТІ У ПЕРІОД ПОВНОМАСШТАБНОГО ВТОРГНЕННЯ

2.1. Основні характеристики інформаційної війни РФ в просторі України

Повномасштабне вторгнення російської федерації проти України у 2022 році стало кульмінацією багаторічного протистояння, що охоплювало військову, економічну та інформаційну сфери. Інформаційна війна як складова гібридної агресії має глибоке історичне коріння, сягаючи періоду Радянського Союзу.

Після здобуття Україною незалежності у 1991 році російська пропаганда систематично формувала негативний образ української держави, ставила під сумнів легітимність державотворення, просуvala наративи про штучність української нації та мови. Анексія Криму та початок збройної агресії на Донбасі

у 2014 році ознаменували новий етап інформаційної війни, що характеризувався посиленням інтенсивності дезінформаційних кампаній та розширенням арсеналу інструментів впливу. Повномасштабне вторгнення 24 лютого 2022 року супроводжувалося безпрецедентною інформаційною кампанією, спрямованою на досягнення декількох стратегічних цілей одночасно: посів паніки серед українського населення, підриг довіри до владних інституцій, переконання міжнародної спільноти у неминучості поразки України, виправдання військових злочинів та створення альтернативної реальності для внутрішньої російської аудиторії [2, 11, 12, 51, 52]. Аналіз еволюції російської інформаційної війни проти України свідчить про свідому стратегію використання радянських методів пропаганди, адаптованих до сучасних умов цифрової епохи.

В цьому випадку йдеться про інституційну пам'ять спецслужб та пропагандистських структур, що зберегли кадровий та методологічний потенціал радянської системи ідеологічного впливу [11]. Багато прийомів інформаційної психологічної операції, методи яких розроблено радянськими спецслужбами, були модернізовані та інтегровані у сучасну російську стратегію

34

гібридної війни. Важливо підкреслити, що тривала інформаційна підготовка до військової агресії, яка розпочалася до 2014 р., свідчить про стратегічне планування масштабного конфлікту, а не про реакцію на поточні події, як це намагається представити російська пропаганда [51]. Формування у російському суспільстві образу ворога, виправдання майбутньої агресії геополітичними аргументами, підготовка міжнародної громадськості до сприйняття можливого конфлікту як внутрішньоукраїнської проблеми – всі ці елементи свідчать про системний та довгостроковий характер інформаційної війни.

Конституція України від 28 червня 1996 року закріпила основні принципи державного суверенітету та територіальної цілісності [17, 24], проте саме ці конституційні засади стали головною мішенню російської інформаційної агресії протягом усього періоду незалежності. Постійне заперечення права України на суверенне існування, систематичне поширення концепцій про «єдиний народ»,

«один народ у трьох державах», «русский мир» створювали ідеологічну базу для майбутніх територіальних претензій та виправдання потенційного збройного вторгнення. Ця довгострокова стратегія легітимізації агресії через історичні та культурні наративи є характерною особливістю російської інформаційної політики щодо України. Події 2014 року стали своєрідним випробувальним полігоном для відпрацювання інформаційних технологій агресора в умовах реального конфлікту. Анексія Криму продемонструвала неготовність України до масштабної інформаційної агресії та відсутність ефективних механізмів оперативної протидії потоку дезінформації [52]. Згаданий досвід був ретельно проаналізований російською стороною та використаний для вдосконалення інструментів інформаційного впливу. Використання присутності спостерігачів ОБСЄ для поширення власних наративів та дискредитації української позиції стало типовим елементом російської стратегії інструменталізації міжнародних інституцій [20]. Така практика підриву довіри до міжнародних організацій через їх вибіркове використання та маніпулювання результатами моніторингових місій продовжується і в умовах повномасштабної війни.

35

Інформаційний вимір сучасних збройних конфліктів перетворився на критичний інструмент впливу, здатний визначати не лише сприйняття подій, а й реальний хід військово-політичних процесів. Повномасштабне вторгнення російської федерації в Україну підтвердило, що війна XXI століття ведеться одночасно на полях бою та у свідомості людей. Інформаційний простір перетворився на окрему сферу протиборства з реальними геополітичними наслідками [57]. Тема НАТО посідає центральне місце в російській інформаційній стратегії через систематичне перебільшення загрози з боку альянсу, представлення розширення НАТО як експансії та використання цієї теми для виправдання власної агресивної політики [2, 58, 73]. Міжнародні організації відіграють важливу роль у документуванні російської інформаційної агресії, при цьому Європейський Союз надає Україні значну допомогу, включаючи підтримку незалежних медіа, програми медіаграмотності та технічну

допомогу у виявленні дезінформації [64, 76]. Міжнародні санкції проти російської федерації активно використовуються пропагандою для просування власних наративів про економічну війну Заходу [60].

Україна поступово розбудовує систему інституційних механізмів протидії, що вимагає координації різних державних органів та достатнього фінансування [17, 49, 53]. Підвищення рівня медіаграмотності населення та розвиток фактчекінгу є критично важливими напрямками протидії інформаційній війні [4, 12]. Стратегічні комунікації включають формування власних наративів, що резонують з аудиторією та ефективно протистоять російській пропаганді [4, 5, 11, 34]. Система територіальної оборони та процес мобілізації стали об'єктами цілеспрямованих інформаційних атак, спрямованих на підрив довіри населення та ослаблення мобілізаційного потенціалу [22, 24, 54]. Майбутнє системи інформаційної безпеки визначатиметься розвитком технологічних можливостей виявлення дезінформації, міжнародною співпрацею та необхідністю реінтеграції постраждалих від інформаційної війни територій [37, 40, 49].

36

Аналіз інструментів та методів російської інформаційної війни свідчить про системний характер пропагандистської машини агресора, що функціонує на декількох взаємопов'язаних рівнях одночасно. Інформаційна війна у повномасштабній фазі конфлікту набула характеристик тотального інформаційного протиборства, де кожна сфера суспільного життя стає об'єктом маніпулятивного впливу. Критичним елементом російської стратегії є використання теми НАТО як універсального виправдання агресії перед різними аудиторіями. Систематичне перебільшення загрози з боку альянсу, інтерпретація його розширення як порушення нібито досягнутих домовленостей, представлення оборонних заходів альянсу як підготовки до нападу на росію створюють ілюзію оточеної та загрозливої для західного блоку країни, яка змушена захищатися превентивними діями [2, 58]. Посилення військової присутності США та НАТО в Європі після 2014 року використовується для підтвердження наративу про агресивні наміри Заходу, при цьому американська

військова присутність у країнах Балтії та Східної Європи представляється як окупація та втручання у внутрішні справи суверенних держав [73]. Власний аналіз показує, що російська пропаганда намагається протиставити азіатську модель безпеки атлантичній, критикуючи НАТО як застарілу блокову структуру часів холодної війни, одночасно просуваючи ідеї про необхідність створення альтернативних макетів безпеки без участі США [62]. Ця стратегія розрахована на послаблення трансатлантичної єдності та формування альтернативних центрів впливу, лояльних до російських геополітичних інтересів.

Міжнародні санкції проти російської федерації стали потужним інструментом економічного тиску, проте російська пропаганда майстерно експлуатує цю тему для зміцнення внутрішньої підтримки режиму та розколу міжнародної коаліції. Для внутрішньої російської аудиторії санкції представляються як економічна війна Заходу, спрямована на знищення російської економіки та покарання російського народу за незалежну зовнішню політику. Створюється образ росії як жертви західної агресії, що має

37

консолідувати населення навколо політичного керівництва перед лицем зовнішньої загрози [60]. Реальні економічні труднощі, спричинені санкційним тиском, використовуються не для критичного переосмислення агресивної політики, а для посилення антизахідних настроїв та мобілізації суспільства на підтримку війни. Для західної аудиторії російська пропаганда одночасно намагається переконати у неефективності санкцій, їхньому руйнівному впливі на світову економіку, несправедливості покарання звичайних росіян за дії влади.

Активно поширюються наративи про бумеранг-ефект санкцій, що завдають шкоди насамперед країнам, які їх запровадили, через зростання цін на енергоносії, інфляцію, зниження життєвого рівня. Метою цієї двосторонньої кампанії є одночасне зміцнення внутрішньої легітимності режиму та послаблення зовнішнього санкційного тиску через формування громадської думки у західних країнах, що вимагає скасування обмежень заради власних економічних інтересів. Україна в умовах тривалої інформаційної агресії

поступово розбудовує систему інституційних механізмів протидії, що вимагає координації діяльності різних державних органів, чіткого розподілу повноважень, достатнього фінансування та підготовки кваліфікованого персоналу [49]. Конституція України встановлює основоположні принципи інформаційної безпеки, гарантуючи свободу слова та інформації, водночас дозволяючи обмеження цих прав у разі загрози національній безпеці [17]. Збалансування демократичних свобод та потреб безпеки є складним завданням, особливо коли агресор систематично використовує демократичні свободи для підривної діяльності. Ефективна система інформаційної безпеки вимагає інтеграції механізмів захисту у всі сфери державної діяльності, включаючи економічну, соціальну та культурну, що дозволяє врахувати специфіку різних секторів та забезпечити комплексний захист [53].

Підвищення рівня медіаграмотності населення є стратегічно важливим напрямом протидії інформаційній війні, оскільки критичне мислення та вміння аналізувати інформацію формують імунітет суспільства до маніпулятивних

38

впливів. Навчання по розпізнаванню дезінформації, перевірці джерел, критичному аналізу контенту, розумінню механізмів маніпулювання має стати невід'ємною частиною освітньої системи на всіх рівнях [4]. Важливим є формування звички перевіряти інформацію з декількох незалежних джерел перед її поширенням та усвідомлення власної відповідальності за розповсюдження недостовірної інформації. Перевірка фактів у сучасних умовах інформаційної війни набуває особливої ваги, оскільки її результативність залежить від швидкості реагування, високого рівня професійної підготовки, доступу до надійних джерел та вміння опрацьовувати великі масиви даних [12]. Фахівці, які здійснюють перевірку фактів, мають залишатися незалежними, неупередженими та забезпечувати прозорість застосовуваних методів. Міжнародна підтримка цієї діяльності через фінансування, навчальні програми та обмін досвідом сприяє формуванню мереж співпраці, що дає змогу оперативно верифікувати інформацію, поширювану в різних країнах, і підвищує

ефективність протидії дезінформації.

Проведений аналіз свідчить, що пасивний захист, обмежений лише спростуванням фейків, є принципово недостатнім для ефективної протидії російській інформаційній агресії. Необхідно формувати власні проактивні наративи, що резонують з цільовою аудиторією та створюють альтернативу російській пропаганді [34]. Стратегічні комунікації включають формування позитивного образу України, просування українських демократичних цінностей, систематичне донесення правди про війну до міжнародної аудиторії. Критично важливим є створення емоційно привабливого контенту, що викликає співчуття, солідарність, бажання підтримати Україну, оскільки сухі факти часто програють емоційним маніпуляціям російської пропаганди. Український досвід протидії включає активне використання соціальних мереж, залучення лідерів думок різних рівнів, створення вірусного контенту, що органічно поширюється аудиторією [4, 5]. Президент України, високопосадовці, військовослужбовці, звичайні громадяни активно комунікують через цифрові платформи, створюючи

39

автентичну альтернативу централізованій російській пропаганді. Автентичність та щирість таких повідомлень є їхньою сильною стороною порівняно з професійною, але фальшивою російською пропагандою, оскільки сучасна аудиторія високо цінує достовірність та особисту відповідальність комунікатора.

Формування ефективних контрнарративів вимагає глибокого розуміння цільової аудиторії, її базових цінностей, актуальних страхів, легітимних прагнень. Сегментація аудиторії та створення адаптованих повідомлень для різних груп є необхідною умовою успіху [11]. Наративи, що резонують із західною ліберально-демократичною аудиторією, можуть бути неефективними або навіть контрпродуктивними для країн глобального Півдня з їхніми специфічними історичними травмами та геополітичними інтересами. Універсальні повідомлення часто програють таргетованим комунікаціям, що враховують культурний контекст та актуальний порядок денний конкретної спільноти. Система територіальної оборони України стала об'єктом

цілеспрямованих багаторівневих інформаційних атак з боку російської федерації. Пропаганда намагається дискредитувати територіальну оборону, представляючи її як неефективну, погано озброєну, недостатньо підготовлену структуру, поширюючи фейки про конфлікти між підрозділами територіальної оборони та регулярними військами, випадки мародерства, перевищення повноважень [54]. Метою таких операцій є підриг довіри населення до територіальної оборони, стримування громадян від добровільного вступу до лав захисників, провокування соціальних конфліктів між цивільними та військовими структурами. Одночасно для західної аудиторії поширюються побоювання щодо неконтрольованого розповсюдження зброї серед цивільного населення, можливості її потрапляння до рук екстремістських угруповань чи організованих злочинних угруповань, що має підірвати міжнародну підтримку України.

Психологічний тиск на військовослужбовців та їхні родини є окремим критичним напрямом російської інформаційної війни. Інформаційна агресія спрямована на підриг морального духу захисників через систематичне

40

поширення дефетистських настроїв, свідоме перебільшення масштабів втрат, створення відчуття безперспективності подальшого опору [22]. Поширюються цілеспрямовані погрози щодо фізичної розправи, переслідування родичів, публікації персональних даних військовослужбовців. Створюються фейкові повідомлення нібито від командування про загибель чи важке поранення військовослужбовців з метою дезорганізації підрозділів та посіву паніки серед родин. Використовуються відео з військовополоненими, демонстрація жорстокого поводження, залякування майбутнім для провокування страху, відчаю, небажання продовжувати боротьбу. Тема мобілізації є однією з найбільш вразливих для маніпуляцій в умовах затяжної війни, оскільки зачіпає життєві інтереси широких верств населення. Систематично поширюються фейки про масове ухилення від мобілізації, жорстокі методи примусового призову, тотальну корупцію у військових комісаріатах, несправедливий розподіл мобілізаційного навантаження між різними соціальними групами та регіонами.

Подібні наративи мають стимулювати страх перед мобілізацією, провокувати масову еміграцію працездатного населення за кордон, породжувати гострі конфлікти між різними групами населення [24]. Будь-які об'єктивні труднощі та поодинокі недоліки мобілізаційної системи миттєво перебільшуються та тиражуються через підконтрольні канали комунікації, створюючи враження системної кризи державних інституцій.

Майбутнє системи інформаційної безпеки України визначатиметься декількома стратегічними чинниками. Розвиток технологічних можливостей виявлення та нейтралізації дезінформації через використання штучного інтелекту, машинного навчання, аналізу великих даних може суттєво підвищити ефективність моніторингу інформаційного простору та оперативного реагування на загрози [49]. Проте технологічні рішення мають обов'язково доповнюватися розвитком людського потенціалу, професійною підготовкою фахівців відповідного профілю, формуванням зрілої експертної спільноти. Міжнародна співпраця залишатиметься критично важливою для ефективної протидії

41

транснаціональним інформаційним загрозам, що не визнають державних кордонів [37]. Україна може використати власний досвід багаторічного протистояння російській інформаційній агресії для налагодження стратегічного партнерства з іншими країнами, систематичного обміну кращими практиками, розбудови глобальної мережі протидії авторитарній дезінформації. Питання відновлення та реінтеграції постраждалих від інформаційної війни територій та груп населення набуде особливої актуальності в післявоєнний період [40]. Деокупація територій вимагатиме систематичної довгострокової роботи з подолання наслідків багаторічної цілеспрямованої російської пропаганди. Населення окупованих територій тривалий час перебувало в умовах тотального інформаційного контролю, було ізольованим від альтернативних джерел інформації, зазнавало систематичного ідеологічного впливу. Реінтеграція таких громадян у єдиний інформаційний та ціннісний простір України вимагатиме значного часу, стратегічного терпіння, виваженого та чутливого підходу без

стигматизації жертв окупації. Повернення біженців також матиме складний інформаційний вимір, оскільки люди, що тривалий час перебували за межами України, могли зазнати впливу різних інформаційних наративів, сформуванати специфічні уявлення про ситуацію в країні [24]. Робота з ветеранами та їхніми родинами потребує особливої професійної уваги до інформаційно-психологічного виміру, що включає не лише медичну та соціальну реабілітацію, а й всебічну допомогу у поверненні до мирного життя, подоланні травматичного досвіду, адаптації до нових суспільних реалій [22]. Інформаційна війна, розгорнута РФ після початку повномасштабного вторгнення, є системним багатовимірним інструментом впливу, спрямованим на формування спотвореного образу реальності та досягнення комплексних політичних, військових і соціальних цілей агресора. Основна стратегічна мета російської пропаганди полягає у тотальному підриві моральної стійкості українського суспільства, системному послабленні міжнародної підтримки України, легітимації агресивних дій перед міжнародною спільнотою та

42

виправданні війни перед власним населенням через конструювання альтернативної реальності. Інформаційна стратегія ворога має виражений адаптивний характер і динамічно змінюється залежно від специфіки цільової аудиторії: для внутрішнього споживача послідовно формується образ росії як країни, що змушена оборонятися від західної агресії, для міжнародної аудиторії конструюється ілюзія локального збройного конфлікту на території України без визнання факту державної агресії. Протидія цим багаторівневим процесам вимагає комплексної системної державної політики, масового розвитку медіаграмотності населення, принципового посилення стратегічних комунікацій та тісної координації зусиль із міжнародними партнерами на всіх рівнях.

2.2. Основні цілі та наративи російської пропаганди у період повномасштабного вторгнення

Повномасштабна фаза інформаційної війни після 24 лютого 2022 року

характеризується принципово новими якісними параметрами. Інтенсивність інформаційних атак зросла в рази порівняно з періодом 2014-2021 років, спектр використовуваних інструментів розширився від традиційних державних медіа до складних мереж координованих ботів, фейкових акаунтів та псевдонезалежних медіа-ресурсів, посилилася міжвідомча координація пропагандистських зусиль на стратегічному, операційному та тактичному рівнях [6]. Власний аналіз динаміки інформаційної агресії показує еволюцію від відносно локальних інформаційних операцій 2014 року, що були географічно та тематично обмежені регіоном Донбасу та Криму, до тотальної інформаційної війни на всіх можливих фронтах одночасно: внутрішньоукраїнському, міжнародному західному та незахідному, економічному, соціальному та гуманітарному, психологічному, енергетичному. Ця багатовимірність та одночасність впливу є характерною рисою сучасного етапу інформаційної агресії.

Системний аналіз російської інформаційної кампанії дозволяє виокремити декілька стратегічних напрямів впливу, кожен з яких має специфічні цілі,

43

інструменти та очікувані наслідки. Політичний напрям спрямований на підрив довіри до української влади через поширення фейків про корупцію, персональні атаки на політичних лідерів та систематичну дискредитацію державних інституцій з метою зниження рівня суспільної підтримки та послаблення національної єдності. Військовий напрям реалізується через маніпуляції інформацією про втрати обох сторін, вигадані успіхи російських військ, спотворення фактів про перебіг бойових дій для створення паніки серед населення та деморалізації військовослужбовців.

Міжнародний напрям використовує кампанії в іноземних медіа, меседжі про загрозу ескалації конфлікту та наслідки санкційної кризи для формування сумнівів щодо доцільності надання допомоги Україні. Економічний напрям поширює фейки про дефолт, девальвацію гривні та економічний крах для провокування панічних настроїв та відтоку капіталу. Соціально-гуманітарний напрям експлуатує теми внутрішньо переселених осіб, мовне питання та

культурні відмінності для послаблення соціальної згуртованості. Енергетичний напрям використовує перебільшення масштабів руйнувань критичної інфраструктури та фейки про нестачу енергоресурсів для зростання невдоволення владою. Психологічний напрям застосовує страх, апеляції до історичних травм та експлуатацію тривоги для зниження стійкості суспільства до стресу [1, 11, 20, 51].

Психологічний вимір інформаційної війни заслуговує окремого розгляду, оскільки саме він визначає ефективність впливу на цільову аудиторію. Російська інформаційна машина використовує весь спектр психологічних методів маніпулювання свідомістю: емоційне зараження через резонансні образи та відео, формування когнітивних упереджень шляхом постійного повторення певних наративів, систематичну експлуатацію базових страхів та тривог населення, створення ефекту спіралі мовчання через імітацію масової підтримки певних позицій, поляризацію суспільних думок для розколу спільноти на ворогуючі групи [22]. Особлива увага приділяється формуванню відчуття

44

безпорадності та неминучості поразки, що має паралізувати волю до опору як серед військовослужбовців, так і серед цивільного населення. Ця психологічна складова інформаційної війни є критично важливою для розуміння механізмів впливу та розробки ефективних заходів протидії.

Маніпулювання історичною пам'яттю є потужним психологічним інструментом російської пропаганди. Систематичне переписування історії, фальсифікація історичних фактів, створення альтернативних історичних наративів, що мають обґрунтувати територіальні претензії до України та заперечити українську ідентичність як самостійну національну спільноту, дозволяє апелювати до глибинних емоційних пластів та формувати довгострокові переконання, що важко піддаються раціональній критиці. Використання історичної тематики особливо ефективне для внутрішньої російської аудиторії, яка виховувалася на радянських та пострадянських історичних міфах про «братні народи» та єдину історичну долю.

Метод інформаційного затоплення є однією з найбільш ефективних тактик російської пропаганди в умовах цифрової епохи. Створення величезної кількості взаємовиключних та суперечливих повідомлень про одну й ту саму подію унеможливорює критичне осмислення інформації пересічним споживачем. Коли людина стикається з десятками різних версій однієї події протягом короткого часу, вона втрачає здатність відрізнити правду від брехні та схильна відмовитися від спроб розібратися у ситуації самотійно. Результатом такого інформаційного перевантаження стає інформаційна апатія, зростання недовіри до всіх джерел інформації без винятку, включаючи достовірні та перевірені, та формування нігілістичного ставлення до можливості об'єктивного пізнання реальності. Ця тактика особливо ефективна у цифрову епоху, коли швидкість поширення інформації у багато разів перевищує можливості її верифікації та критичного аналізу. Власний аналіз свідчить, що метод затоплення трансформує інформаційний простір з арени конкуренції ідей та фактів у хаотичне середовище, де неможливо встановити істину, що є стратегічною метою

45

агресора. Організаційна структура російської інформаційної війни характеризується високим рівнем ієрархічної координації та централізації управління. Функціонування інформаційної кампанії реалізується на трьох рівнях. Стратегічний рівень передбачає визначення загальних напрямів та пріоритетів політичним керівництвом держави, координацію зусиль здійснює Адміністрація Президента російської федерації. Операційний рівень включає діяльність спеціалізованих підрозділів спецслужб, зокрема Головного розвідувального управління та Федеральної служби безпеки, що відповідають за планування та проведення конкретних інформаційних операцій різного масштабу та спрямування. Тактичний рівень охоплює широку мережу виконавців: державні медіа-холдинги, тролінгові фабрики, хакерські групи, координовані мережі блогерів та активістів у соціальних мережах, псевдонезалежні медіа-ресурси [19]. Така багаторівнева ієрархічна структура забезпечує ефективну координацію дій різних суб'єктів інформаційного впливу,

швидке реагування на зміни ситуації та масштабне охоплення цільових аудиторій у різних країнах та регіонах світу.

Систематична дискредитація української державності, політичних інститутів та керівництва країни є одним з пріоритетних напрямів російської інформаційної агресії. Інформаційні атаки спрямовані на підрив легітимності української влади в очах власного населення та міжнародної спільноти через поширення фейків про системну корупцію, неефективне управління, зраду національних інтересів [11]. Персоналізовані атаки на українських політичних лідерів включають створення фейкових біографій, поширення неперевіраних інсинуацій про особисте збагачення, фабрикування компрометуючих матеріалів. Метою цих атак є не стільки досягнення конкретних юридичних наслідків, скільки формування стійкого негативного образу та тотальний підрив довіри населення до керівництва держави. Ця тактика є частиною ширшої стратегії гібридної війни, де інформаційна дискредитація синхронізується з економічним тиском, дипломатичним протистоянням та підтримкою деструктивних рухів

46

[49]. Етнічна та мовна тематика традиційно використовується російською пропагандою як інструмент розколу українського суспільства. Маніпулювання мовним питанням залишається важливим елементом російської інформаційної стратегії навіть в умовах повномасштабної збройної агресії [2].

Пропаганда послідовно намагається представити Україну як штучне державне утворення, що механічно об'єднує несумісні регіони з принципово різною ідентичністю та геополітичними орієнтаціями. Активно поширюються наративи про утиск російськомовного населення, примусову українізацію, мовні репресії з боку української влади. Метою цих наративів є створення враження глибокого внутрішнього конфлікту в Україні та виправдання російського збройного втручання як захисту співвітчизників від дискримінації. Паралельно російська інформаційна машина системно намагається заперечити саме існування української нації як окремої етнічної та культурної спільноти, просуваючи концепції про єдиний народ, один народ у трьох державах, єдину

цивілізацію російського мира. Подібні історичні та етнокультурні конструкції мають створити ідеологічну базу для обґрунтування територіальних претензій та повного заперечення права України на суверенне існування як незалежної держави.

Поширення дезінформації про перебіг військових дій є критично важливою складовою російської інформаційної війни, оскільки безпосередньо впливає на моральний дух як військовослужбовців, так і цивільного населення. Серед найпоширеніших типів військових фейків можна виокремити систематичне перебільшення російських успіхів на полі бою, послідовне применшення власних втрат особового складу та техніки, регулярні звинувачення України у провокаціях та військових злочинах, фабрикування історій про масову здачу в полон українських військовослужбовців [45]. Водночас документально підтверджені численні російські військові злочини або категорично заперечуються, або представляються як постановки та провокації української сторони. Таким чином створюється паралельна інформаційна

47

реальність, де агресор представляється невинною жертвою обставин та захисником мирного населення, а реальна жертва агресії звинувачується у всіх злочинах та порушеннях міжнародного гуманітарного права. Фальсифікація інформації про військові дії має декілька стратегічних цілей: деморалізація українського суспільства та військовослужбовців, формування образу переможної російської армії для внутрішньої аудиторії, виправдання агресії перед міжнародною спільнотою [34].

Міжнародна аудиторія є пріоритетною ціллю російської інформаційної війни, оскільки від позиції міжнародної спільноти значною мірою залежить обсяг військової, фінансової та гуманітарної допомоги Україні. Противник витрачає колосальні ресурси на формування сприятливого образу у західних країнах та країнах глобального Півдня [5]. Для західної аудиторії російська пропаганда активно використовує наративи про загрозу третьої світової війни як наслідку підтримки України, ядерний шантаж та залякування можливою

ескалацією конфлікту, акцентування на економічних наслідках санкцій проти росії та витратах на підтримку України для бюджетів західних країн. Просуваються тези про необхідність реалістичної політики, врахування законних інтересів безпеки російської федерації, небезпеку ескалації конфлікту у разі надання Україні сучасних видів озброєння. Метою цієї багатовекторної кампанії є послаблення згуртованості західної коаліції підтримки України та створення передумов для поступового зняття економічних санкцій проти російської федерації. Європейський Союз надав Україні значну допомогу у різних формах [26], проте російська пропаганда системно намагається дискредитувати цю допомогу, представляючи її як марнотратство коштів європейських платників податків, збагачення корумпованих українських чиновників, штучне затягування конфлікту замість досягнення справедливого миру. Активно поширюються фейки про нецільове використання західної військової допомоги, продаж зброї на чорному ринку терористичним організаціям, розкрадання гуманітарних вантажів.

48

Для аудиторії країн глобального Півдня російська пропаганда використовує принципово інший набір наративів та аргументів. Активно експлуатується антизахідна риторика, історичні звинувачення колишніх метрополій у колоніалізмі та експлуатації, представлення конфлікту не як російської агресії проти України, а як опосередкованого протистояння між колективним Заходом та росією як альтернативним центром сили. Просуваються наративи про західні подвійні стандарти у питаннях міжнародного права, систематичне ігнорування інтересів незахідних країн глобальною елітою, використання України західними країнами як інструменту стримування росії та ослаблення її геополітичних позицій. Тема розширення НАТО та посилення військової присутності альянсу на східних кордонах активно використовується для виправдання агресії проти України як превентивної оборонної операції [73].

Економічна складова інформаційної війни російської федерації проти України спрямована на підриз довіри до стабільності української економіки,

залякування потенційних інвесторів, провокування фінансової паніки серед населення та бізнесу. Інформаційна кампанія активно намагається перекласти відповідальність за глобальну продовольчу кризу, спричинену блокадою українських портів та знищенням сільськогосподарської інфраструктури, на Україну та західні санкції проти російської федерації [1]. Виокремлюються декілька напрямів економічної дезінформації: систематичне перебільшення масштабів руйнувань української економічної інфраструктури, песимістичні прогнози щодо можливостей постконфліктного економічного відновлення, звинувачення української влади у неефективному та корумпованому управлінні економікою в екстремальних умовах війни, цілеспрямоване поширення паніки щодо неминучого державного дефолту та катастрофічної девальвації національної валюти [21]. Інформаційна війна значно посилює об'єктивні економічні виклики воєнного часу та створює додаткові штучні ризики через маніпулювання очікуваннями економічних агентів [3]. Поширення фейкової та маніпулятивної інформації про реальний стан української економіки може

49

спровокувати цілком реальні негативні економічні наслідки через відтік капіталу з країни, різке зниження обсягів прямих іноземних інвестицій, втрату традиційних ринків збуту для української продукції.

Інформаційна війна російської федерації проти України є цілеспрямованим і системним явищем, що органічно поєднує політичні, психологічні, технологічні та економічні інструменти інформаційного впливу. Вона стала невід'ємною складовою комплексної гібридної агресії, стратегічно спрямованої на тотальний підриг основ української державності, масову деморалізацію суспільства та створення максимально сприятливого інформаційного середовища для реалізації довгострокових геополітичних та військових цілей агресора. Стратегічна мета російської інформаційної війни полягає не просто у ситуативному спотворенні окремих фактів, а у системному конструюванні цілісної альтернативної реальності, де агресор послідовно подається як захисник справедливості та міжнародного права, а реальна жертва збройної агресії

трансформується у головну загрозу регіональній та глобальній безпеці.

2.3. Пропагандистські платформи рф та їх вплив на інформаційний український простір

Інформаційна війна російської федерації проти України реалізується через комплексну систему пропагандистських платформ, що охоплюють практично всі сегменти медіапростору [4]. Ворожа пропагандистська машина функціонує як багаторівнева система з координацією різних структур за єдиним планом [11]. Виокремлюються три основні рівні організації: офіційні державні медіа, напівофіційні псевдонезалежні видання та мережа інтернет-ресурсів з блогерами, формально не пов'язаними з державою [12]. Аналіз специфіки функціонування пропагандистських платформ свідчить про їхню технологічну досконалість та адаптивність до змін медіаландшафту.

Телебачення, попри цифровізацію, залишається ключовим каналом впливу на старше покоління через систематичну трансляцію емоційно забарвленого

50

контенту, де факти замінюються інтерпретаціями [5, 6]. Ток-шоу та новинні програми використовують єдину методологію подачі матеріалу з залученням псевдоекспертів для створення ілюзії об'єктивності. Власний аналіз показує, що телевізійний формат дозволяє найефективніше впливати на емоційний стан аудиторії через поєднання візуальних образів, драматичного монтажу та риторичних прийомів. Цифрові платформи суттєво розширили арсенал пропагандистських інструментів. Створена розгалужена мережа веб-сайтів, що професійно імітують незалежні медіа, аналітичні центри або навіть академічні інституції [12, 38]. Використовуються домени, схожі на відомі українські видання, що дезорієнтує необережну аудиторію. Виокремлюються функціональні категорії: прямі онлайн-копії державних медіа, псевдоаналітичні центри з вбудованою пропагандою, розважальні портали з маніпулятивними вставками. Така диверсифікація дозволяє охопити різні сегменти аудиторії з відмінними медійними звичками. Соціальні мережі перетворилися на критично

важливу платформу завдяки вірусному поширенню інформації та можливості точного таргетування [71]. Створена масштабна мережа координованих фейкових акаунтів, що систематично експлуатують теми регіональних відмінностей, мовного питання, релігійних розбіжностей, соціальної нерівності для підриву національної єдності. Силові структури росії демонструють високу адаптивність, оперативно змінюючи тактику на протидію через складні схеми перенаправлення трафіку, зміну доменів, створення дзеркальних сайтів [49].

Економічний вимір пропаганди заслуговує окремої уваги, оскільки спрямований на реальне завдання матеріальної шкоди через підрив інвестиційного клімату [8, 73]. Систематичне поширення фейків про фінансову нестабільність, ризики для інвесторів, проблеми підприємств негативно впливає на макроекономічні процеси та відлякує потенційний капітал. Власний аналіз свідчить, що економічна дезінформація має подвійний ефект: безпосередній через провокування панічних настроїв та опосередкований через формування негативних очікувань бізнес-спільноти. Культурно-гуманітарна сфера зазнає

51

впливу через систематичне спотворення історичних фактів, заперечення української ідентичності, нав'язування наративів про спільну історію [42]. Пропагандистські платформи атакують українську культуру на міжнародній арені, намагаючись делегітимізувати її визнання та привласнити видатних діячів. Псевдонаукові платформи створюють ілюзію академічної легітимації агресії через публікацію історичних та культурологічних конструкцій, що представляють війну як історичну необхідність [18]. Такі матеріали спрямовані на інтелектуальну еліту для створення видимості наукового консенсусу.

Критично важливою особливістю є синхронізація пропагандистських операцій з військовими діями [19]. Платформи різко активізуються напередодні наступів, масово поширюючи дезінформацію про фронт, завищуючи власні успіхи, применшуючи втрати. Одночасно транслюється маніпулятивна інформація про катастрофічні втрати українських військ. Поширюються фейки про погане ставлення військових до цивільних, мародерство, порушення прав

для підриву довіри між суспільством та армією [28]. Дезінформація про утримання військовополонених звинувачує Україну у порушенні Женевських конвенцій, приховуючи злочини російських військових [20]. Історична політика перетворюється на інструмент пропаганди через нав'язування спотвореної версії минулого, де СРСР представлений виключно як визволитель, а злочини режиму табууються [33]. Така інтерпретація обґрунтовує агресію як продовження боротьби проти фашизму. Сучасна система пропаганди органічно успадкувала репресивні методи часів СРСР, адаптувавши їх до цифрових можливостей [39].

Технологічні інновації радикально розширили можливості інформаційної війни. Впровадження штучного інтелекту, ботів, автоматичних систем генерації текстів, дипфейків та синтетичних медіа дозволяє створювати колосальні обсяги контенту за короткий час, імітувати масову підтримку, ускладнювати виявлення джерел дезінформації [45]. Посилення ролі візуального контенту обумовлене його привабливістю та вірусним поширенням, водночас він складніше піддається оперативній верифікації [34]. Трансформація медіаспоживання,

52

зокрема перехід до ультракоротких відео, змусила пропаганду освоювати нові платформи, створюючи контент, що відповідає їхнім алгоритмам просування. Протидія вимагає багаторівневого підходу. Міжнародна співпраця є критично важливою, оскільки російські платформи працюють на різноманітні аудиторії [26]. Спільні зусилля з партнерами дозволяють ефективніше виявляти та блокувати кампанії на ранніх стадіях. Пропаганда часто перетворюється на психологічний тероризм, що вимагає не лише технічних заходів, а й професійної психологічної підтримки постраждалих [47]. Молодь є особливо вразливою через інтенсивне користування соціальними мережами, що актуалізує систематичну роботу в освітніх закладах з розвитку критичного мислення та медіаграмотності [41].

Правове регулювання має забезпечувати баланс між свободою слова та національною безпекою [23, 29]. Юридична кваліфікація пропаганди є складним завданням через необхідність чітких критеріїв відмежування від легітимної

журналістики. Технічні та юридичні складнощі боротьби у цифровому середовищі обумовлені швидкістю поширення інформації, анонімністю користувачів, транскордонним характером інтернету [9]. Правоохоронні органи відіграють важливу роль через виявлення та притягнення до відповідальності осіб, що займаються розповсюдженням дезінформації [32]. Міжнародний досвід демонструє тісний зв'язок інформаційної та економічної безпеки, оскільки пропагандистські кампанії спрямовані на підрив економічної стабільності [43].

Пропагандистські платформи росії становлять високоорганізовану систему багаторівневого впливу, що характеризується складною структурою, стратегічною координацією, технологічною досконалістю та високою адаптивністю. Пропаганда росії системно охоплює традиційні медіа, інтернет ресурси, соціальні мережі, активно використовує штучний інтелект та автоматизацію. Вплив на український простір є багатовимірним та охоплює політичну, економічну, культурну, психологічну сфери. Системний характер

53

кампаній та їхня координація з військовими діями свідчать про стратегічне значення інформаційної війни у загальній агресії проти України.

Висновки до розділу 2

Дослідження основних характеристик інформаційної війни рф в просторі України дозволяє сформулювати декілька важливих висновків. Інформаційна війна є невід'ємною складовою гібридної агресії росії проти України, що має глибоке історичне коріння та характеризується систематичністю, масштабністю, використанням широкого спектра методів та інструментів впливу. Інформаційна стратегія росії спрямована на досягнення декількох взаємопов'язаних цілей: дискредитацію української державності та політичного керівництва, підрив міжнародної підтримки України, посів паніки та дефетизму серед українського населення, виправдання власної агресії та військових злочинів, формування альтернативної реальності для внутрішньої російської та міжнародної аудиторії. Технологічний арсенал російської інформаційної війни включає соціальні

мережі, месенджери, ботоферми, кібератаки, псевдонезалежні медіа-ресурси. Психологічний вимір інформаційного впливу використовує маніпулювання емоціями, когнітивні упередження, історичну пам'ять, створення інформаційного хаосу. Організаційна структура російської інформаційної агресії характеризується високим рівнем централізації та координації між різними державними та квазідержавними структурами. Основні напрями інформаційних атак охоплюють політичну, економічну, соціальну, культурну сфери. Україна поступово розбудовує систему протидії інформаційній агресії, що включає інституційні механізми, програми медіаграмотності, підтримку незалежних медіа та фактчекінгу, розвиток стратегічних комунікацій. Міжнародна співпраця, координація зусиль демократичних країн, залучення технологічних компаній є критично важливими для ефективної протидії транснаціональним інформаційним загрозам.

54

РОЗДІЛ 3. ПЕРСПЕКТИВИ ВПРОВАДЖЕННЯ РЕКОМЕНДАЦІЙ ЩОДО ІНСТРУМЕНТІВ ІНФОРМАЦІЙНОЇ ВІЙНИ РФ В УКРАЇНІ

3.1. Інформаційно-психологічні та кібероперації як інструменти стратегічного впливу російської федерації

Інформаційно-психологічні операції російської федерації проти України становлять комплексну систему заходів, спрямованих на деформацію суспільної свідомості, підриг довіри до державних інституцій та дестабілізацію внутрішньополітичної ситуації. Стратегія психологічного впливу росії базується на створенні альтернативної реальності, де факти замінюються емоційно забарвленими інтерпретаціями [44]. Виокремлюються пріоритетні напрями: формування образу України як держави, позбавленої суверенітету та контрольованої зовнішніми суб'єктами [19]. Спостерігається синергетичне поєднання психологічних операцій з військовими діями, що посилює деморалізуючий ефект [12]. Використовуються складні алгоритми таргетування для адресації специфічних меседжів різним соціальним групам залежно від їхніх

психологічних особливостей [6]. Психологічні операції характеризуються чіткою періодичністю, що корелює з військовими подіями та міжнародними процесами [45]. На сучасному етапі спостерігається використання штучного інтелекту для генерації контенту та автоматизації поширення дезінформації [11]. Психологічна стратегія базується на історичних маніпуляціях для делегітимізації української державності [17, 33]. Наукове середовище всередині росії перетворилося на інструмент пропаганди, продукуючи псевдонаукові дослідження [18]. Виявлення психологічних операцій ускладнюється через децентралізованість та використання легітимних каналів комунікації [26].

Існує правовий вакуум, що ускладнює протидію у цифровому просторі [9, 23, 29]. Студентська аудиторія є пріоритетною ціллю через високу активність у цифровому просторі [41]. Захист особистості вимагає розвитку індивідуальної медіаграмотності та психологічної стійкості [13]. Кібероперації становлять

55

технологічний фундамент інформаційної війни через дестабілізацію критичної інфраструктури [75]. Кіберактаки координуються з інформаційно психологічними операціями, створюючи синергетичний ефект [21]. Кіберзагрози впливають на бізнес-процеси і загальну економічну ситуацію [8, 54]. Ефективна протидія вимагає інтегрованого підходу та міжнародної координації [62, 69, 70].

Аналіз механізмів інформаційно-психологічного впливу свідчить про стратегічну трансформацію російських операцій від локальних маніпуляцій до системної кампанії з деморалізації українського суспільства. Ключовою особливістю сучасного етапу є синхронізація психологічних операцій з кінетичними ударами, що створює ефект подвійного стресу для населення. Координація інформаційних атак з військовими діями на фронті посилює деморалізуючий вплив через формування атмосфери тотальної невизначеності й безперервного страху [12]. На основі аналізу літератури, ми можемо стверджувати, що інформаційно-психологічний тиск має циклічний характер з передбачуваними піками активності, які передують або супроводжують значні військові операції. Наприклад, напередодні наступу на Харківщину у вересні

2022 року різко активізувалися кампанії з поширення чуток про масові евакуації, можливе використання тактичної ядерної зброї, неминучий економічний колапс. Ці синхронізовані дії мали на меті створити паніку серед цивільного населення та підірвати довіру до здатності держави захистити громадян.

Технологічна досконалість сучасних психологічних операцій проявляється у використанні складних алгоритмів таргетування, що дозволяють адресувати персоналізовані меседжі різним соціальним групам залежно від їхніх демографічних характеристик, політичних переконань, емоційних станів та психологічних вразливостей [6]. Маніпулювання базовими емоціями, зокрема страхом, невизначеністю та втомою від тривалого конфлікту, є центральним елементом російської стратегії. Аналіз контенту російських пропагандистських каналів демонструє систематичне використання апокаліптичних наративів про неминучість поразки, марність опору, зраду союзників, економічний крах. Ці

56

повідомлення розраховані на виснаження психологічних ресурсів опору суспільства через постійне підтримування високого рівня тривожності.

Маніпулювання історичною пам'яттю служить довгостроковим інструментом психологічного впливу через конструювання наративу про спільне минулого та спільну долю українського й російського народів [33]. Систематичне спотворення історичних фактів, особливо подій Другої світової війни, використовується для створення псевдоісторичного підґрунтя територіальних претензій та виправдання сучасної агресії як продовження героїчної боротьби проти фашизму. Делегітимізація української державності через наративи про штучність української нації розрахована на формування у міжнародній аудиторії сприйняття конфлікту як внутрішньої справи слов'янських народів [17].

Власний аналіз свідчить, що історичні маніпуляції особливо ефективні для впливу на старше покоління, виховане на радянських історичних міфах, та на західну аудиторію з обмеженими знаннями про регіональну специфіку.

Псевдонаукова легітимізація агресії через російське академічне середовище створює інтелектуальне підґрунтя для психологічних операцій [18]. Публікація

псевдонаукових праць, що обґрунтовують історичну необхідність або цивілізаційну місію війни, спрямована на інтелектуальну еліту та має створити видимість наукового консенсусу.

Ці матеріали активно використовуються пропагандистськими медіа для надання ілюзії об'єктивності та раціональності агресивній політиці. Конкретним прикладом є масова публікація у російських наукових виданнях статей про «денацифікацію» України, що представляють збройну агресію як антифашистську операцію. Подібні псевдонаукові конструкції тиражуються через освітню систему російської федерації, формуючи покоління з деформованим сприйняттям реальності.

Виявлення та нейтралізація російських психологічних операцій ускладнюється через їхню децентралізованість та професійне використання легітимних каналів комунікації [26]. На відміну від традиційної пропаганди з

57

очевидними державними джерелами, сучасні операції реалізуються через мережу формально незалежних акторів: блогерів, лідерів думок, псевдоаналітичних центрів, громадських організацій. Це створює ілюзію органічної суспільної дискусії, де деструктивні наративи поширюються нібито природним шляхом. Правовий вакуум у регулюванні цифрового простору додатково ускладнює ефективну протидію [9]. Відсутність чіткої правової кваліфікації інформаційних атак, недосконалість механізмів притягнення до відповідальності, транскордонний характер загроз створюють сприятливі умови для безкарного поширення деструктивного контенту.

Технологічний вимір протидії передбачає застосування систем автоматичного моніторингу, аналізу контенту, виявлення аномальної активності та координованих кампаній [29]. Організаційний аспект вимагає координації зусиль державних органів, незалежних медіа, громадянського суспільства та міжнародних партнерів. Правовий складник охоплює вдосконалення законодавства у сфері інформаційної безпеки та адаптацію правових механізмів до специфіки цифрового середовища [23]. Студентська аудиторія потребує

особливої уваги через високу активність в Інтернеті, відкритість до нових ідей та потенціал впливу на майбутні суспільні процеси [41]. Розвиток критичного мислення, медіаграмотності та навичок верифікації інформації у освітніх закладах формує довгострокову стійкість суспільства до маніпулятивних технологій. Захист особистості від інформаційно-психологічного впливу вимагає комплексного підходу, що поєднує індивідуальну медіаграмотність, критичне мислення та психологічну резильєнтність [13].

Кібероперації російської федерації становлять технологічний фундамент інформаційної війни, забезпечуючи дестабілізацію критичної інфраструктури, викрадення конфіденційної інформації та порушення функціонування життєво важливих державних систем. Встановлено системність та скоординованість кібератак з військовими діями, що свідчить про їхню інтеграцію у загальну стратегію гібридної війни [75]. Суттєву небезпеку становлять цілеспрямовані

58

атаки на енергетичну інфраструктуру, фінансові системи, транспортні мережі, урядові канали зв'язку та системи критичного забезпечення. Власний аналіз свідчить, що російські кібероперації мають чітку стратегічну мету: не лише завдати технічної шкоди, а й посилити психологічний ефект через демонстрацію вразливості критичної інфраструктури. Наприклад, масовані кібератаки на енергосистему України взимку 2022-2023 років були синхронізовані з ракетними ударами по енергетичних об'єктах, створюючи кумулятивний ефект через одночасне фізичне руйнування та цифрову дестабілізацію.

Сучасні кібероперації передбачають використання вразливостей програмного забезпечення, експлуатацію людського фактору через методи соціальної інженерії, впровадження шкідливого коду в ланцюги постачання технологічних продуктів [38]. Технологічна складність атак постійно зростає через використання передових методів обходу систем захисту, шифрування шкідливого трафіку, маскуванню під легітимну активність. Кібертероризм як окрема категорія загроз передбачає використання цифрових технологій не лише для технічної шкоди, а й для масового поширення страху та дестабілізації

суспільної психології [47]. Фахівці з росії застосовують такі методи для підриву довіри до здатності держави захистити критичну інфраструктуру та особисті дані громадян. Інтеграція кібероперацій у загальну стратегію гібридної війни проявляється у координації з інформаційно-психологічними операціями, військовими діями та дипломатичним тиском, що створює синергетичний ефект та посилює загальний деструктивний вплив [21]. Кіберактаки часто супроводжуються інформаційними кампаніями з перебільшення їхніх наслідків, поширення паніки, звинувачення української сторони у неготовності захистити населення. Економічний вимір кіберзагроз виходить за межі суто технічних проблем безпеки та безпосередньо впливає на бізнес-процеси, фінансову стабільність підприємств, інвестиційний клімат та загальну макроекономічну ситуацію [8]. Систематичні кібератаки на фінансовий сектор, банківські системи,

59

платіжні інфраструктури спрямовані на підрив довіри до фінансових інституцій та провокування економічної паніки серед населення.

Ефективна протидія кіберзагрозам вимагає інтегрованого підходу, що охоплює технологічні засоби захисту, організаційні процедури, систематичне навчання персоналу та координацію з державними органами безпеки [54]. Превентивні заходи включають регулярний аудит безпеки, оновлення програмного забезпечення, сегментацію мереж, резервування критичних даних. Оперативне реагування на інциденти вимагає наявності кваліфікованих команд реагування, чітких протоколів дій, технічних засобів виявлення та нейтралізації загроз. Стратегічне планування розвитку систем захисту має враховувати еволюцію загроз, впровадження нових технологій, підготовку спеціалістів відповідної кваліфікації. Концептуальна модель інформаційної безпеки враховує специфіку сучасних кіберзагроз та включає технічні, організаційні, правові та психологічні компоненти з обґрунтуванням взаємозв'язку різних рівнів від індивідуального до національного та міжнародного [62].

Трансформація загроз національній безпеці в цифрову епоху вимагає адаптації системи стратегічного планування до нових викликів через

довгострокове планування розвитку технологій, підготовку висококваліфікованих кадрів, міжнародну співпрацю та системне зміцнення цифрової стійкості [69]. Транснаціональний характер кіберзагроз актуалізує необхідність міжнародної координації зусиль для ефективної протидії російським кіберактам [70]. Глобалізація цифрового простору створює додаткові можливості для безкарної кіберагресії через експлуатацію юрисдикційних розривів, водночас відкриваючи перспективи для міжнародного співробітництва у сфері кібербезпеки, обміну інформацією про загрози, спільної розробки стандартів захисту.

Інформаційно-психологічні та кібероперації російської федерації становлять інтегровану систему стратегічного впливу, що органічно поєднує технологічні можливості цифрової епохи з традиційними методами пропаганди

60

та психологічного тиску. Синергетичний ефект від одночасного застосування психологічних маніпуляцій та кібератак значно посилює загальний деструктивний вплив на українське суспільство та державні інституції. Ефективна протидія російським загрозам вимагає комплексного багаторівневого підходу, що охоплює технологічне зміцнення кібербезпеки критичної інфраструктури, масовий розвиток медіаграмотності населення, системне вдосконалення правової бази, активну міжнародну співпрацю та стратегічне довгострокове планування розвитку цифрової оборони. Критичного значення набуває координація зусиль державних органів різного профілю, приватного технологічного сектору, активного громадянського суспільства та міжнародних партнерів для створення резильєнтної системи комплексної протидії інформаційно-психологічним та кіберзагрозам.

3.2. Вплив російських інформаційних атак у соціальних мережах та шляхи їхньої нейтралізації

Соціальні мережі перетворилися на пріоритетну арену російської інформаційної війни проти України, забезпечуючи безпрецедентні можливості

для масштабного поширення дезінформації, маніпулювання громадською думкою та формування альтернативної картини реальності [72]. Стратегія росії у цифровому середовищі відзначається багатошаровістю, високим рівнем організованості та адаптивністю до алгоритмічних і комунікаційних особливостей різних платформ, що пріоритезують емоційно забарвлений, конфліктний і контроверсійний контент [12]. Використовуються складні алгоритми таргетування для адресації специфічних меседжів різним соціальним групам залежно від їхніх соціально-демографічних характеристик, інтересів та поведінкових патернів; при цьому базові стратегії впливу включають створення розгалужених мереж фейкових акаунтів, застосування ботів для масового поширення узгодженого контенту, компрометацію реальних акаунтів і розбудову формально легітимних медіаплатформ, які імітують незалежну

61

журналістику [72]. Після початку повномасштабної агресії ці підходи були модифіковані: відбулася переорієнтація наративів на виправдання війни, дискредитацію української державності та її союзників, а також інтенсифікація присутності в міжнародному цифровому просторі [5]. Водночас Україна сформувала комплексну систему протидії, що поєднує технологічні інструменти виявлення дезінформації, організаційні механізми взаємодії державних і недержавних акторів, цілеспрямовану комунікаційну політику та розгортання міжнародних партнерств у сфері інформаційної безпеки [4, 26].

Соціальні мережі стали основним каналом інформаційного впливу не лише через їхню масовість і доступність, а й через надзвичайну складність централізованого контролю контенту та швидкість його поширення [19]. У цьому середовищі розгортається конкуренція наративів і боротьба за інформаційний порядок денний, де російська пропаганда системно експлуатує історичні маніпуляції, наративи про «штучність» української нації та заперечення її суб'єктності [11, 17]. Значну роль відіграють таргетовані кампанії, адаптовані до специфіки різних регіонів України, що враховують відмінності в соціально-економічному становищі, історичному досвіді та мовно-культурному

середовищі [31]. Багатовимірність цього впливу посилюється економічними й соціальними компонентами: цілеспрямоване поширення панічних наративів щодо економічної стабільності, інвестиційного клімату та соціальної злагоди сприяє формуванню негативних очікувань, підриву довіри до інститутів та загостренню внутрішніх протиріч [8, 54].

Функціонування російських інформаційних кампаній у соціальних мережах супроводжується серйозними правовими та технологічними викликами. Транснаціональний характер платформ, анонімність значної частини користувачів і розмитість юрисдикційних меж ускладнюють правове регулювання і притягнення до відповідальності організаторів і координаторів дезінформаційних операцій [9]. Додаткову загрозу створюють колосальні обсяги контенту та швидкість його ротації, що ускладнює ідентифікацію і своєчасну

62

нейтралізацію шкідливих інформаційних потоків навіть за наявності розвинених технічних засобів моніторингу [29]. За цих умов ефективна протидія можлива лише на основі скоординованих міжнародних зусиль, спільних механізмів обміну даними, узгоджених санкційних та регуляторних підходів щодо платформ і організаторів кампаній [26]. Водночас критично важливим залишається індивідуальний рівень захисту, пов'язаний із розвитком медіаграмотності, критичного мислення та навичок безпечної поведінки в цифровому середовищі; саме ці компетентності дозволяють користувачам самостійно ідентифікувати маніпулятивний і фейковий контент [13]. Особливо вразливою, але водночас потенційно найактивнішою групою є молодь, яка є пріоритетною ціллю дезінформаційних кампаній і водночас ключовим ресурсом для формування стійкості до пропаганди в довгостроковій перспективі [41]. Формування ефективної політики протидії вимагає постійного пошуку балансу між забезпеченням національної безпеки, захистом демократичних цінностей, свободою слова та правом на доступ до інформації, що визначає складність нормативно-правового та інституційного реагування на загрози, пов'язані з функціонуванням соціальних мереж у контексті війни [23].

Аналіз російської стратегії у соціальних мережах свідчить про високий рівень технологічної досконалості та стратегічної координації різних інструментів впливу. Ключовою особливістю є створення багаторівневої системи поширення дезінформації, де кожен рівень виконує специфічну функцію у загальній кампанії. Перший рівень представлений мережами фейкових акаунтів, що професійно імітують реальних користувачів через використання автентичних фотографій, детальних біографій, природної мовної поведінки [72]. Ці акаунти створюють ілюзію широкої органічної підтримки проросійських позицій, формують псевдогромадську думку та впливають на сприйняття інформаційних подій реальними користувачами через ефект соціального підтвердження. Власний аналіз показує, що фейкові акаунти часто функціонують роками, поступово набуваючи довіри аудиторії через публікацію

63

нейтрального контенту, перш ніж активізуватися для поширення дезінформації у критичні моменти. Другий рівень базується на використанні ботів та автоматизованих систем для промислового масового поширення контенту, створення штучного ажіотажу навколо потрібних тем та виведення дезінформаційних матеріалів у топові позиції соціальних платформ через маніпулювання алгоритмами ранжування. Боти здатні генерувати тисячі повідомлень за короткий час, створюючи враження масового обговорення певної теми та формуючи хибне уявлення про її актуальність та значущість.

Конкретним прикладом є координована ботова кампанія у Twitter навесні 2023 року, коли протягом декількох годин було створено понад 50 тисяч повідомлень з хештегами про нібито масове невдоволення українців політикою влади, при цьому переважна більшість акаунтів була створена протягом попередніх днів та демонструвала ознаки автоматизованої поведінки. Третій рівень передбачає компрометацію реальних акаунтів через хакерські атаки, методи соціальної інженерії або пряму купівлю облікових записів у їхніх власників [72]. Компрометовані акаунти реальних людей мають принципово вищий рівень довіри аудиторії порівняно з новоствореними профілями завдяки

наявності історії активності, мережі реальних зв'язків, попередньої репутації. Використання таких акаунтів для поширення дезінформації забезпечує значно більшу ефективність впливу, оскільки підписники сприймають повідомлення як думку знайомої людини, а не анонімного пропагандиста. Четвертий рівень полягає у створенні формально легітимних медіаплатформ, псевдоаналітичних центрів та громадських організацій, які систематично просувають проросійські позиції під професійним виглядом незалежної експертної думки з використанням термінології, статистичних даних, посилань на дослідження.

Після початку повномасштабного вторгнення російська пропаганда продемонструвала високу адаптивність, оперативно модифікувавши наративи відповідно до нових реалій [5]. Пріоритетним напрямом стало формування негативного образу України у західних соціальних мережах через систематичне

64

поширення матеріалів про нібито тотальну корупцію українського уряду, масові порушення прав людини, неефективне розкрадання міжнародної допомоги. Ці наративи розраховані на підриг міжнародної підтримки України через формування у західної аудиторії сумнівів щодо доцільності допомоги країні з нібито корумпованою владою. Власний аналіз свідчить, що російська стратегія еволюціонувала від прямих фейків, які легко спростовувалися, до більш витончених маніпуляцій, що базуються на напівправді, вирваних з контексту фактах, тенденційних інтерпретаціях реальних подій.

Україна у відповідь розробила комплексну багаторівневу систему протидії російським інформаційним атакам у соціальних мережах [4]. Технологічний компонент включає системи цілодобового моніторингу соціальних мереж, автоматичного виявлення координованих кампаній дезінформації, аналізу аномальної активності через виявлення ботів та блокування шкідливого контенту. Використовуються алгоритми машинного навчання для ідентифікації патернів поведінки, характерних для фейкових акаунтів та автоматизованих систем. Організаційний аспект передбачає стратегічну координацію зусиль державних органів різного профілю, незалежних медіа, спеціалізованих

фактчекінгових організацій, активного громадянського суспільства та міжнародних партнерів через створення міжвідомчих робочих груп та центрів стратегічних комунікацій. Комунікаційна складова включає проактивне систематичне інформування населення про поточні російські дезінформаційні кампанії, масове підвищення медіаграмотності громадян через освітні програми, формування критичного ставлення до інформації в соціальних мережах, публічні оперативні спростування найбільш резонансних фейків.

Міжнародний вимір охоплює активну співпрацю з глобальними технологічними платформами для оперативного видалення дезінформаційних матеріалів, блокування акаунтів ідентифікованих російських пропагандистів, алгоритмічної протидії поширенню шкідливого контенту через зниження його видимості у стрічках користувачів. Правовий компонент передбачає поступове

65

вдосконалення нормативної бази для забезпечення легітимних механізмів притягнення до відповідальності за поширення дезінформації та розвиток міжнародного правового співробітництва у цій сфері.

Стратегія росії у цифровому просторі базується на професійній експлуатації алгоритмічних особливостей соціальних платформ, що природним чином пріоритезують емоційно забарвлений, суперечливий, скандальний контент для максимізації залученості користувачів [12]. Силові структури цілеспрямовано створюють провокативні матеріали, що викликають сильні емоційні реакції страху, обурення, ненависті, стимулюють конфліктні дискусії та забезпечують максимальне вірусне поширення через природні механізми соціальних мереж без необхідності штучного просування.

Стратегія передбачає системну диверсифікацію каналів впливу через використання різних соціальних платформ залежно від специфіки цільової аудиторії та синхронізацію активності в цифровому просторі з подіями на фронті, міжнародними політичними процесами, економічними кризами [19]. Соціальні мережі функціонують як критична інфраструктура сучасної інформаційної війни, де безперервно відбувається інтенсивна конкуренція

конфліктних наративів, боротьба за контроль над інформаційним порядком денним, формування домінуючої громадської думки [11]. Систематичне поширення у цифровому просторі історичних маніпуляцій служить фундаментом російської пропаганди через викривлені інтерпретації історичних подій, штучні міфи про нібито спільне минуле українців та росіян, деструктивні наративи про штучність української нації та нелегітимність української державності [17]. Ці довгострокові маніпуляції розраховані на поступову зміну історичної свідомості через постійне повторення спотворених наративів. Проводяться таргетовані дезінформаційні кампанії, професійно адаптовані до культурної, мовної та історичної специфіки різних регіонів України [31]. Пропаганда систематично використовує регіональні відмінності для цілеспрямованого поглиблення внутрішніх розколів та підриву національної

66

єдності через експлуатацію реальних чи вигаданих протиріч між регіонами. Пріоритетними цілями є східні та південні регіони, де історично існували різні рівні ідентифікації з українською державністю.

Правове регулювання соціальних мереж стикається з принциповими складнощами через їхній транснаціональний характер, технологічну складність платформ та критичну необхідність балансування між забезпеченням інформаційної безпеки та збереженням фундаментальних демократичних свобод [9]. Українське законодавство потребує системної модернізації для створення ефективних механізмів протидії російським інформаційним атакам при збереженні основоположних прав громадян. Надмірні обмеження можуть призвести до порушення свободи слова, тоді як недостатнє регулювання створює сприятливі умови для безкарного поширення пропаганди [23].

Технологічні виклики ідентифікації дезінформації пов'язані з величезними щоденними обсягами контенту, блискавичною швидкістю його вірусного поширення, об'єктивною складністю відмежування навмисної дезінформації від помилкової інформації, сатири, гіперболізації або легітимного вираження суб'єктивної особистої думки [29]. Автоматизовані системи виявлення

дезінформації демонструють обмежену ефективність через складність природної мови, контекстуальні нюанси, культурні відмінності та високу здатність російських акторів швидко адаптувати технології поширення пропаганди до нових методів детекції. Транскордонний глобальний характер цифрового простору вимагає узгодженої міжнародної координації зусиль між суверенними державами, транснаціональними технологічними компаніями, активним громадянським суспільством та міжнародними організаціями для створення комплексної системи ефективної протидії дезінформації [26]. Індивідуальний рівень захисту від інформаційних атак передбачає масовий розвиток особистої медіаграмотності та критичного мислення через систематичні освітні програми [13]. Ефективна протидія вимагає не лише системних державних заходів технологічного та організаційного характеру, але й принципового підвищення

67

індивідуальної психологічної стійкості громадян до витончених маніпулятивних технологій. Молодіжна аудиторія є найбільш активною в цифровому просторі, що робить її пріоритетною ціллю російських пропагандистських кампаній та водночас потенційним стратегічним ресурсом для протидії дезінформації через формування покоління з високою медіаграмотністю [41].

Багатовекторний вплив російських інформаційних атак у соціальних мережах виходить далеко за межі суто політичної сфери та безпосередньо впливає на економічні процеси через підрив інвестиційного клімату, соціальну стабільність через провокування конфліктів, психологічний стан населення через постійний інформаційний стрес [8]. Ефективна нейтралізація російських інформаційних загроз вимагає інтегрованої стратегії, що органічно поєднує технологічні інструменти безперервного моніторингу та оперативного блокування шкідливого контенту, організаційні механізми координації різних суб'єктів протидії, комунікаційні стратегії систематичного інформування населення, правові засоби збалансованого регулювання цифрового простору [54]. Необхідна системна взаємодія державних органів, приватного технологічного сектору, громадянського суспільства та міжнародних партнерів.

Соціальні мережі залишаються критично важливою ареною російської інформаційної війни проти України, проте комплексний багаторівневий підхід до протидії створює реальні можливості для ефективної нейтралізації ворожих інформаційних атак. Першочергово необхідно масово розвивати медіаграмотність населення через освітні програми на всіх рівнях, систематично удосконалювати технологічні системи моніторингу цифрового простору, активно зміцнювати міжнародне співробітництво з технологічними платформами та партнерськими державами, створювати збалансовану правову базу, що забезпечує надійну інформаційну безпеку без непропорційного порушення фундаментальних демократичних свобод.

68

3.3. Перспективи формування цифрової оборони в Україні: стратегічні пріоритети та безпекові виклики

Повномасштабна збройна агресія російської федерації проти України актуалізувала питання формування комплексної системи цифрової оборони держави. В умовах гібридної війни, де інформаційні атаки органічно поєднуються з кіберопераціями та традиційними військовими діями, створення надійної цифрової інфраструктури безпеки стає пріоритетним завданням державної політики. Необхідність стратегічного аналізу безпекового середовища передбачає врахування як внутрішніх, так і зовнішніх загроз цифровому простору [37]. Сучасний стан цифровізації українського суспільства створює як нові можливості для розвитку, так і додаткові вразливості перед зовнішніми інформаційними впливами [13]. Захист цифрового простору вимагає розробки багаторівневої системи безпеки, що охоплює державний, корпоративний та індивідуальний рівні. Формування правової політики акцентує увагу на необхідності створення правових механізмів регулювання цифрового простору в умовах воєнного стану [16]. Впровадження технологій штучного інтелекту для аналізу великих масивів даних дозволить своєчасно ідентифікувати потенційні загрози [38]. Організаційна структура має базуватися на принципах міжвідомчої

взаємодії та чіткого розподілу повноважень [23]. Кадрове забезпечення становить один із найбільших викликів через необхідність підготовки фахівців у галузі кібербезпеки [22]. Правове забезпечення вимагає створення комплексної нормативної бази на основі конституційних принципів [24].

Міжнародне співробітництво відкриває додаткові можливості через участь у європейських ініціативах [17, 64]. Технологічні виклики пов'язані з необхідністю забезпечення стійкості критичної інфраструктури [66]. Соціальний вимір передбачає підвищення рівня цифрової грамотності населення [9]. Система моніторингу та аналітики має стати важливим елементом оборони [19]. Протидія вимагає формування стратегічної комунікації держави [21]. Захист

69

державних установ потребує багаторівневої системи безпеки [7]. Розвиток вітчизняної індустрії кібербезпеки має стати напрямом економічної політики [75]. Технологічне партнерство з країнами НАТО відкриває доступ до передових розробок [2]. Інтеграція систем потребує створення єдиного координаційного центру [58]. Довгострокова стійкість залежить від здатності створити самодостатню екосистему [70]. Соціально-психологічна стійкість має підтримуватися через освіту та виховання [44]. Перспективи визначаються внутрішніми зусиллями та міжнародною підтримкою [1, 51, 65].

Аналіз стратегічних пріоритетів формування цифрової оборони України свідчить про необхідність комплексного підходу, що інтегрує технологічні, організаційні, правові, кадрові та соціальні виміри у єдину систему національної безпеки. Специфіка сучасних інформаційних загроз вимагає переосмислення традиційних підходів до безпеки та створення принципово нової архітектури захисту, адаптованої до реалій цифрової епохи та характеру російської гібридної агресії. Зростання цифрової присутності громадян у мережі Інтернет закономірно супроводжується експоненційним розширенням каналів поширення деструктивної інформації, що створює якісно нові виклики для системи національної безпеки [13]. Власний аналіз показує, що цифровізація суспільства має амбівалентний характер: з одного боку, вона відкриває безпрецедентні

можливості для економічного розвитку, ефективного державного управління, соціальної мобілізації, а з іншого – створює додаткові поверхні атаки для ворожих інформаційних операцій та кібератак.

Технологічна складова цифрової оборони передбачає впровадження сучасних інтегрованих систем виявлення та оперативної нейтралізації кіберзагроз на всіх рівнях цифрової інфраструктури [38]. Створення автоматизованих систем безперервного моніторингу цифрового простору з використанням алгоритмів машинного навчання та технологій штучного інтелекту дозволить аналізувати величезні масиви даних в режимі реального часу, своєчасно ідентифікувати аномальні патерни активності, прогнозувати

70

потенційні загрози та автоматично координувати заходи реагування. Власний аналіз свідчить, що ефективність цих систем критично залежить від якості навчальних даних, адаптивності алгоритмів до еволюції загроз та здатності мінімізувати хибні спрацювання, що можуть перевантажити операторів та знизити довіру до системи. Конкретним прикладом успішного впровадження таких технологій є створення українською ІТ-індустрією системи моніторингу соціальних мереж, яка автоматично виявляє координовані кампанії дезінформації через аналіз патернів публікацій, мережевих зв'язків між акаунтами, лінгвістичних маркерів та часових характеристик активності.

Організаційна архітектура цифрової оборони має базуватися на принципах стратегічної міжвідомчої взаємодії, чіткого функціонального розподілу повноважень та відповідальності, оперативної координації дій у кризових ситуаціях [23]. Ефективна координація діяльності Служби безпеки України, Міністерства цифрової трансформації, Генерального штабу Збройних Сил України, Національної поліції, Державної служби спеціального зв'язку та захисту інформації має забезпечити комплексний багаторівневий підхід до захисту цифрового простору через синхронізацію зусиль, уникнення дублювання функцій, швидкий обмін критичною інформацією про загрози. Власний аналіз показує, що ключовим викликом є подолання відомчої

роз'єднаності, коли різні структури мають частково дублюючі повноваження, але недостатньо координують свої дії, що створює прогалини у захисті та знижує загальну ефективність системи. Необхідне створення єдиного національного координаційного центру кібербезпеки з чіткими повноваженнями щодо стратегічного планування, координації оперативного реагування на інциденти, розподілу ресурсів та відповідальності.

Кадрове забезпечення цифрової оборони об'єктивно становить один із найбільших стратегічних викликів для української держави через дефіцит висококваліфікованих фахівців у критичних галузях кібербезпеки, інформаційної безпеки, цифрового захисту [22]. Створення комплексної

71

багаторівневої системи підготовки спеціалістів потребує фундаментального реформування освітніх програм на всіх рівнях від середньої школи до університетів та професійної перепідготовки, активного залучення міжнародного досвіду через програми обміну та стажування, партнерства з провідними глобальними технологічними компаніями. Критично важливим є підготовка не лише штатних спеціалістів у державних структурах, але й резервістів та кваліфікованих волонтерів, здатних оперативно підключитися до роботи у цифровому середовищі у кризових ситуаціях. Власний аналіз свідчить про успішний досвід мобілізації українського ІТ-сектору для потреб цифрової оборони, коли провідні компанії та фахівці добровільно надають експертизу, технологічні рішення, людські ресурси для захисту критичної інфраструктури, що демонструє потенціал публічно-приватного партнерства у цій сфері.

Правове забезпечення цифрової оборони вимагає створення комплексної сучасної нормативної бази, що регулюватиме складний комплекс питань кібербезпеки, захисту персональних даних громадян, протидії інформаційним загрозам, юридичної відповідальності за кіберзлочини [24]. Конституція України закріплює фундаментальні принципи забезпечення національної безпеки, які мають бути детально конкретизовані у спеціальному галузевому законодавстві щодо різних аспектів цифрової оборони. Ключовим викликом є збалансування

легітимних потреб національної безпеки з конституційним захистом прав та свобод громадян, зокрема права на приватність, свободу вираження поглядів, доступ до інформації. Надмірно репресивне законодавство може підірвати демократичні цінності та довіру суспільства до держави, тоді як недостатнє регулювання створює правовий вакуум, що використовується агресором для безкарної діяльності. Міжнародне співробітництво у сфері цифрової оборони відкриває критично важливі додаткові можливості для України у протидії російським багаторівневим інформаційним атакам через доступ до передових технологій, обмін оперативною інформацією про загрози, спільні навчання та операції [17]. Участь України у європейських та трансатлантичних ініціативах з

72

кібербезпеки сприяє трансферу найкращих практик, стандартів, методологій захисту цифрового простору. Європейський Союз надає значну фінансову, технологічну та експертну підтримку Україні у різних сферах цифрової безпеки через спеціалізовані програми технічної допомоги, грантове фінансування проектів, направлення радників [64]. Власний аналіз показує, що ефективність міжнародного співробітництва критично залежить від здатності України не лише отримувати допомогу, але й активно ділитися власним унікальним досвідом протистояння російській гібридній агресії, що має величезну цінність для партнерів у контексті глобального протистояння авторитарним режимам.

Технологічні виклики формування цифрової оборони пов'язані з фундаментальною необхідністю забезпечення стійкості критичної національної інфраструктури до масованих кібератак [66]. Енергетичні системи, транспортна інфраструктура, фінансовий сектор, системи водопостачання, телекомунікаційні мережі потребують впровадження багаторівневих систем захисту з резервуванням критичних компонентів, сегментацією мереж для локалізації можливих інцидентів, регулярним аудитом безпеки, навчанням персоналу. Конкретним прикладом критичної важливості цього напрямку є масовані російські кібератаки на українську енергосистему у 2015-2016 роках, коли успішні атаки призвели до тимчасового знеструмлення значних територій, що

продемонструвало вразливість цифрових систем управління інфраструктурою та необхідність системного підвищення їхньої стійкості.

Соціальний вимір цифрової оборони передбачає масове підвищення рівня цифрової грамотності населення та формування культури безпечної відповідальної поведінки в мережі Інтернет через систематичні освітні кампанії [9]. Інформування широких верств громадян про конкретні методи російської пропаганди, типові технології маніпулятивних впливів, практичні способи захисту від дезінформації сприятиме підвищенню колективної стійкості суспільства до інформаційних атак. Власний аналіз свідчить, що найбільш вразливими до інформаційних маніпуляцій є соціальні групи з низьким рівнем

73

цифрової грамотності, обмеженим доступом до альтернативних джерел інформації, що актуалізує необхідність таргетованих освітніх програм для цих категорій населення.

Система безперервного моніторингу та професійної аналітики інформаційного простору має стати критично важливим елементом цифрової оборони України через створення потужних спеціалізованих аналітичних центрів для систематичного вивчення російських інформаційних операцій, виявлення нових технік та тактик, прогнозування майбутніх кампаній [19]. Автоматизовані системи збору та інтелектуальної обробки інформації з відкритих джерел, соціальних мереж, медіа дозволять своєчасно виявляти зароджувані тенденції у російській пропаганді, ідентифікувати нові наративи на ранніх стадіях їх формування, оперативно координувати адекватні заходи протидії. Інтеграція людської експертизи з технологічними можливостями штучного інтелекту забезпечить оптимальний баланс між швидкістю обробки великих даних та глибиною контекстуального аналізу.

Протидія російським інформаційним атакам у довгостроковій стратегічній перспективі вимагає формування ефективної системи державної стратегічної комунікації, здатної не лише реактивно спростовувати дезінформацію, але й проактивно формувати інформаційний порядок денний [21]. Створення

професійної системи державної комунікації, що спроможна швидко реагувати на виклики, продукувати якісний контент, формувати позитивний достовірний наратив про Україну для різних аудиторій, має стати абсолютним пріоритетом цифрової оборони. Координація національних та міжнародних комунікаційних зусиль у протидії російській дезінформації у вітчизняному та глобальному інформаційних просторах потребує узгодження меседжів, синхронізації кампаній, спільного планування. Захист цифрової інфраструктури державних установ потребує впровадження сучасної багаторівневої системи безпеки з використанням найкращих світових практик та технологій [7]. Забезпечення безперервності функціонування критичних державних органів навіть за умов

74

масованих координованих кібератак вимагає резервування систем, географічного розподілу дата-центрів, регулярного тестування планів відновлення після інцидентів. Розвиток вітчизняної індустрії кібербезпеки має стати стратегічним напрямом довгострокової економічної політики держави через зменшення критичної залежності від іноземних постачальників технологій [75]. Цільова підтримка українських розробників програмного забезпечення для кібербезпеки, створення спеціалізованих інноваційних хабів, залучення венчурних інвестицій у галузь, податкові стимули для технологічних компаній сприятимуть розвитку власного технологічного потенціалу та створенню робочих місць для висококваліфікованих спеціалістів.

Технологічне партнерство з країнами НАТО відкриває для України унікальні можливості отримання доступу до передових розробок у галузі цифрової безпеки, сумісності систем, спільних навчань [2]. Адаптація західних стандартів, технологій, методологій до специфічних українських потреб та реалій вимагає виваженого підходу, що враховує національні особливості при збереженні сумісності з системами партнерів. Довгострокова стійкість цифрової оборони України критично залежить від здатності держави створити самодостатню національну екосистему кібербезпеки з власними технологіями, кваліфікованими кадрами, науковою базою [70]. Масштабні інвестиції у

фундаментальні та прикладні наукові дослідження, цільова підтримка технологічних стартапів у галузі кібербезпеки, створення максимально сприятливих умов для розвитку ІТ-індустрії забезпечать технологічну незалежність та стійкість України у довгостроковій перспективі.

Соціально-психологічна стійкість українського суспільства до російських інформаційних атак має систематично підтримуватися через комплексну систему освіти та виховання [44]. Включення обов’язкових курсів медіаграмотності, цифрової безпеки, критичного мислення до шкільних та університетських навчальних програм на всіх рівнях сприятиме підготовці нового покоління громадян, максимально стійких до витончених

75

маніпулятивних впливів та здатних самостійно критично аналізувати інформацію. Формування цифрової оборони України відбувається в умовах безпрецедентного багатовимірного тиску з боку російської федерації, що демонструє взаємопов’язаність різних аспектів загрози [1]. Комплексний системний підхід до формування цифрової оборони, що органічно поєднує технологічні, організаційні, правові, кадрові та соціальні аспекти у єдину інтегровану систему, має забезпечити довгострокову стійкість України до інформаційних атак. Перспективи визначаються як внутрішніми послідовними зусиллями держави та суспільства, так і масштабом міжнародної підтримки [51, 65]. Створення стійкої адаптивної системи цифрової оборони потребує постійного вдосконалення, швидкої адаптації до еволюції загроз, консолідації зусиль усього суспільства. Тільки комплексний та системний підхід забезпечить надійний захист національних інтересів України у цифровому просторі та сприятиме перемозі у тривалому протистоянні з російською агресією. Зведені напрямки описано у таблиці (див. Таблиця 3.1).

Таблиця 3.1

Стратегічні напрями формування цифрової оборони України

Напрямок	Ключові завдання	Інструменти реалізації	Показники успіху
----------	------------------	------------------------	------------------

Технологічний	Впровадження систем виявлення загроз	ШІ, автоматизований моніторинг	Виявлення 80% загроз за 1 годину
Організаційний	Координація взаємодії	Нац. центр кібербезпеки	Час реагування <2 години
Кадровий	Підготовка фахівців	Реформа освіти	+500 спеціалістів/рік
Правовий	Створення норм. бази	Спеціальне законодавство	5 ключових законів до 2026
Міжнародний	Інтеграція у систему	Партнерство НАТО/ЄС	Участь у 10+ міжнар. проєктах

Складено автором на основі джерел [2, 9, 13, 16, 17, 19, 21, 22, 23, 24, 37, 38, 44, 64, 66, 70, 73, 75].

Аналіз стратегічних напрямів формування цифрової оборони України свідчить про необхідність комплексного системного підходу, що інтегрує технологічні, організаційні, правові, кадрові, міжнародні, соціальні та

76

економічні виміри. Ключовими викликами є подолання відомчої роз'єднаності, дефіцит кваліфікованих кадрів, збалансування національної безпеки з демократичними цінностями, забезпечення стійкості критичної інфраструктури. Успішний досвід мобілізації українського ІТ-сектору та міжнародне партнерство створюють основу для формування самодостатньої екосистеми кібербезпеки. Довгострокова стійкість цифрової оборони критично залежить від здатності держави інвестувати у технології, освіту, міжнародну співпрацю та формування цифрової грамотності населення. Тільки комплексний підхід забезпечить надійний захист національних інтересів України у цифровому просторі та сприятиме перемозі у протистоянні з російською агресією.

Висновки до розділу 3

Третій розділ магістерської роботи присвячено аналізу перспектив впровадження рекомендацій щодо протидії інструментам інформаційної війни російської федерації проти України в умовах широкомасштабної збройної

агресії. Проведене дослідження дозволило сформулювати низку важливих висновків щодо стратегічних напрямів формування цифрової оборони держави та механізмів нейтралізації російських інформаційних загроз. Аналіз перспектив формування цифрової оборони в Україні засвідчив необхідність створення багаторівневої системи захисту цифрового простору, яка інтегрує технологічні, організаційні, правові та соціальні механізми протидії інформаційним загрозам. Встановлено, що формування ефективної системи цифрового захисту вимагає координації зусиль державних органів, приватного сектору та громадянського суспільства через створення єдиного координаційного центру, який би здійснював стратегічне планування та оперативне реагування на загрози.

Дослідження показало, що розвиток технологічної складової цифрової оборони має включати впровадження сучасних систем виявлення кіберзагроз, автоматизованих механізмів моніторингу інформаційного простору та технологій штучного інтелекту для аналізу великих масивів даних.

77

Організаційна структура має базуватися на принципах міжвідомчої взаємодії та чіткого розподілу повноважень між Службою безпеки України, Міністерством цифрової трансформації та Генеральним штабом Збройних Сил України. Важливим елементом технологічної інфраструктури має стати національна система раннього попередження про кіберзагрози, інтегрована з аналогічними системами країн-партнерів НАТО та Європейського Союзу. Особливу увагу приділено кадровому забезпеченню цифрової оборони, оскільки дефіцит кваліфікованих спеціалістів становить одну з найбільших загроз для національної безпеки. Визначено необхідність реформування освітніх програм, створення системи безперервної професійної підготовки фахівців та залучення експертів з приватного сектору на конкурентоспроможних умовах. Аналіз правового регулювання виявив потребу гармонізації законодавства з європейськими стандартами, зокрема з Директивою NIS2 Європейського Союзу.

Підсумовуючи результати третього розділу, можна стверджувати, що формування ефективної системи цифрової оборони України вимагає

комплексного підходу, який інтегрує технологічні, організаційні, правові, освітні та міжнародні компоненти. Результати аналізу засвідчили необхідність створення національної платформи моніторингу інформаційного простору для виявлення дезінформаційних кампаній та забезпечення оперативного реагування. Запропоновані нами рекомендації формують стратегічну основу для довгострокового розвитку національної системи інформаційної безпеки, здатної протистояти гібридним загрозам як в умовах активних військових дій, так і у післявоєнний період.

78

ВИСНОВКИ

У процесі дослідження теоретико-методологічних засад інформаційної війни встановлено, що це явище являє собою складну багатовимірну систему цілеспрямованого впливу на свідомість та поведінку цільових аудиторій з метою досягнення стратегічних політичних, військових та економічних цілей без застосування або поряд із застосуванням традиційної військової сили. Систематизовано наукові підходи до визначення сутності інформаційної війни, що дозволило виокремити її ключові ознаки: цілеспрямованість інформаційного впливу, використання широкого спектру каналів поширення дезінформації, координація інформаційних операцій з іншими формами тиску, спрямованість на деформацію суспільної свідомості та підрив довіри до державних інституцій.

Аналіз світового досвіду ведення інформаційних війн у XX–XXI століттях продемонстрував еволюцію механізмів дезінформації та пропаганди від примітивних форм до витончених технологій маніпулювання суспільною свідомістю. Досвід Першої та Другої світових воєн засвідчив ефективність пропаганди як інструменту мобілізації населення та деморалізації противника через контроль над засобами масової інформації та створення образу ворога. Радянська пропагандистська машина часів холодної війни відпрацювала методи довгострокового ідеологічного впливу, маніпулювання історичною пам'яттю, використання агентів впливу у західних суспільствах, що стали прототипом сучасних російських інформаційних операцій. Систематизація світового досвіду

дозволила виявити універсальні закономірності інформаційних воєн: пріоритетність контролю над інформаційним простором, використання емоційного впливу над раціональним дискурсом, експлуатація існуючих соціальних розколів, координація інформаційних операцій з військовими діями, адаптація методів до технологічних можливостей епохи.

Дослідження стратегії, етапів та основних інструментів інформаційної війни російської федерації проти України в умовах повномасштабного

79

вторгнення виявило системний та довгостроковий характер інформаційної агресії. Встановлено, що російська інформаційна війна має глибоке історичне коріння, сягаючи періоду Радянського Союзу, та еволюціонувала від локальних маніпуляцій після здобуття Україною незалежності до тотальної інформаційної кампанії після анексії Криму у 2014 році. Повномасштабна фаза після 24 лютого 2022 року характеризується якісно новими параметрами: різким зростанням інтенсивності інформаційних атак, розширенням спектру використовуваних інструментів від традиційних медіа до координованих мереж ботів, посиленням міжвідомчої координації пропагандистських зусиль. Виокремлено стратегічні напрями російської інформаційної агресії: політичний напрям спрямований на підриг довіри до української влади через фейки про корупцію та персональні атаки на лідерів; військовий напрям реалізується через маніпуляції інформацією про втрати та перебіг бойових дій; міжнародний напрям використовує кампанії в іноземних ЗМІ для формування сумнівів щодо доцільності допомоги Україні; економічний напрям поширює фейки про фінансовий крах для провокування паніки; соціально-гуманітарний напрям експлуатує теми переселенців та мовного питання для послаблення національної єдності; психологічний напрям застосовує страх та апеляції до історичних травм для зниження суспільної стійкості. Також проаналізовано структуру російських пропагандистських платформ: офіційні державні медіа транслують позицію Кремля через емоційно забарвлений контент; напівофіційні псевдонезалежні видання створюють ілюзію плюралізму; розгалужена мережа інтернет-ресурсів професійно імітує незалежні

медіа; координовані мережі фейкових акаунтів та ботів у соціальних мережах забезпечують вірусне поширення дезінформації.

Дослідження інформаційно-психологічних та кібероперацій як інструментів стратегічного впливу виявило їхню інтеграцію у єдину систему гібридної агресії. Психологічні операції базуються на створенні альтернативної реальності через маніпулювання історичною пам'яттю, експлуатацію базових емоцій страху та невизначеності, використання складних алгоритмів

80

таргетування для персоналізованого впливу на різні соціальні групи. Метод інформаційного затоплення через створення величезної кількості суперечливих повідомлень призводить до інформаційної апатії та недовіри до всіх джерел інформації. Кібероперації становлять технологічний фундамент інформаційної війни через дестабілізацію критичної інфраструктури, викрадення конфіденційної інформації, порушення функціонування державних систем. Встановлено координацію кібератак з інформаційно-психологічними операціями та військовими діями, що створює синергетичний ефект. Соціальні мережі перетворилися на пріоритетну арену інформаційного протиборства через безпрецедентні можливості для масштабного поширення дезінформації та таргетованого впливу. Виокремлено базові стратегії російського впливу: створення мереж фейкових акаунтів для імітації масової підтримки, використання ботів для штучного посилення тем, компрометація реальних акаунтів через хакерські атаки, створення псевдолегітимних медіаплатформ під виглядом незалежних експертних джерел. Обґрунтування напрямів та перспектив розбудови системи цифрової оборони України виявило необхідність комплексного підходу, що інтегрує технологічні, організаційні, правові, кадрові, міжнародні, соціальні та економічні виміри.

Узагальнюючи результати дослідження, слід констатувати, що інформаційна війна російської федерації проти України є системним багатовимірним явищем, що органічно поєднує політичні, психологічні, технологічні та економічні інструменти впливу як складову комплексної

гібридної агресії. Стратегічна мета російської інформаційної війни полягає не просто у ситуативному спотворенні окремих фактів, а у системному конструюванні цілісної альтернативної реальності, де агресор послідовно подається як захисник справедливості, а реальна жертва збройної агресії трансформується у головну загрозу безпеці. Ефективна протидія російським інформаційним загрозам вимагає комплексного багаторівневого підходу, що поєднує технологічне зміцнення кібербезпеки, масовий розвиток