НАЦІОНАЛЬНИЙ УНІВЕРСТИТЕТ БІОРЕСУРСІВ І ПРИРОДОКОРИСТУВАННЯ УКРАЇНИ

Гуманітарно-педагогічний факультет

ПОГОДЖЕНО **Декан гуманітарно-педагогічного факультету**	**ДОПУСКАЄТЬСЯ ДО ЗАХИСТУ** **В.о завідувача кафедри міжнародних відносин і суспільних наук**
_____ Савицька І. М.	_____ Хвіст В. О.
«___» _____ 2025р.	«___» _____ 2025р.

МАГІСТЕРСЬКА КВАЛІФІКАЦІЙНА РОБОТА

на тему:

«ІНФОРМАЦІЙНА СКЛАДОВА ЯК КЛЮЧОВИЙ АСПЕКТ ГІБРИДНОЇ ВІЙНИ»

Спеціальність	291 «Міжнародні відносини, суспільні комунікації та регіональні студії»
Освітня програма	«Міжнародні відносини, суспільні комунікації та регіональні студії»
Орієнтація освітньої програми	освітньо-професійна

Гарант освітньої програми	кандидат іст. наук, доцент	_____	Кравченко Н.Б.
Керівник магістерської кваліфікаційної роботи	кандидат іст. наук, доцент	_____	Кравченко Н.Б.
Виконала		_____	Кот К.В.

КИЇВ – 2025

НАЦІОНАЛЬНИЙ УНІВЕРСТИТЕТ БІОРЕСУРСІВ І ПРИРОДОКОРИСТУВАННЯ УКРАЇНИ
Гуманітарно-педагогічний факультет

ЗАТВЕРДЖУЮ
В.о. завідувача кафедри
Міжнародних відносин і суспільних наук
_____ Хвіст В.О.
"___" _____ 2025 р

ЗАВДАННЯ

до виконання магістерської кваліфікаційної роботи студенту
Кот Катерині Василівні

Спеціальність **291 «Міжнародні відносини, суспільні комунікації та регіональні студії»**
Освітня програма **«Міжнародні відносини, суспільні комунікації та регіональні студії»**
Орієнтація освітньої програми **освітньо-професійна**

Тема магістерської кваліфікаційної роботи: «**Інформаційна складова як ключовий аспект гібридної війни»**
затверджена наказом ректора НУБіП України від «26» листопада 2024 року №2086 «С»
Термін подання завершеної роботи на кафедру «21» листопада 2025 року

Вихідні дані до магістерської кваліфікаційної роботи:
1) наукові дослідження з питань гібридної війни у військово-політичній сфері;
2) вітчизняні та зарубіжні літературні джерела з проблеми дослідження;
3) тексти протоколів зустрічей, спільні заяви, декларіції, меморандуми, угоди.

Перелік питань, що підлягають дослідженню:
1. Провести аналіз теоретико-методологічних засад інформаційної складової гібридної війни, визначивши сутність понять «інформаційні операції» та «інформаційні війни».
2. Вивчити основні методи ведення інформаційних операцій, зокрема маніпуляції, пропаганду та фейкові новини як інструменти впливу на суспільство.
3. Проаналізувати роль соціальних медіа в інформаційній складовій гібридної війни та механізми інформаційних атак на державні інституції.
4. Дослідити інформаційні операції в українському контексті, визначивши методи протидії інформаційним загрозам та роль державних і міжнародних організацій у забезпеченні інформаційної безпеки.

Дата видачі завдання		26.11.2024 р.
Керівник магістерської роботи	_____	Кравченко Н.Б.
Завдання прийняла до виконання	_____	Кот К.В.

РЕФЕРАТ

магістерської роботи
студента магістратури гуманітарно-педагогічного факультету
спеціальності 291 «Міжнародні відносини, суспільні комунікації та регіональні студії»,
освітньо-професійної програми «Міжнародні відносини, суспільні комунікації та регіональні студії»
Національного університету біоресурсів і природокористування України
Кот Катерини Василівни
на тему: «Інформаційна складова як ключовий аспект гібридної війни»

Кваліфікаційна робота складається зі вступу, чотирьох розділів, висновку, списку використаних джерел та додатків. Загальний обсяг роботи складає 100 сторінок, з яких 90 сторінок основного тексту, який містить 10 таблиць та 8 рисунків. Список використаних джерел налічує 90 найменувань.

Робота присвячена комплексному дослідженню інформаційної складової як ключового компонента сучасної гібридної війни, з особливим акцентом на досвід російсько-українського конфлікту. Обрана тема є надзвичайно актуальною в контексті триваючої повномасштабної агресії Російської Федерації проти України, яка демонструє безпрецедентне поєднання традиційних військових дій з витонченими методами інформаційного впливу, психологічного тиску та дезінформації.

У кваліфікаційній роботі було використано комплекс загальнонаукових (системний аналіз, логічний метод, статистичний метод, порівняльний аналіз) та спеціальних (контент-аналіз, метод кейс-стаді, структурно-функціональний метод) методів дослідження, що дозволило всебічно проаналізувати інформаційну війну як невід'ємний елемент гібридного протистояння та визначити ефективні механізми протидії інформаційним загрозам.

У першому розділі розглянуто теоретико-методологічні основи інформаційної складової гібридної війни. Проаналізовано категорії «інформаційні операції» та «інформаційні війни» в контексті сучасних міжнародних відносин, визначено місце інформаційного компонента в системі гібридних впливів. Охарактеризовано еволюцію концепцій інформаційної боротьби від Холодної війни до цифрової епохи. Особливу увагу приділено джерельній базі дослідження, включаючи нормативно-правові акти, аналітичні звіти міжнародних організацій та наукові публікації провідних дослідників у галузі інформаційної безпеки.

Другий розділ присвячений детальному аналізу інформаційної війни як інструменту гібридної агресії. Досліджено основні методи ведення інформаційних операцій, включаючи використання традиційних та цифрових

медіа, соціальних мереж, ботоферм та тролів. Розглянуто маніпуляції, пропаганду та фейкові новини як ключові інструменти впливу на суспільну свідомість. Проаналізовано конкретні приклади застосування інформаційних технологій у відомих гібридних конфліктах, включаючи досвід війн у Сирії, втручання у вибори в США та Європі, а також інформаційні кампанії Китаю щодо Тайваню.

У третьому розділі досліджено інформаційні стратегії в сучасних конфліктах. Вивчено стратегії інформаційного впливу в міжнародних відносинах, включаючи концепції «м'якої сили» та публічної дипломатії. Визначено ключову роль соціальних медіа як платформ для швидкого поширення інформації та формування громадської думки. Проаналізовано інформаційні атаки та їх вплив на державні інституції, демократичні процеси та громадянське суспільство. Здійснено детальний аналіз інформаційних операцій в українському контексті, зокрема на прикладі конфлікту на Сході України, що розпочався у 2014 році та продовжується досі.

У четвертому розділі систематизовано методи протидії інформаційним загрозам. Досліджено комплекс заходів, що включають технічні рішення (моніторинг інформаційного простору, кіберзахист, блокування дезінформаційних ресурсів), правові механізми (законодавча база, санкції проти поширювачів фейків), освітні ініціативи (підвищення медіаграмотності населення, розвиток критичного мислення) та міжнародну співпрацю. Визначено роль державних інституцій, неурядових організацій та міжнародних структур у боротьбі з інформаційною агресією. Розроблено практичні рекомендації щодо створення ефективної системи інформаційної безпеки в умовах гібридної війни.

Дослідження демонструє, що інформаційна складова гібридної війни стала не просто додатковим елементом сучасних конфліктів, а їх центральною віссю, що визначає перебіг та результати протистояння. Від здатності держави і суспільства розпізнавати інформаційні загрози, оперативно на них реагувати, зберігати внутрішню єдність та спиратися на об'єктивну інформацію залежить не лише успіх у конкретному конфлікті, а й збереження демократичних цінностей, національного суверенітету та свободи слова в глобальному масштабі.

Ключові слова за темою кваліфікаційної роботи: інформаційна війна, гібридна війна, дезінформація, пропаганда, фейкові новини, кібератаки, медіаграмотність, інформаційна безпека, стратегічні комунікації, російсько-українська війна, соціальні медіа, інформаційні операції, протидія дезінформації.

Зміст

ПЕРЕЛІК УМОВНИХ ПОЗНАЧЕНЬ

ІТ – інформаційні технології;

НУО – неурядові організації;

США – Сполучені Штати Америки;

СРСР – Союз Радянських Соціалістичних Республік;

ЗМІ – Засоби масової інформації;

ООН – організація об’єднаних націй;

ОБСЄ – Організація з безпеки і співробітництва в Європі

НАТО – Організація Північноатлантичного договору;

РФ – Російська Федерація;

ІПсО – Інформаційно-психологічні операції

ЗСУ – Збройні Сили України

ШІ – Штучний інтелект;

РНБО – Рада національної безпеки і оборони;

ЄС – Європейський Союз;

СБУ – Служба безпеки України;

Проекти ГО – Громадські організації;

USAID – Агентство США з міжнародного розвитку.

ВСТУП

Актуальність дослідження. У сучасному глобалізованому світі, де інформація стала одним з найпотужніших стратегічних ресурсів, інформаційна складова гібридної війни набуває критичного значення для національної безпеки держав. Традиційні форми збройного протистояння дедалі частіше доповнюються або навіть замінюються складними інформаційно-психологічними операціями, спрямованими на деморалізацію суспільства, підрив довіри до державних інституцій та дестабілізацію політичної ситуації без безпосереднього застосування військової сили.

Російсько-українська війна, що розпочалася у 2014 році та перейшла у фазу повномасштабного вторгнення у 2022 році, стала яскравим прикладом сучасної гібридної війни, де інформаційний компонент відіграє не менш важливу роль, ніж збройне протистояння. Систематичне поширення дезінформації, фейкових новин, маніпулятивних наративів через традиційні та цифрові медіа, кібератаки на критичну інфраструктуру, психологічний тиск на населення – усе це демонструє еволюцію форм і методів ведення сучасних воєн.

Актуальність дослідження зумовлена також необхідністю формування ефективних механізмів протидії інформаційним загрозам, підвищення рівня медіаграмотності населення та розробки державної стратегії інформаційної безпеки в умовах триваючого конфлікту. Досвід України у протистоянні російській інформаційній агресії має важливе значення не лише для нашої держави, а й для міжнародної спільноти, що стикається з подібними викликами.

Мета роботи – комплексно проаналізувати інформаційну складову як ключовий аспект сучасної гібридної війни, з'ясувати механізми, методи та інструменти інформаційного впливу, а також визначити ефективні шляхи протидії інформаційним загрозам на прикладі російсько-українського конфлікту.

Завдання дослідження:

- охарактеризувати теоретико-методологічні засади гібридної війни та визначити місце інформаційної складової в системі гібридних впливів;
- проаналізувати сутність понять «інформаційні операції» та «інформаційні війни» у контексті сучасних міжнародних відносин;
- виявити основні методи ведення інформаційних операцій та інструменти впливу на суспільство (маніпуляції, пропаганда, фейки);
- дослідити роль соціальних медіа в інформаційній складовій гібридної війни та їх вплив на формування громадської думки;
- проаналізувати конкретні приклади застосування інформаційних технологій у гібридних конфліктах, зокрема в українському контексті;
- визначити методи та механізми протидії інформаційним загрозам на державному та міжнародному рівнях;
- розробити практичні рекомендації щодо створення системи інформаційної безпеки в умовах гібридної війни.

Об'єктом дослідження є гібридна війна як сучасна форма збройного та інформаційного конфлікту.

Предметом дослідження виступає інформаційна складова як системний елемент гібридної війни, її форми, методи, інструменти впливу та механізми протидії.

Методи дослідження. У процесі написання роботи використано комплекс загальнонаукових та спеціальних методів дослідження: системний аналіз – для розгляду інформаційної війни як цілісної системи взаємопов'язаних елементів; контент-аналіз – для вивчення змісту медіаповідомлень, пропагандистських матеріалів та дезінформаційних кампаній; порівняльний аналіз – для зіставлення різних підходів до визначення сутності інформаційної війни та методів протидії їй; метод кейс-стаді – для детального вивчення конкретних випадків інформаційного впливу в умовах російсько-українського конфлікту; структурно-функціональний метод – для визначення ролі та функцій державних інституцій і міжнародних організацій у протидії інформаційним загрозам.

Теоретична значущість роботи полягає у систематизації та розширенні наукових уявлень про природу, сутність та особливості інформаційної складової гібридної війни, узагальненні теоретико-методологічних підходів до вивчення інформаційних операцій у сучасних конфліктах, а також у розробці концептуальної моделі протидії інформаційним загрозам в умовах гібридного протистояння.

Прикладна цінність результатів дослідження визначається можливістю їх використання для удосконалення державної інформаційної політики України, розробки практичних рекомендацій для підрозділів стратегічних комунікацій та інформаційної безпеки, підготовки навчальних курсів з медіаграмотності та інформаційної гігієни, а також для підготовки фахівців у галузі національної безпеки, стратегічних комунікацій та протидії гібридним загрозам.

Інформаційну базу дослідження становлять нормативно-правові акти України у сфері інформаційної безпеки та національної оборони, офіційні документи міжнародних організацій (ООН, НАТО, ОБСЄ, ЄС), аналітичні звіти та доповіді профільних дослідницьких центрів, наукові монографії та статті вітчизняних і зарубіжних учених з проблематики інформаційних війн та гібридних конфліктів, матеріали незалежних медіа та фактчекінгових організацій, статистичні дані державних органів, а також результати моніторингу інформаційного простору під час російсько-українського конфлікту.

Апробація результатів роботи.

Роботу апробовано на конференціях:

1. Кот Катерина Василівна, Інформаційна складова як ключовий аспект гібридної війни. Всеукраїнський науково-практична конференція з міжнародною участю «Національна безпека в умовах війни, післявоєнні відбудови та глобальних викликів XXI століття» (12-13 грудня 2024 рік) (ст. 102-104)

2. Кот Катерина Василівна, Інформаційна складова гібридної війни. Міжнародна науково-практична конференція «Українська дипломатія: становлення, розвиток та перспективи» (м. Київ, 10 квітня 2025р.) (ст. 126-127)
3. Кот Катерина, Аналіз інформаційних операцій в українському контексті (на прикладі на Сході України). Всеукраїнський науково-практичний вебінар “Європейський вибір України: Школа юного міжнародника” (01-03 квітня 2025), м. Київ (ст. 126-127)
4. Кот Катерина, Дезінформація як зброя: механізми інформаційного впливу в умовах гібридної війни. 2-га Міжнародна науково-практична конференція “Scientific Progress: Theories, Applications and Global Impact” (27-29 жовтня 2025), Брага, Португалія (ст. 82-84)
5. Кот Катерина, Дезінформація як зброя: механізми інформаційного впливу в умовах гібридної війни. 4-та Міжнародна науково-практична конференція “Achievements of Science and Applied Research” (10-12 листопада 2025), Дублін, Ірландія (ст. 138-143)

Структура роботи.

Дослідження складається із вступу, 4 розділів, висновку, списку використаних джерел, з них вітчизняних джерел – 84 найменувань, зарубіжних джерел – 6, додатків. Загальний обсяг роботи складає 91 сторінку.

РОЗДІЛ 1
ТЕОРЕТИКО-МЕТОДОЛОГІЧНІ АСПЕКТИ ІНФОРМАЦІЙНОЇ СКЛАДОВОЇ ГІБРИДНОЇ ВІЙНИ

1.1 Категорії "інформаційні операції", "інформаційні війни" в сучасних міжнародних відносинах

У сучасному глобалізованому світі, де інформація стала одним з головних ресурсів, а технології цифрової комунікації стрімко розвиваються, значення інформаційного впливу на суспільства, політичні системи та міждержавні відносини суттєво зросло. У цьому контексті поняття «інформаційна війна» та «інформаційні операції» вийшли за межі публіцистичних і політичних висловлювань, набувши статусу самостійних наукових категорій. Вони активно вивчаються в рамках міжнародних досліджень, безпекових студій, соціології, психології масової свідомості, стратегічних комунікацій та кібербезпеки [15; 56, с.30].

Інформаційна війна в сучасному науковому розумінні - це систематичне застосування інформаційних засобів з метою досягнення політичного, військового або економічного домінування, при цьому використовуються інструменти дезінформації, маніпуляції громадською думкою, кібератак, фальсифікацій, психологічного тиску тощо. Зміст інформаційної війни охоплює як відкриті, так і приховані форми впливу, що дозволяє її застосовувати як у періоди активного воєнного конфлікту, так і у відносно мирний час [13, с.34; 25].

Поняття «інформаційні операції» тісно пов’язане з терміном «інформаційна війна», проте має більш прикладний та тактичний характер. Інформаційна операція - це цілеспрямована сукупність дій, спрямованих на збір, обробку, розповсюдження чи спотворення інформації з метою отримання переваги над супротивником. Такі операції можуть бути частиною більш масштабної гібридної стратегії, у межах якої інформаційна складова доповнює воєнні, економічні та дипломатичні заходи [1; 37].

Історично термін «інформаційна війна» вперше був уведений американським дослідником Т. Роном у звіті «Системи зброї та інформаційна війна» (1976 р.), в якому він наголошував на вразливості інформаційної інфраструктури США у випадку зовнішнього втручання. Його позиція заклала фундамент для подальшого осмислення ролі інформації як окремого середовища протистояння нарівні з сушею, морем, повітрям і космосом. У XXI столітті, особливо після гучних інформаційних кампаній у США, Європі, Росії та на Близькому Сході, термін «інформаційна війна» набув нового значення, охоплюючи не лише військові конфлікти, а й міждержавну конкуренцію на рівні ідеологій, цінностей, медіапростору та громадської думки [1; 29, с.57].

У контексті гібридної війни, яку активно застосовують окремі держави (зокрема РФ у війні проти України), інформаційна складова набуває критичного значення. Інформаційна війна може бути складовою ширшої гібридної стратегії, що поєднує традиційні та нетрадиційні форми протистояння. Вплив на суспільну свідомість, зниження морального духу населення, дестабілізація політичної ситуації, а також злам критичної інфраструктури усе це здійснюється за допомогою інформаційних операцій [15; 39].

У сучасних міжнародних відносинах інформаційні війни і операції стали ключовими інструментами впливу та контролю. Їх вивчення є необхідним не лише для розуміння механізмів гібридної агресії, але й для розробки ефективних заходів інформаційної безпеки на національному рівні (табл. 1.1).

Таблиця 1.1

Ключові компоненти інформаційної війни в контексті гібридного протистояння

Інформаційні маніпуляції	Намірене викривлення фактів через фейки, напівправду або перебільшення з метою впливу на громадську свідомість.
Кібернетичні загрози	Атаки на цифрові системи, сервіси та інфраструктуру з метою дестабілізації чи отримання конфіденційної інформації.
Політичний вплив через медіа	Використання інформаційних каналів для формування вигідних наративів у контексті виборів, протестів чи рішень урядів.

Глобальний інформаційний вплив	Створення міжнародних інформаційних кампаній, спрямованих на послаблення союзів, вплив на зовнішню політику тощо.
Захист цифрового простору	Комплекс заходів, спрямованих на протидію кібератакам та захист державних і стратегічно важливих систем.
Медіа-інструменти війни	Активне застосування соцмереж, блогів, месенджерів для швидкого поширення меседжів, а також мобілізації аудиторії.
Виклики для демократії	Підрив довіри до ЗМІ, державних інституцій і виборчого процесу через цілеспрямовані кампанії дезінформації.

Джерело: розроблено на основі [1, с.16]

В науковому та аналітичному дискурсі відсутність єдиного, універсального визначення цього поняття зумовлена не лише складністю самого явища, але й динамікою його проявів у контексті гібридних конфліктів. Залежно від контексту застосування, термін «інформаційна війна» може означати як сукупність організованих дій в інформаційному просторі, так і складову частину ширшого поняття «гібридна війна», що поєднує військові, політичні, економічні та інформаційні інструменти [15; 16, с.200; 59, с.56].

У межах сучасних міжнародних відносин інформаційна війна виступає не лише як засіб супроводу бойових дій, а й як самостійна форма стратегічного протиборства, спрямована на підрив внутрішньої стабільності держави-противника. Особливе значення в цьому процесі надається психологічному впливу на масову свідомість, маніпуляції інформаційними потоками, формуванню вигідних для суб'єкта впливу інтерпретацій реальності. Таким чином, інформаційна війна може охоплювати як агресивне впровадження фейкових наративів, так і спроби делегітимізувати уряди, інститути демократії, міжнародні союзи [23; 59, с.56].

Водночас важливо наголосити, що інформаційна складова гібридної війни проявляється не тільки у відкритих актах інформаційної агресії, а й у прихованих формах через культурну експансію, просування пропагандистських меседжів, інфільтрацію ворожих медіаресурсів у локальні інформаційні екосистеми [11].

На сьогодні поняття «інформаційна війна» у міжнародному контексті набуває рис багатогранного інструмента геополітичного впливу, який, попри

відсутність чітких кордонів та правових регламентацій, чинить потужний вплив на державну безпеку, міждержавні стосунки та глобальну стабільність (рис. 1.1.).

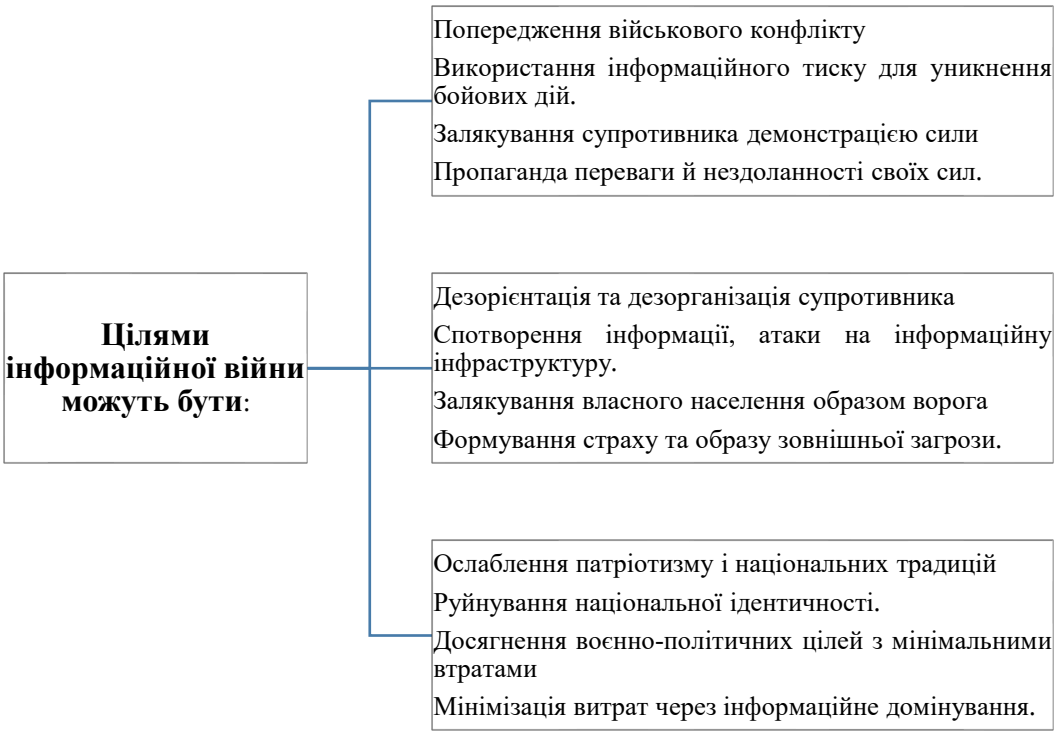

Рис.1.1. Цілі інформаційних війн [25]

Інформаційна війна є не просто частиною сучасних конфліктів, а їх ключовим компонентом, що формує уявлення суспільства про події, ворога та навіть про саму реальність. Її ефективність зумовлюється здатністю глибоко проникати у свідомість індивідів та груп, впливаючи на їхню поведінку, цінності, рішення та емоційний стан [15; 37].

Інформаційна війна здебільшого не потребує фізичного вторгнення або застосування зброї вона ведеться через слова, образи, символи, емоційно забарвлені повідомлення та дезінформаційні кампанії. Саме тому одним з найнебезпечніших аспектів цього типу війни є її невидимість: вона часто сприймається не як агресія, а як звичайний інформаційний потік, що паралізує здатність суспільства до опору [3; 61, с.70].

Водночас, через постійний розвиток цифрових технологій і комунікацій, інформаційна війна стає ще більш адаптивною та масштабною. Штучний інтелект, алгоритми персоналізації контенту, боти, фейкові акаунти усе це стало інструментами, за допомогою яких реалізується маніпулятивний вплив на

цільову аудиторію. Таким чином, межі між правдою і фальшивою інформацією розмиваються, а довіра до традиційних джерел інформації поступово знижується [56, с.47].

Для ефективного протистояння інформаційним загрозам необхідно формувати суспільний імунітет до маніпуляцій через медіаосвіту, розвиток критичного мислення, підтримку незалежної журналістики та активне залучення громадян до верифікації отримуваної інформації. Також важливим є технічне удосконалення державних та недержавних систем виявлення й протидії дезінформації, з дотриманням засад демократичного врядування та захисту прав людини [33, с.323].

Інформаційна війна – це стратегічний виклик сучасності, який вимагає не лише технічної, а й гуманітарної відповіді, де на перший план виходять знання, свідомість і цінності громадянського суспільства [25].

Продовжуючи розгляд природи та особливостей інформаційної війни, слід наголосити, що вона дедалі частіше виступає як ключовий інструмент у сучасних конфліктах. Використання інформаційних технологій таких як інтернет-платформи, соціальні мережі, месенджери, блоги, електронна пошта дозволяє значно розширити масштаби впливу на масову свідомість. Таким чином, інформаційна війна стає не лише способом маніпулювання даними, а й могутнім механізмом формування громадської думки в глобальному масштабі [13, с.45; 52, с.31].

Однією з головних характеристик інформаційної війни є її спрямованість на психологічне та емоційне тиснення. Через навмисне створення інформаційного шуму, поширення фейкових новин, пропаганди чи суперечливої інформації створюється атмосфера плутанини, недовіри та дестабілізації. У такому середовищі людина втрачає здатність чітко розрізняти правду і брехню, а це, своєю чергою, створює передумови для впливу на її поведінку, мотивацію та навіть цінності [82, с.127; 83, с.21].

Соціальні мережі відіграють у цьому процесі особливо важливу роль, адже вони дозволяють швидко та масово поширювати повідомлення, при цьому

роблячи вплив на різні цільові аудиторії максимально адресним. Штучний інтелект, алгоритми персоналізації контенту, використання ботів і тролів – усе це посилює ефективність інформаційного тиску.

Інформаційна війна часто не має чітко визначених меж чи форм. Вона може бути відкритою, тобто помітною для суспільства, або прихованою коли маніпуляції відбуваються під виглядом об'єктивної журналістики, патріотичного висвітлення чи навіть нібито незалежної експертної оцінки. Та ускладнює ідентифікацію джерел впливу та вироблення відповідних стратегій захисту [61, с.70; 66, с.23].

Інформаційна війна має ознаки високої динамічності та адаптивності. Вона змінюється залежно від ситуації, цілей і наявних технологій. Завдяки цьому вона може швидко охоплювати нові сфери від економіки до культури і залишатися ефективною навіть без використання військової сили [3,с.100].

У зв'язку з цим виникає необхідність розвивати медіаграмотність, формувати критичне мислення та інформаційну культуру в суспільстві. Громадяни мають вміти не лише споживати інформацію, але й аналізувати її джерела, зміст та можливі цілі. Окрім цього, важливо створювати і підтримувати інституції, що займаються виявленням фейкових повідомлень, інформаційного впливу та пропаганди, одночасно дотримуючись демократичних стандартів і прав людини [11, с.115].

Таким чином, сучасна інформаційна війна - це не просто боротьба за контроль над фактами, а за вплив на свідомість, ідентичність та поведінку громадян. Тому ефективна протидія їй має охоплювати як технологічні, так і соціально-психологічні аспекти.

1.2. Особливості інформаційних компонентів у гібридній війні

Інформаційна війна є однією з ключових складових гібридної війни, що характеризується широким спектром методів і технологій, спрямованих на вплив на свідомість і поведінку населення, державних структур та міжнародну

політику. Вона є важливим інструментом досягнення стратегічних цілей у рамках сучасних конфліктів, де поєднуються традиційні військові засоби та інформаційні маніпуляції.

Особливості інформаційних компонентів у гібридній війні можна розглядати через кілька ключових аспектів, зокрема через етапи розвитку та методи впливу, які характерні для цієї форми боротьби. Підготовчий етап включає збір і аналіз інформації, а також створення інфраструктури для поширення впливу, включаючи кіберплатформи, соціальні мережі, новітні інформаційні технології. Активний етап передбачає інтенсивне використання цих інструментів для досягнення політичних, військових або економічних цілей. Тут з'являється поширення пропаганди, дезінформації, маніпуляцій емоціями громадськості, а також активне використання фейкових новин і інформаційних атак. Завершальний етап, в свою чергу, полягає в оцінці результатів впливу на суспільство, державні інститути, а також міжнародну ситуацію [24, с.46].

Засоби та методи впливу в інформаційних компонентах гібридної війни є багатогранними. Може бути використання різних каналів передачі інформації традиційних засобів масової інформації, таких як телебачення та радіо, а також сучасних технологій: соціальних мереж, месенджерів, блогів і онлайн-платформ. Інформаційні атаки часто поєднуються з психологічними маніпуляціями, такими як емоційний тиск, страх або апеляція до національної гордості, що дає змогу впливати на свідомість і переконання громадськості. Усі ці засоби створюють «сітку» для маніпулювання соціальною та політичною ситуацією в державі [4, с.156; 35, с.138].

Цілі та об'єкти впливу в рамках гібридної війни мають широкий спектр. На першому плані стоїть вплив на стабільність держави, що може проявлятися в розколах у суспільстві, сприянні політичним і соціальним конфліктам, викликанню нестабільності в управлінні або загостренні міжнародних відносин. Окрім цього, інформаційні компоненти можуть бути спрямовані на зміну поведінки конкретних груп населення або на розмивання єдності національної ідентичності. Наприклад, за допомогою дезінформації та пропаганди можна

створювати зображення «ворога» або формувати вигадані загрози, які будуть сприяти агресії або дестабілізації суспільства [23].

Актори інформаційної війни в гібридних конфліктах є різноманітними. Окрім державних структур, які можуть використовувати інформаційні засоби для досягнення своїх стратегічних цілей, в цьому процесі активно беруть участь неурядові організації, терористичні угруповання, а також приватні компанії та інші суб'єкти. Кожен з цих акторів має свої цілі, методи та можливості впливу на інформаційне середовище. Наприклад, терористичні групи можуть використовувати соціальні мережі для вербування нових членів і пропаганди насильницьких ідей, в той час як держави можуть координувати інформаційні кампанії на міжнародному рівні, залучаючи медіа-ресурси або створюючи фальшиві новини [11, с.116].

Маніпуляція громадською думкою є важливим інструментом у гібридній війні. Особливо це стає очевидним через поширення дезінформації, фейків і пропаганди, що здатні формувати хибну картину реальності, що, в свою чергу, веде до дестабілізації суспільства. Важливими інструментами тут є маніпуляція емоціями, розпалювання страху, агресії або апатії, що дозволяє створювати атмосферу невизначеності і недовіри до влади чи інших суспільних інститутів [31, с.280].

Роль технологій в інформаційних компонентах гібридної війни є критично важливою. Сучасні технології дозволяють значно посилити ефективність інформаційних атак. Інтернет, соціальні мережі, кібератаки, хакерські методи впливу, усе це створює унікальні можливості для досягнення поставлених цілей. Особливо важливими є можливості автоматизації процесів маніпуляцій, використання бот-мереж для створення псевдонастільки реалістичної інформаційної картини, що звичайним користувачам стає важко відрізнити правду від вигадки [12; 55, с.45].

Інформаційна війна є одним із основних інструментів гібридної війни, що включає в себе не лише традиційні військові методи, а й складні інформаційні операції. Вона змінює природу сучасних конфліктів, роблячи їх більш

динамічними та багатоаспектними, вимагаючи від держав та громадянських структур нових підходів до захисту від інформаційних атак та маніпуляцій [23].

У сучасному глобалізованому світі роль різних суб'єктів в інформаційних війнах дедалі зростає. Інформаційні війни більше не є виключною прерогативою держав у них активно беруть участь неурядові організації, корпорації, медіа, журналісти, активісти та інші елементи громадянського суспільства. Взаємодія цих акторів у межах інформаційного простору створює складну мережу впливів, які можуть як сприяти формуванню демократичного суспільства, так і стати інструментом маніпуляції масовою свідомістю. Розглянемо це більш докладно [10, с.157; 57, с.65].

Держави відіграють провідну роль у формуванні та реалізації стратегій інформаційної боротьби. У межах інформаційних війн вони не лише використовують медіа для просування зовнішньополітичних наративів, але й активно розробляють та впроваджують кібероперації, спрямовані на ослаблення супротивника. Сучасна війна вже не обмежується полем бою тепер вона включає кіберпростір, де стратегічна інформація може відігравати вирішальну роль. На додаток до цього, держава активно формує внутрішній інформаційний простір, що проявляється у створенні "керованого" медіаполя, де одні теми замовчуються, а інші навпаки нав'язуються суспільству як пріоритетні [10, с.157; 75, с.147].

За допомогою стратегічних комунікацій і кампаній публічної дипломатії держави впливають на міжнародну аудиторію, формуючи позитивний імідж, відбілюючи власну політику або дискредитуючи супротивника. Це може проявлятись у вигляді офіційних заяв, міжнародних конференцій, культурних програм тощо. На внутрішньому рівні інформаційні кампанії сприяють консолідації населення, мобілізації патріотичних почуттів, посиленню довіри до уряду, а іноді й маніпулюванню громадською думкою.

Неурядові організації відіграють важливу роль у розкритті правди та забезпеченні прозорості у політичних процесах. В умовах інформаційних війн вони часто виступають не лише свідками подій, але й активними гравцями, які

використовують інформаційні ресурси для підвищення обізнаності суспільства. Їхня діяльність може полягати у висвітленні порушень прав людини, звітуванні про зловживання владою, а також у формуванні альтернативної точки зору, що балансує офіційну інформацію [10, с.158].

Багато НУО мають власні інформаційні платформи, звідки транслюють важливі меседжі про демократичні цінності, екологію, гендерну рівність, права меншин тощо. Завдяки мобільності, автономності та довірі з боку громадськості, вони часто стають важливим джерелом інформації як для громадян, так і для міжнародної спільноти. Особливо важливою є їхня функція моніторингу, коли НУО документують порушення, здійснюють незалежні розслідування та публікують доповіді, що можуть мати широкий резонанс у суспільстві.

В умовах цифрової епохи глобальні корпорації, особливо ті, що працюють у сфері ІТ, соціальних мереж і медіа, фактично контролюють величезні обсяги інформації. Їх вплив виходить далеко за межі бізнесу. Компанії як-от Meta, Google чи X (Twitter) стають учасниками геополітичних процесів, оскільки контролюють платформи, на яких відбувається комунікація між мільйонами людей. Через зміну алгоритмів, модерування контенту або навіть вибірково заблоковані акаунти, вони можуть прямо чи опосередковано впливати на розвиток подій [4, с.156; 86].

Журналісти, своєю чергою, опиняються на передовій інформаційного фронту. У найкращому випадку вони стають захисниками правди, борцями проти цензури та дезінформації. Але водночас саме журналістика є одним із найуразливіших елементів у ланцюгу інформаційного впливу. У багатьох випадках медіа стають інструментом політичного впливу або поширюють неперевірену інформацію, свідомо чи несвідомо стаючи учасниками інформаційних операцій [33].

Громадянське суспільство – це ще один потужний гравець. Участь громадян в інформаційних війнах проявляється через соціальні мережі, краудсорсингові ініціативи, онлайн-петиції, флешмоби та інші цифрові форми

протесту або підтримки. Активна громадянська позиція може сприяти викриттю маніпуляцій, підтримці демократичних процесів і протидії пропаганді [11, с.116].

У сучасних умовах інформаційні війни перестали бути виключною справою держав. Вони охоплюють широкий спектр акторів, кожен з яких має власні інтереси, засоби впливу та стратегії. Держава, неурядові організації, корпорації, ЗМІ та громадяни взаємодіють між собою, створюючи динамічне поле інформаційної боротьби, де йде боротьба не лише за факти, але й за інтерпретацію, емоції, довіру. Розуміння ролі кожного з цих суб'єктів є ключовим для формування ефективної інформаційної безпеки та стійкості суспільства перед зовнішніми і внутрішніми викликами [19; 20].

Інформаційна війна є не лише складовою сучасних міжнародних відносин, а й серйозним викликом, що потребує постійної адаптації засобів захисту й аналізу. Її стратегічна важливість зростає паралельно з розвитком цифрових технологій, що дозволяють проводити масові кампанії впливу, маніпулювати фактами та нав'язувати певні наративи як всередині країни, так і за її межами. На сучасному етапі інформаційні війни впливають не лише на політичну стабільність і громадську думку, а й на національну безпеку, економіку, енергетику, системи управління та критичну інфраструктуру [29, с.58; 77].

У цьому контексті Україна постає як одна з держав, яка стала безпосереднім учасником інформаційного протистояння. З початком активної фази конфлікту з Росією інформаційна складова війни стала ключовим елементом у збереженні державності, формуванні міжнародної підтримки та протидії дезінформаційним кампаніям ворога. Це вимагає від державних структур та громадянського суспільства системної координації дій у кіберпросторі, посилення інформаційної грамотності населення, розвитку національних інформаційних ресурсів і створення ефективних механізмів верифікації інформації.

Значення цифрового середовища як поля битви між державами та недержавними акторами зростає щодня. Інтернет, соціальні мережі, інформаційні платформи перетворились на інструменти впливу, які можуть

змінювати хід політичних подій, знижувати рівень довіри до влади, розпалювати конфлікти та загрожувати національній єдності. У зв'язку з цим особливої уваги потребує формування державної інформаційної політики, яка б враховувала як внутрішні, так і зовнішні ризики, забезпечувала стійкість до інформаційного тиску та сприяла розвитку критичного мислення у суспільстві [74, с.147; 76, с.189].

Таким чином, інформаційні війни – це не короткотривалі інформаційні кампанії, а довготривалий, системний процес, що потребує високого рівня технологічної готовності, аналітичного потенціалу та міждержавної співпраці. Сучасна світова практика засвідчує, що лише завдяки скоординованим зусиллям урядів, міжнародних організацій, експертного середовища та громадянського суспільства можна ефективно протидіяти інформаційним загрозам та зберігати стабільність у глобальному політичному просторі.

1.3. Джерельна база дослідження

Дослідження інформаційної складової гібридної війни спирається на широкий спектр історичних і сучасних джерел, які дають змогу простежити еволюцію інформаційного впливу в міжнародних конфліктах. Важливим етапом у формуванні інформаційної боротьби як окремої складової гібридної війни стала Перша світова війна (1914–1918), коли, окрім збройного протистояння, активно використовувалася психологічна війна. Пропаганда, фейкові новини та маніпулятивна інформація вже тоді набули масштабного характеру, демонструючи силу інформаційного впливу на суспільну свідомість [73, с.67; 84, с.4].

З історичних джерел видно, що вже під час Першої світової війни багато країн створювали спеціальні пропагандистські структури, які займалися поширенням ідеологічно вмотивованих матеріалів через газети, плакати, листівки, кінохроніку. Дані джерела свідчать про те, що завданням такої інформації було не лише формування патріотичних настроїв, а й демонізація противника, створення образу ворога та зміцнення морального духу власного

населення. Пропаганда працювала на формування емоційної напруги, страху й ненависті, що забезпечувало необхідний рівень мобілізації населення [32; 53].

У джерелах також зафіксоване активне використання фейкових повідомлень і викривленої інформації – наприклад, перебільшення перемог своїх військ чи створення вигаданих історій про жорстокість ворога. Практики підтверджують, що інформаційна складова війни, зокрема через спотворення фактів, відігравала не менш важливу роль, ніж фізичне збройне протистояння.

Аналіз історичних джерел дозволяє зробити висновок, що витоки сучасних інформаційних воєн, у тому числі й у форматі гібридного протистояння, мають глибокі корені. Пропагандистські кампанії Першої світової війни стали своєрідною основою для подальшого розвитку інформаційної зброї в XX і XXI століттях. Сучасні дослідники використовують ці історичні приклади як емпіричну базу для розуміння механізмів дезінформації, психологічного впливу та пропаганди у теперішніх гібридних конфліктах. У контексті інформаційної складової гібридної війни ці історичні джерела набувають нового значення, оскільки допомагають простежити трансформацію методів інформаційного впливу – від друкованих плакатів до високотехнологічних кібератак і соціальних мереж [24, с.46].

а) Еволюція інформаційної боротьби: від Холодної війни до цифрової епохи [75, с.147].

Холодна війна стала поворотним моментом в історії розвитку не лише військових, але й інформаційних технологій. В умовах глобального протистояння інформація набуває стратегічного значення, а методи її отримання, обробки й поширення з кожним роком ускладнювалися та вдосконалювалися. Досвід Холодної війни у сфері медіа- та інформаційного впливу заклав основи для майбутніх цифрових стратегій, які сьогодні активно використовуються в умовах новітніх гібридних конфліктів [52, с.32].

У XXI столітті інформаційна війна значно трансформувалася, але її витоки – саме в тому періоді напруженого протистояння, коли формувалися ідеологічні

наративи, засоби впливу на масову свідомість і підходи до контролю над інформаційним середовищем.

Сучасні технології, такі як соціальні мережі, big data, штучний інтелект і технології стеження, є прямими спадкоємцями систем і методів, що були започатковані у другій половині XX століття. На відміну від радіо чи телебачення, сьогоднішні медіаплатформи дозволяють досягати набагато ширшої аудиторії за коротший час, а також здійснювати цільовий вплив, використовуючи алгоритми персоналізації контенту.

б) Інформаційна безпека як спадщина Холодної війни.

Холодна війна продемонструвала, наскільки вразливим може бути суспільство до маніпуляцій через мас-медіа. У сучасному світі, де дані стали однією з найцінніших ресурсів, інформаційна безпека вийшла на передній план. Протягом Холодної війни вперше почали формуватися концепції захисту інформаційних систем, криптографії, боротьби з дезінформацією. Відтоді еволюціонувало не лише технологічне забезпечення, а й методологія аналізу інформаційних загроз [48, с.75].

Кібербезпека, захист персональних даних, боротьба з фейковими новинами – усе це стало продовженням тих процесів, які виникли в умовах ідеологічної боротьби між США та СРСР. І сьогодні держави, компанії та громадяни змушені формувати нові моделі реагування на виклики цифрової доби, спираючись на досвід минулого.

в) Вплив Холодної війни на медіаграмотність суспільства.

Період Холодної війни змусив суспільства з обох сторін конфлікту критично оцінювати інформацію, що надходила з різних джерел. Люди навчалися аналізувати, порівнювати, розрізняти пропаганду та факти. Цей історичний досвід став передумовою для формування перших підходів до розвитку медіаграмотності – здатності критично осмислювати інформацію, розуміти її джерело, мету і вплив.

У сучасному світі, де інформаційний потік став практично неконтрольованим, а фейки поширюються зі швидкістю світла, розвиток

медіаграмотності є одним з ключових інструментів у протидії маніпуляціям. Досвід Холодної війни показує, що без критичного мислення суспільство стає надзвичайно вразливим до зовнішнього впливу [6, с.203].

г) Ідеологічний вплив як стратегічний інструмент у сучасності.

Як і під час Холодної війни, сьогодні боротьба за «серця й розуми» людей не припиняється. Проте змінилася форма – замість радіо й телебачення з'явилися TikTok, YouTube, Telegram-канали. Пропагандистські повідомлення маскуються під розважальний чи аналітичний контент. Проте суть залишилася тією ж: вплив на мислення, емоції та поведінку громадян через системне формування інформаційного середовища.

д) Виклики та шляхи протидії дезінформації у цифрову епоху.

У контексті інформаційних війн дезінформація стала не менш небезпечною, ніж традиційні форми агресії. Вона здатна підірвати довіру до державних інституцій, сприяти соціальній поляризації, провокувати паніку серед населення та навіть впливати на перебіг військових дій або політичних кампаній. Особливо вразливими до дезінформації є суспільства з високим рівнем цифрової активності та невисоким рівнем медіаграмотності [10].

З огляду на це, держави та міжнародні організації все більше приділяють увагу питанням протидії дезінформації та інформаційним маніпуляціям. Одним із ключових напрямів є розвиток медіаосвіти: впровадження програм критичного мислення, аналізу джерел інформації та виявлення маніпуляцій в освітніх закладах та через громадські ініціативи.

Крім того, уряди багатьох країн запроваджують інституційні механізми реагування на фейки та інформаційні атаки. Наприклад, створення центрів стратегічних комунікацій або інформаційних аналітичних груп, які займаються виявленням та спростуванням фейкових новин у режимі реального часу. Вони взаємодіють із соціальними мережами, надаючи докази маніпуляцій, а також формують державну комунікаційну політику у відповідь на інформаційні атаки [6, с.203].

Окрему роль відіграють алгоритмічні рішення, які розробляються платформами соціальних мереж з метою зниження поширення неправдивого контенту. Це, зокрема, маркування потенційно фейкових новин, зменшення охоплення підозрілих публікацій, а також блокування облікових записів, які систематично поширюють дезінформацію. Водночас такі дії викликають дискусії щодо балансу між свободою слова та інформаційною безпекою.

е) Етичні та правові аспекти боротьби з дезінформацією.

Боротьба з дезінформацією неможлива без чіткої правової бази. В умовах цифрового середовища необхідно формувати міжнародно визнані стандарти інформаційної безпеки. Проте тут постає серйозна проблема розмитість меж між цензурою та захистом інформаційного простору. Якщо надмірно обмежити контент можна порушити права громадян на свободу вираження. Якщо ж дозволити вільний потік інформації без регулювання відкривається простір для маніпуляцій, деструктивних наративів і втручання іноземних акторів [19,с.117].

Необхідна балансована система правових норм, яка дозволяє запобігати шкоді від дезінформації без придушення легітимної критики чи альтернативних точок зору. Особливо актуально для демократичних країн, які намагаються зберігати відкритість суспільного дискурсу, не втрачаючи при цьому контролю над загрозами.

є) Перспективи майбутнього: технології, які можуть змінити хід інформаційної війни.

Інформаційні війни, як і традиційні конфлікти, адаптуються до технологічного прогресу. На горизонті вже з’являються нові виклики використання штучного інтелекту для створення глибоких фейків (deepfakes), генеративних моделей для масового виробництва пропагандистського контенту, а також використання алгоритмів для маніпуляції масовою свідомістю на основі зібраних даних про поведінку користувачів [50, с.11].

Протистояти цим викликам можливо лише шляхом глобального об’єднання зусиль, інвестицій у дослідження безпечного розвитку цифрових технологій, впровадження етичних стандартів для розробників та виробників

цифрового контенту. Також зростає потреба у міжнародному регулюванні впливу новітніх технологій на інформаційне середовище [31, 280].

Можна стверджувати, що Холодна війна стала першим великим етапом в історії глобального інформаційного протистояння, заклавши фундамент для сучасних підходів до інформаційної боротьби. Роль технологій, медіа та ідеології у цьому процесі лише зросла. І сьогодні, як і раніше, контроль над інформацією залишається питанням національної безпеки [70; 74, с.147].

Продовжуючи розгляд проблематики інформаційних війн, слід наголосити, що сучасна геополітична ситуація вимагає не лише розуміння сутності інформаційного протистояння, а й активного формування стратегій інформаційного захисту. В умовах цифрового світу кожна країна, незалежно від рівня технологічного розвитку, може стати як джерелом, так і об'єктом інформаційного впливу. Означає, що питання кібербезпеки та інформаційної безпеки мають глобальний вимір і не можуть бути розв’язані ізольовано в межах однієї держави [19,с.115].

Із ключових тенденцій сучасності є еволюція інструментів інформаційного впливу: від традиційних ЗМІ до динамічних цифрових платформ, що мають здатність миттєво транслювати меседжі на мільйони користувачів. У цьому контексті особливого значення набуває боротьба з дезінформацією та фейковими новинами, які дедалі частіше використовуються як інструмент політичного впливу. Для ефективного протистояння таким викликам держави повинні не лише розвивати технічні засоби захисту, але й інвестувати в медіаграмотність населення, зокрема молоді, яка є найбільш вразливою до інформаційних маніпуляцій.

Спостерігається чітка тенденція до зростання ролі штучного інтелекту в інформаційних війнах. Генерація фейкових відео, зображень та текстів за допомогою нейромереж значно ускладнює виявлення джерела інформації та формує новий вимір інформаційних загроз. Підкреслює потребу у створенні спеціалізованих центрів аналітики, які могли б оперативно виявляти,

класифікувати та нейтралізовувати інформаційні атаки, орієнтуючись на алгоритмічний аналіз цифрового контенту.

Важливим аспектом у сфері міжнародної кібербезпеки є створення єдиної правової бази, яка б визначала правила поведінки держав у кіберпросторі. Наразі міжнародне право лише частково охоплює питання інформаційної безпеки, що дозволяє деяким суб'єктам міжнародних відносин діяти в «сірій зоні» правової невизначеності. Ініціативи, спрямовані на створення універсальних юридичних механізмів у цій сфері, потребують підтримки як з боку провідних держав світу, так і міжнародних організацій. Пріоритетним завданням має стати розробка кодексу поведінки в інформаційному просторі, який базувався б на принципах прозорості, відповідальності та взаємоповаги.

Значну роль у цьому процесі відіграють міжурядові структури, зокрема ООН, ОБСЄ, Європейський Союз та НАТО, які ініціюють резолюції, створюють робочі групи, координують дії країн-членів у випадку кіберінцидентів. Зокрема, в межах діяльності ООН відбувається обговорення концепції «відповідальної поведінки держав у кіберпросторі», що передбачає не лише запобігання агресії, а й розвиток довіри між державами. Водночас НАТО все активніше розвиває свою кіберстратегію, надаючи технічну, консультаційну та оборонну підтримку державам, які зазнають інформаційного тиску або атак.

Успішність міжнародної взаємодії у сфері кібербезпеки залежить також від участі недержавних акторів IT-компаній, громадських організацій, експертного середовища. Вони можуть відігравати посередницьку роль між урядами та суспільством, сприяючи розробці ефективних механізмів реагування на кіберзагрози. Створення мультиакторних платформ для обговорення та розробки політик у сфері інформаційної безпеки дозволяє охопити ширший спектр проблем і сприяє формуванню більш стійких та адаптивних моделей захисту [64, с.151].

Таким чином, майбутнє кіберпростору напряму залежить від здатності міжнародної спільноти діяти узгоджено, оперативно та відповідально. Інформаційні війни, які стали новим полем бою у XXI столітті, вимагають

переосмислення традиційних підходів до безпеки, поглиблення співпраці між країнами та активного залучення всіх зацікавлених сторін. Лише шляхом спільних зусиль можна сформувати безпечне, стійке та захищене інформаційне середовище для всього людства.

РОЗДІЛ 2
ІНФОРМАЦІЙНА ВІЙНА ЯК ІНСТРУМЕНТ ГІБРИДНОЇ АГРЕСІЇ

2.1. Основні методи ведення інформаційних операцій

У сучасну епоху стрімкої цифровізації, коли інформація стала ключовим стратегічним ресурсом, сутність конфліктів значно трансформувалася. Інформаційна війна, як складова гібридної агресії, дедалі більше визначає перебіг подій у глобальному політичному, економічному та безпековому просторі. Її методи дедалі витонченіші, адаптивніші та більш підступні. У центрі таких інформаційних операцій стоїть прагнення не стільки до фізичного знищення противника, скільки до його деморалізації, дезорієнтації та дестабілізації шляхом впливу на масову свідомість, уявлення про реальність і систему цінностей (табл. 2.1).

Таблиця 2.1

Основні складові інформаційної окупації як елементу гібридної агресії

Сфера впливу	Зміст дій РФ на окупованих територіях	Мета впливу
Телерадіомовлення	Блокування українських каналів, трансляція російських програм	Формування однобокої картини світу та легітимація окупації
Друковані та онлайн-медіа	Створення клонів російських медіа, цензура та пропаганда	Контроль над інформаційним полем
Освітня система	Впровадження російських підручників, викривлення історичних подій	Ідеологічне виховання молоді у проросійському ключі
Кіберпростір	Використання ботів, фейкових акаунтів, кібератак	Дискредитація України, деморалізація, ілюзія підтримки РФ
Культурна політика	Пропаганда «спільного минулого», просування російської культури	Підміна національної ідентичності, створення прив’язаності до РФ

Психоемоційний тиск	Інформаційна інтоксикація, залякування, хаос у повідомленнях	Зниження критичного мислення, втрата довіри до альтернатив

Джерело: розроблено на основі [12]

Одним із базових методів ведення інформаційної війни є масоване використання дезінформації, що передбачає цілеспрямоване поширення неправдивих або маніпулятивно спотворених даних з метою формування хибного уявлення про події, позиції сторін чи моральний стан населення. Така дезінформація не завжди є відвертою брехнею – часто вона подається фрагментарно, вирвана з контексту, або ж навмисне інтерпретується у вигідному для агресора ключі [13, с.50].

Другим ключовим методом є поширення фейкових новин та діпфейків, що з допомогою сучасних технологій штучного інтелекту набули високого рівня достовірності. Зображення, відео та аудіо, створені штучно, але стилізовані під автентичні матеріали, дозволяють не лише дискредитувати окремих політичних діячів чи інституції, але й викликати масову недовіру до медіа як джерела правди загалом.

Не менш небезпечним методом є створення альтернативної інформаційної реальності – цілеспрямоване нав'язування певного наративу, який базується на симулякрах, тобто інформаційних конструктах, що лише зовні нагадують правду. В такій реальності агресор – герой, а жертва – провокатор; правозахисні кроки сприймаються як репресії, а міжнародна допомога трактується як втручання у внутрішні справи. Цей метод забезпечує не лише дезорієнтацію широких мас, а й створює глибокі розколи в суспільстві, поляризуючи громадську думку.

Особливої ваги в умовах гібридного конфлікту набуває інформаційно-психологічний тиск, що здійснюється через емоційно насичений контент: тривожні повідомлення, драматичні кадри, повідомлення про нібито невдачі чи втрати. Це формує відчуття постійної загрози, безсилля, втрати контролю, що

веде до масової апатії або паніки. У підсумку суспільство поступово втрачає здатність до критичного мислення і стає вразливим до зовнішніх маніпуляцій.

Способом впливу є системна дискредитація національних інституцій. Через підконтрольні інформаційні платформи формуються негативні уявлення про владу, армію, громадянське суспільство. Застосовується стратегія підриву довіри – будь-яка помилка чи внутрішній скандал гіперболізується, зводячи нанівець навіть успішні ініціативи. Дозволяє агресору досягти двох цілей: послабити управлінську стійкість держави та викликати зневіру в її громадян.

Суттєвим інструментом залишається інформаційне зараження через соціальні мережі. Завдяки алгоритмам персоналізації контенту, ворожі актори мають змогу цілеспрямовано впливати на окремі аудиторії – за віком, політичними переконаннями, мовою тощо. Через ботів, тролів і псевдоблогерів розповсюджуються меседжі, що розхитують єдність, провокують протистояння між різними верствами населення, створюючи ілюзію масовості певних настроїв [87].

На особливу увагу заслуговує використання культурних кодів, історичних символів і мемів, які агресор включає до свого інформаційного арсеналу. Через них відбувається не лише викривлення історичної пам’яті, а й нав’язування чужої ідентичності, що в умовах війни рівнозначне інформаційному колоніалізму. За допомогою таких «смислових маркерів» агресор не лише модифікує сприйняття минулого, а й впливає на бачення майбутнього.

Усі згадані методи є складовими інформаційно-психологічних операцій (ІПсО) – скоординованих дій, спрямованих на зміну когнітивних установок, емоційного стану та поведінки об’єкта впливу. Операції мають чітку стратегічну мету: не допустити консолідації суспільства, деморалізувати населення і підірвати обороноздатність країни не силою, а словом і образом [79, с.137].

Системний аналіз методів інформаційного впливу у контексті гібридної війни, варто звернути особливу увагу на спосіб, у який Російська Федерація формує контрольоване інформаційне середовище на тимчасово окупованих територіях. Така стратегія передбачає не лише фізичну присутність ворожих

військових формувань, але й створення комплексної моделі інформаційного панування, що охоплює медіа, цифрову інфраструктуру, культурну політику та систему освіти [35].

Фундаментальним інструментом у цьому процесі стало повне перезавантаження інформаційної екосистеми: блокування доступу до українських телеканалів, друкованих та електронних медіа, витіснення українського культурного наративу з публічного простору, створення клонів російських медіаструктур, які заміщують місцеві ЗМІ. Встановлення інформаційної ізоляції, поєднане з агресивною пропагандистською кампанією, дозволяє формувати альтернативну реальність, де російські наративи сприймаються як об'єктивна істина (рис. 2.1).

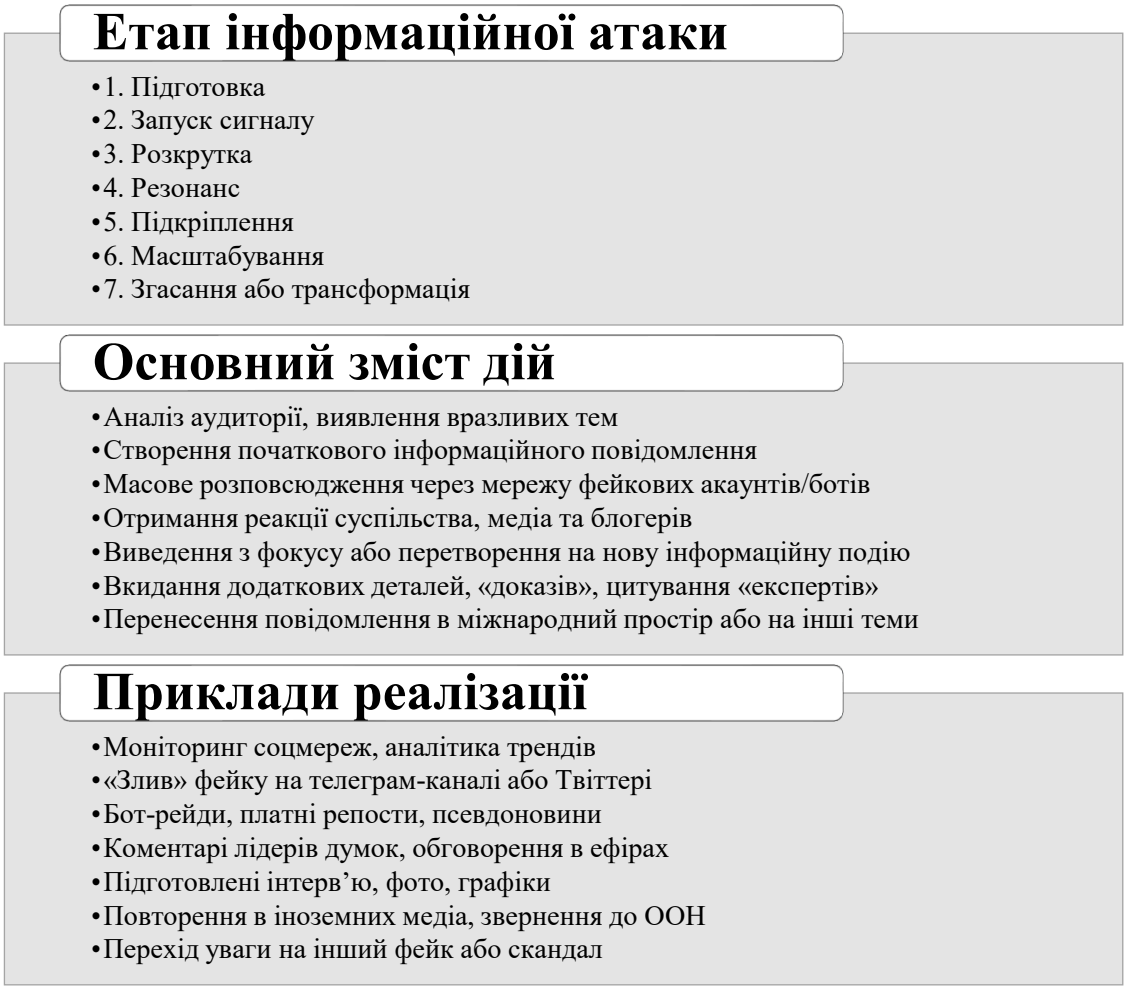

Рис.2.1.Структурна модель сценарію інформаційної атаки у гібридній війні

На структурному рівні цей контроль реалізується через створення квазідержавних інституцій, які імітують функціонування органів державної влади України, проте повністю координуються з Кремлем. Особлива роль відводиться формуванню міністерств інформаційної політики, підконтрольних окупаційним адміністраціям, що діють за калькою російських державних структур. Через такі органи здійснюється вертикальний розподіл інформаційних меседжів, визначається редакційна політика підконтрольних ЗМІ, координуються інформаційні атаки, зокрема у цифровому середовищі [8; 88, с.54].

Важливим інструментом є також інституціоналізація пропаганди в освітній сфері. Шкільні програми, адаптовані за зразком російської освітньої політики, впроваджують спотворену версію історії, виправдовують агресію РФ, формують лояльне ставлення до окупаційної влади. Таким чином, інформаційна війна набуває не лише оперативного, а й стратегічного виміру, формуючи майбутнє покоління у парадигмі викривлених цінностей і наративів [29, с.58].

Однією з найнебезпечніших форм впливу в цьому контексті є інформаційна інтоксикація – цілеспрямоване перенасичення медіапростору емоційно зарядженими, суперечливими або недостовірними повідомленнями. Створює відчуття інформаційної втоми, викликає недовіру до будь-яких джерел, посилює залежність від «офіційної» точки зору окупаційної влади. В умовах постійного інформаційного тиску зникає критичне мислення, а будь-яка альтернативна думка автоматично трактується як ворожа.

Суттєвою особливістю стратегії РФ є використання концепту «м'якої сили» через культурну експансію: трансляцію російських фільмів, концертів, популяризацію російських героїв, організацію культурних заходів, орієнтованих на ностальгійне відтворення «спільного радянського минулого». Дозволяє формувати відчуття єдності з «великою Росією», підміняючи поняття національної ідентичності, мови та історії.

Слід згадати про активне використання кіберпростору для створення хибних інформаційних картин, зокрема за допомогою бот-мереж, фейкових

акаунтів, інформаційних атак на незалежні джерела інформації. Дозволяє не лише формувати ілюзію громадської підтримки політики Кремля, а й цілеспрямовано дискредитувати українських лідерів, військових та активістів. Така діяльність не лише підриває авторитет української влади, а й створює передумови для легітимізації окупаційних структур у свідомості населення.

Усе це свідчить про те, що інформаційна агресія на окупованих територіях не є другорядною складовою гібридної війни. Вона виконує стратегічну функцію консолідації контролю, впровадження ідеологічного наративу та довготривалої маніпуляції масовою свідомістю, що в сукупності створює перешкоди для процесів деокупації, реінтеграції та побудови стабільного демократичного простору після завершення збройного конфлікту [88, с.54].

Створення штучної інформаційної реальності на окупованих територіях є не просто засобом пропаганди, а складовою частиною великої стратегії інформаційного поневолення, що чинить довготривалий вплив на свідомість, ідентичність та політичну поведінку населення, яке проживає в умовах постійної інформаційної облоги.

Методи ведення інформаційної війни в умовах гібридної агресії охоплюють цілу низку як відкритих, так і прихованих інструментів впливу, що ґрунтуються на сучасних інформаційно-комунікаційних технологіях і психологічних механізмах впливу. Від ефективного виявлення, аналізу та нейтралізації таких методів значною мірою залежить інформаційна безпека держави, збереження суверенітету та стабільність демократичних процесів у суспільстві [7, с.111].

У таблиці 2.2 та 2.3 подано формати інформаційного впливу у цифровому середовищі та види ботів у системі інформаційної атаки

Таблиця 2.2

Формати інформаційного впливу у цифровому середовищі

Формат впливу	Канали поширення	Приховане навантаження

Меми та візуальний гумор	Instagram, Telegram, Reddit, TikTok	Знецінення, висміювання, дискредитація
Емоційні відеоролики	YouTube, Facebook, TikTok	Виклик страху/співчуття, посилення драми
Псевдоаналітика	YouTube-блоги, фейкові «розслідування»	Надання брехні вигляду об'єктивності
Анонімні телеграм-канали	Telegram	Спотворення фактів, поширення паніки
Інфографіка з перекрученими даними	Twitter, презентації, вікі-сайти	Легалізація фейку через візуальний формат
Інтерактивні карти або графіки	GIS-боти, Telegram-канали, сайти	Псевдооб'єктивність, геоінформаційний тиск

Джерело: розроблено на основі [35, с.138]

Таблиця 2.3

Види ботів у системі інформаційної атаки

Тип бота	Основне завдання	Поведінкові риси
Ретвіт-боти	Поширення контенту з ключовими тегами	Висока активність без оригінального контенту
Коментарні боти	Імітація підтримки/критики	Однотипні меседжі, агресивні або зловтішні тону
Інфо-боти	Вкидання псевдоаналітики	Використання технічної або експертної лексики
Боти-перевертні	Створення видимості «прозріння»	Зміна позиції: «раніше був за, тепер проти»
Гіперактивні боти	Спамлення у всіх темах одночасно	24/7 онлайн, нав'язливість, постійні теги/згадки

Джерело: розроблено на основі [7, с.111]

Інформаційні операції у контексті гібридної агресії Росії проти України передбачають використання багаторівневої системи інструментів впливу, які об'єднують класичні прийоми психологічної війни, інноваційні цифрові технології, а також глибоку соціокультурну інженерію. Основною метою таких

операцій є не лише вплив на опонента в умовах збройного протистояння, але й тривала трансформація свідомості, деморалізація, дестабілізація внутрішнього інформаційного простору та легітимізація окупаційного режиму.

Одним із наріжних каменів є маніпуляція фактами: подача правдивої інформації в перекрученому контексті, використання емоційно забарвленої лексики, драматизація, або, навпаки, замовчування ключових подій. Та дозволяє формувати викривлену картину реальності без прямої фальсифікації фактів.

Також активно застосовується метод масового повторення (ефект «тисячі джерел») – багаторазове тиражування одного й того самого повідомлення через різні платформи для створення ілюзії об'єктивної істини. У межах такого підходу значну роль відіграють ботоферми, фейкові акаунти, дезінформаційні сторінки у соціальних мережах, а також легітимізовані пропагандистські медіа.

Не менш ефективним є використання емоційно заряджених наративів: страху, ненависті, героїзації, зради. Такі наративи сприяють поділу суспільства, радикалізації окремих груп, підвищенню градусу суспільного напруження [89].

Інформаційні атаки реалізуються шляхом імітації громадського резонансу (інформаційні хвилі, твітер-шторми), у межах яких інформація поширюється під виглядом спонтанної реакції соціуму. Посилює ефект соціального підтвердження та змушує користувача вважати певну позицію загальноприйнятою.

У таблиці 2.4 подано систематизацію основних методів ведення інформаційних операцій.

Таблиця 2.4

Класифікація методів ведення інформаційних операцій у гібридній війні

Метод впливу	Засоби реалізації	Цільове спрямування
Перекручування фактів	Напівправда, зміщення акцентів, зміна контексту	Формування викривленої реальності

Масове повторення	Синхронне тиражування через ЗМІ, соцмережі, телеграм-канали	Закріплення інформації як «очевидної істини»
Створення інформаційного шуму	Навмисне перенасичення простору суперечливими повідомленнями	Деморалізація, апатія, зниження довіри
Емоційна мобілізація	Використання страху, гніву, героїзації, образу ворога	Поляризація суспільства, стимулювання радикальних настроїв
Імітація громадської думки	Боти, фейки, коментарі на замовлення, лайки, флешмоби	Ілюзія масової підтримки
Дискредитація	Спрямована критика, меми, фотожаби, звинувачення в зраді	Знищення авторитету опонента
Псевдоекспертність	Публікації під виглядом аналітики, коментарі «експертів»	Надання фальшивій інформації вигляду наукової або офіційної
Культурна інженерія	Впровадження нових смислів, альтернативна історія, символіка	Зміна національної ідентичності

Джерело: розроблено на основі [1, с.15]

Таким чином, інформаційна операція у гібридній війні – це не випадковий процес, а високотехнологічна стратегія, побудована на точному психологічному розрахунку, що поєднує елементи масової культури, нейролінгвістичного програмування та кібермеханізмів впливу на суспільну свідомість. Її ефективність залежить від здатності цільової аудиторії критично мислити, а також від рівня стійкості національного інформаційного простору.

2.2. Маніпуляції, пропаганда та фейки як інструменти впливу на суспільство

У контексті сучасних гібридних конфліктів, таких як російсько-українська війна, війна в Сирії, втручання у вибори в США та інформаційні кампанії Китаю щодо Тайваню, особливої актуальності набувають питання маніпуляцій,

пропаганди та поширення фейкової інформації як складових елементів інформаційної агресії. Інструменти є ключовими у боротьбі за свідомість мас, формування сприйняття подій і легітимізацію певної політичної лінії. Пропаганда та дезінформація стають інструментами стратегічного контролю над реальністю, що поширюється через цифрові медіа, телебачення, соціальні мережі та навіть через культурні наративи.

На відміну від нейтрального інформування, пропаганда – це процес, що цілеспрямовано формує бажану картину світу через емоційний вплив, відбір фактів, створення символічного контексту. Її головна мета – не передача об'єктивної інформації, а вплив на переконання і поведінку мас, у тому числі шляхом заміни реальності симулякрами – образами, що імітують дійсність [32, с.25].

Такі техніки були масово використані Росією не лише проти України (фейкові новини про «розіп'ятих хлопчиків», «біолабораторії НАТО» тощо), а й під час війни в Сирії, де пропагандистські ресурси намагалися дискредитувати «Білі шоломи» – організацію, яка документувала наслідки авіаударів. У США ж 2016 року масована кампанія дезінформації з боку російських тролів і ботів була спрямована на розпалювання соціальної напруги та втручання у вибори (табл. 2.5).

Таблиця 2.5

Порівняльна характеристика пропагандистських кампаній у гібридних війнах

Конфлікт	Основні інструменти пропаганди	Ціль впливу	Приклади маніпуляцій
Російсько-українська	Симулякри, телебачення, боти, Telegram-канали	Легітимізація агресії, демонізація супротивника	«Фашисти в Києві», «біолабораторії НАТО»
Сирійська війна	Звинувачення у фейкових хіматаках, дискредитація гуманітарників	Захист режиму Асада, делегітимація опозиції	Відео з постановками «Білих шоломів»

США, 2016 (вибори)	Мем-контент, бот-ферми, розпалювання конфліктів	Дестабілізація демократії, вплив на результат	«Pizzagate», масові фейкові акаунти
Китай – Тайвань	Вкидання про біолабораторії, загрози «об'єднання» силою	Страх, підрив авторитету Тайваню	Меметизація лідерів, спотворення фактів

Пропаганда у гібридних війнах зазвичай супроводжується маніпуляціями – прихованими формами впливу, що передбачають підміну понять, зміщення акцентів, емоційну драматизацію. Типовими є фейкові новини, що апелюють не до логіки, а до емоцій. Їхній вплив небезпечний тим, що вони здатні змінювати погляди мас без усвідомлення цього аудиторією (табл. 2.6).

Таблиця 2.6

Типологія фейкових повідомлень у гібридних війнах

Тип фейку	Механізм дії	Приклад
Абсолютний фейк	Повністю вигаданий факт	«Зґвалтування дітей українськими військовими»
Маніпулятивний фейк	Зміщення контексту або підміна частини правди	Відео з інших конфліктів, видане за нове
Фейк-пародія	Сатира, яку видають за серйозну інформацію	Мемні новини, які сприймаються як реальні
Токсичний фейк	Емоційне маніпулювання із шок-контентом	Фото нібито жертв «українських обстрілів»
«Фейк-уточнення»	Подання фейку з посиланням на «анонімне джерело»	«Джерела повідомляють про наступ НАТО»

Джерело: розроблено на основі [6, с.204]

Сьогодні, в умовах інформаційної перенасиченості, найбільш небезпечними є саме гібридні фейки, які частково базуються на достовірних даних, що ускладнює їх спростування. Вони швидко поширюються в мережах через емоційну залученість користувачів, створюють альтернативну реальність і змінюють суспільну поведінку.

Телебачення, зокрема, зберігає потужний вплив, перетворюючи події на ідеологічні міфи. За словами Г. Почепцова, ми живемо у світі чужої інформації, яку сприймаємо через призму зовнішніх повідомлень, часто без можливості перевірити її правдивість. Цим активно користуються авторитарні режими, створюючи довготривалі наративи для контролю над населенням (табл. 2.7).

Таблиця 2.7

Маніпулятивні технології у гібридній війні: характеристика та вплив

Технологія	**Суть дії**	**Емоційна мета впливу**	**Географія використання**
Симулякр	Створення вигаданих образів замість реальності	Впровадження хибної реальності	РФ, Китай
Наративна агресія	Побудова ідеологічної схеми (герой-зрадник-ворог)	Поляризація, ескалація	США, Угорщина, Білорусь
Використання культурних символів	Дискредитація історії, мови, традицій	Позбавлення ідентичності	Сирія, Україна
Псевдоекспертність	Просування думок фейкових аналітиків	Створення ілюзії об’єктивності	Глобально

Джерело: розроблено на основі [35, с.140]

У сучасному інформаційному просторі маніпуляції, пропаганда та фейки перетворилися на потужну зброю, яка здатна трансформувати суспільну свідомість, впливати на політичні рішення, створювати ворожі наративи та руйнувати основи демократії. Росія, особливо під час війни проти України, демонструє вражаючий масштаб і системність використання цих інструментів для досягнення своїх геополітичних цілей. Інформаційний вплив стає частиною ширшої стратегії гібридної війни, де дезінформація служить не лише підтримкою бойових дій, а й самостійною формою агресії [53, с.113].

Пропаганда, яку просуває Кремль, не є спонтанною чи хаотичною – вона побудована на ретельно вивіреній ідеологічній та емоційній конструкції. Основна мета – формування викривленої картини світу, у якій Росія постає як останній бастіон «традиційних цінностей», «миротворець», «захисник братніх народів» або «жертва агресивного Заходу». У цій парадигмі будь-яка протидія з боку України чи міжнародної спільноти зображується як ворожа кампанія, натомість дії самої Росії подаються як необхідні, справедливі або вимушені [54, с.207].

Фейки – це складова цієї системи, яку активно використовують не лише державні ЗМІ Росії, а й лояльні до Кремля так звані «альтернативні» закордонні медіа. Пропагандистські фабрики зосереджуються на створенні емоційно забарвленого контенту, який апелює до страху, гніву, ненависті та моральної розгубленості аудиторії. Як наслідок, люди нерідко втрачають здатність до критичного мислення, не розрізняють факти й інтерпретації, починають сприймати вигадані наративи як правду [6, с.204].

Особливу загрозу становлять гібридні інформаційні атаки, які поєднують у собі частково достовірні факти з навмисно спотвореною інтерпретацією. Та дозволяє пропаганді виглядати правдоподібно, а отже – набагато небезпечніше. У випадку з Україною типовими стали міфи про «нацизм», «утиски російськомовного населення», «громадянську війну», «постмайданну анархію». Такі конструкції транслюються масово, повторюються на різних платформах, підтримуються ботами і арміями тролів, що формують ілюзію загального консенсусу.

Маніпуляція суспільною свідомістю особливо ефективна тоді, коли вона спрямована на вразливі групи населення – людей із низьким рівнем медіаграмотності, обмеженим доступом до якісних джерел інформації або таких, що перебувають у стресових, кризових умовах (наприклад, у зоні бойових дій чи на окупованих територіях). У таких умовах брехня може здаватися переконливою, а правда – занадто складною або неймовірною.

Варто також підкреслити, що пропаганда рідко працює в ізоляції. Вона ефективна саме тоді, коли вбудована в ширшу систему дій: дипломатичний тиск, економічні шантажі, кібератаки, роздмухування міжнаціональної ворожнечі, релігійних конфліктів, підтримка радикальних рухів у європейських державах. Усе це – елементи того самого гібридного механізму, що має на меті розхитати стабільність, створити розкол і посіяти зневіру [12].

Фейки, як елемент інформаційної війни, мають ще одну небезпечну характеристику – вони здатні самовідтворюватися. Люди, які раз піддалися дезінформації, часто самі стають її носіями: поширюють через соціальні мережі, діляться в побуті, підтримують у публічних дискусіях. У результаті формується замкнене коло: чим більше фейків – тим більше носіїв дезінформації, і тим складніше розірвати цю пастку [82, с.127].

Наслідки такого впливу – катастрофічні. Йдеться не лише про викривлене сприйняття подій, але й про дегуманізацію противника, деморалізацію власного суспільства, роз'єднання громадян, зростання ворожнечі, недовіри, ксенофобії. Російська пропаганда використовує лексичні маркери та риторику, покликану позбавити опонентів людських рис, представити їх як «небезпечних», «дикіх», «фашистів», «зрадників», що створює психологічне підґрунтя для виправдання насильства й агресії [54, 207].

Боротьба з такими інформаційними атаками вимагає не лише технічних чи юридичних засобів, але й активної просвітницької діяльності, розвитку критичного мислення, медіаграмотності, обізнаності громадян про природу дезінформації та її механізми. Освітні інституції, журналістські спільноти, організації громадянського суспільства та держава повинні діяти синхронно, щоб створити стійку інформаційну екосистему [33, с.323].

У підсумку, маніпуляції, фейки та пропаганда, які активно застосовує російський режим – це не просто засоби політичного впливу. Інструменти руйнації, здатні паралізувати волю суспільства, підірвати демократію та гуманістичні цінності, а отже – перетворити інформацію на зброю масового ураження. У таких умовах протидія – це не лише захист України, а й оборона

глобального демократичного ладу, який російська імперська машина прагне знищити.

Таким чином, маніпуляції, пропаганда та фейки стали потужними інструментами впливу в глобальних гібридних конфліктах. Їх використання не обмежується локальними цілями, а спрямоване на стратегічну зміну політичного ландшафту, культурної ідентичності та суспільної свідомості. Протистояти цьому можна лише через розвиток критичного мислення, медіаграмотності, міжнародного моніторингу інформаційного простору та посилення етичних стандартів у журналістиці

2.3. Приклади застосування інформаційних технологій у відомих гібридних війнах

Інформаційна війна як ключовий інструмент гібридного протистояння сьогодні відіграє надзвичайно важливу роль у системі національної та міжнародної безпеки. Вона являє собою форму конфлікту, в якому боротьба ведеться не на полі бою з використанням зброї, а в цифровому просторі, у свідомості людей, через слова, зображення, емоції, сенси та символи. Важливим є те, що цей тип війни позбавлений чітких географічних меж, а головною його особливістю є невидимість, розмитість джерел атак і складність їх ідентифікації. Саме в такому вигляді інформаційна війна стала невід'ємним елементом гібридних війн, зокрема з боку Російської Федерації проти України, Заходу та інших демократичних держав.

Історично термін «інформаційна війна» вперше був використаний американським аналітиком Томасом Рона у 1976 році в його звіті «Системи зброї та інформаційна війна», підготовленому для корпорації «Боїнг». У цьому звіті він звернув увагу на те, що інформаційна інфраструктура стає не лише життєво важливою частиною економіки, а й особливо вразливою до атак у мирний та воєнний час. Вже з 1980-х років ця ідея стала предметом глибоких досліджень у військових колах США, де з'явилося розуміння того, що інформація може бути

не лише ресурсом чи засобом передачі знань, а й зброєю та об'єктом нападу [29, с.58].

У гібридних війнах, які передбачають одночасне поєднання воєнних, політичних, економічних, дипломатичних, кібер- та інформаційних засобів впливу, інформаційні технології стали надзвичайно ефективним засобом досягнення стратегічних цілей. Однією з головних переваг такого підходу є можливість впливати на поведінку великих мас населення, владних еліт і військових структур без безпосереднього застосування військової сили. Достатньо змінити інтерпретацію реальності, трансформувати систему цінностей та уявлень суспільства, щоб посіяти хаос, зневіру, розкол і підкорити його зсередини.

Одним із найяскравіших прикладів використання інформаційних технологій у гібридній війні стала агресія Росії проти України, що триває з 2014 року і досягла апогею у 2022 році. Кремль активно використовував медіа-ресурси, соціальні мережі, бот-мережі, телеграм-канали, фейкові новини, пропагандистські фільми та візуальні матеріали для формування у громадян Росії, мешканців окупованих територій і навіть частини західного населення перекрученого образу реальності. Наприклад, основними наративами стали твердження про «громадянську війну в Україні», «утиски російськомовних», «фашистський переворот» на Майдані та інші фейки, що мали за мету не лише виправдати агресію, але й деморалізувати українське суспільство, ізолювати його на міжнародній арені.

Один показовий випадок – втручання Росії у президентські вибори у США 2016 року. У межах гібридної операції під прикриттям інформаційної кампанії було створено десятки тисяч фейкових акаунтів у соціальних мережах, які поширювали поляризуючі повідомлення, розпалювали ворожнечу, дискредитували політичних опонентів певного кандидата, маніпулювали фактами та створювали ілюзію «народного невдоволення». Втручання виявилося настільки масштабним, що розслідування його наслідків тривало кілька років та призвело до перегляду інформаційної безпеки у багатьох країнах [64, с.151].

У Сирії, ще одному театрі гібридної війни, інформаційні технології застосовувалися для створення вигідної Росії та її союзникам картини конфлікту. За допомогою соціальних мереж поширювалися постановочні відео, сфабриковані репортажі про «хімічні атаки повстанців» або «провокації Заходу», водночас приховуючи злочини режиму Асада та російської авіації. Такі інформаційні кампанії мали на меті вплинути на міжнародну думку та мінімізувати критику з боку світової спільноти [55, с.45].

Увагу заслуговують кібератаки, які доповнюють інформаційні кампанії в межах гібридної війни. Злам урядових сайтів, розсилання фішингових листів, проникнення у системи критичної інфраструктури – все це часто супроводжується потужними хвилями дезінформації, спрямованими на підрив довіри до влади та дестабілізацію суспільного порядку. Кібератаки на Україну – від вірусів типу NotPetya до атак на державні реєстри – стали невід'ємною частиною гібридного наступу [12].

Гібридна війна XXI століття – це не лише зіткнення армій, а передусім боротьба за контроль над інформаційним простором. В епоху цифрових технологій, де мільйони людей отримують новини через соцмережі й месенджери, а інформаційні джерела нерідко мають сумнівне походження, саме маніпуляції, фейки та інформаційні вкиди здатні змінювати хід історії. Тому завданням держав, міжнародних організацій і громадянського суспільства є не лише фіксація фактів такої агресії, а й розробка ефективних стратегій протидії. Розпізнавання гібридного впливу, захист інформаційної суверенітету та розвиток критичного мислення населення – це ключові умови виживання демократії в умовах новітніх війн [16; 36].

Розгляд інформаційної війни як ключового інструменту сучасних гібридних конфліктів, варто звернути увагу на її багаторівневу структуру, що дозволяє системно й послідовно впливати на суспільну свідомість, руйнувати основи стабільності держав, підривати демократичні інститути та провокувати внутрішні конфлікти. Сутність інформаційного впливу полягає не лише у

передачі викривлених фактів чи поширенні фейків – це глибокий багатошаровий процес, який вбудовується в ціннісні орієнтири суспільства та особистості [83].

Перший рівень – емпіричний полягає у навмисному перекручуванні фактів в політичній, економічній, культурній та інших сферах. На цьому рівні народжуються фейкові новини – потужна зброя у боротьбі за вплив, що використовуються для дестабілізації внутрішньополітичної ситуації та дискредитації інституцій. Такі повідомлення рідко апелюють до раціонального мислення – вони спираються передусім на емоційне сприйняття, використовуючи образи, відео, маніпулятивні заголовки. Метою є швидке формування емоційної реакції: обурення, страху, ненависті. Водночас іде підміна понять, коли правду заміщують ідеологічно зручні фальсифікати [71, с.15].

Другий рівень – концептуальний пов'язаний із структурованим і цілеспрямованим формуванням інтерпретацій. Саме на цьому рівні здійснюється конструювання наративів, через які населення сприймає події. Тут важливо не тільки що повідомляється, а й як саме подається інформація, в якому контексті, з якою інтонацією. Поле боротьби за сенс. Якщо у суспільства немає доступу до альтернативного тлумачення, а критичне мислення відсутнє – громадяни починають ототожнювати запропоновану інтерпретацію з істиною.

Третій рівень – смисловий найглибший і найнебезпечніший. Тут націлено на зміну екзистенційних цінностей, на переформатування ідентичності, світогляду, уявлень про добро і зло, справедливість, державність, гідність. Вплив здійснюється через повторюване нагнітання страху, дегуманізацію ворога, висміювання власної культури та героїв. Рівень інформаційного терору, на якому людина може повністю втратити здатність до незалежного мислення (рис. 2.2).

Рис. 2.2. Цілі інформаційної війни

Інформаційні війни можуть розгортатися в будь-яких сферах життя, охоплюючи як приватну комунікацію між індивідами, так і глобальні міжнародні відносини. Але в усіх випадках найпотужнішою зброєю залишається сама інформація, яка здатна змінювати не лише свідомість, а й поведінку, політичну позицію, навіть ментальність суспільств (рис. 2.3) [78, с.2].

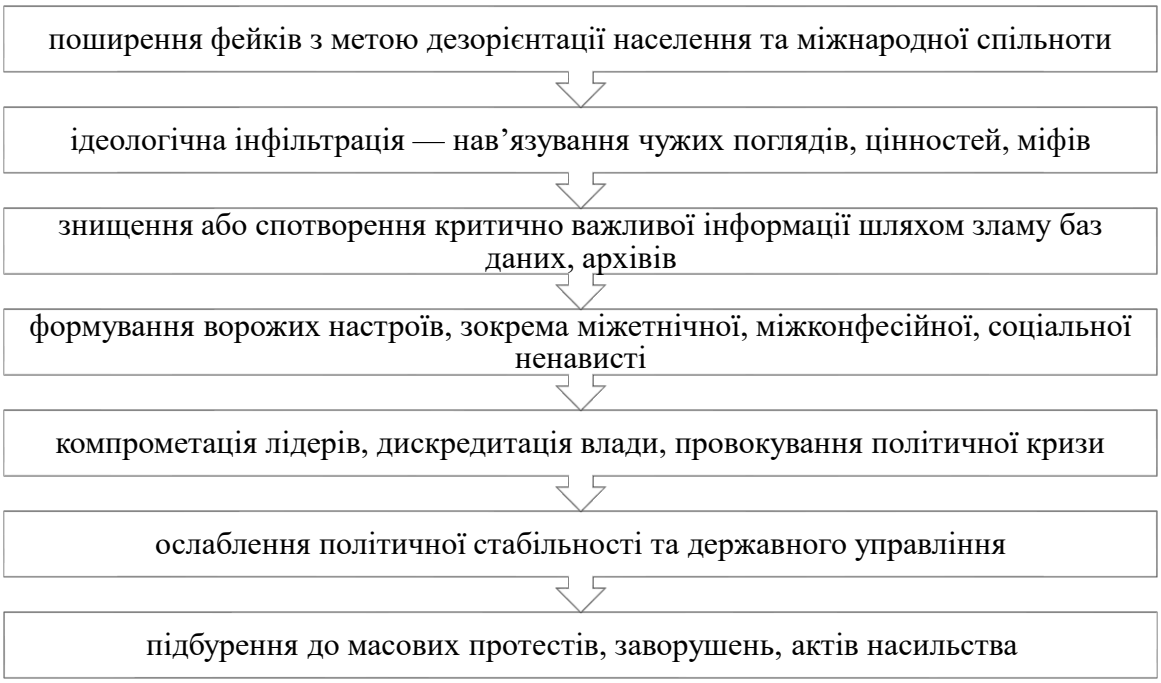

Рис. 2.3. Ключові завдання, які вирішує інформаційна війна

Особливу увагу в межах гібридної війни приділяють інформаційно-психологічному впливу – створенню стійкого емоційного стану тривоги, розпачу, ненависті, параної. Такий вплив супроводжується ще одним потужним механізмом – зовнішнім тиском через санкції, економічні війни, політичну ізоляцію, що лише посилює ефект від пропаганди, оскільки соціальні проблеми починають трактуватися як результат «зради», «впливу ворога», «зовнішнього управління» [90].

Система інформаційного тиску може супроводжуватися підтримкою внутрішніх деструктивних сил. Опозиційні політичні сили, неурядові організації чи навіть популярні блогери можуть стати носіями вигідних противнику ідей, які посилюють розкол суспільства, знижують довіру до держави і мобілізують населення проти легітимної влади.

Інформаційна війна стала однією з найнебезпечніших форм гібридної агресії, що загрожує національній безпеці сучасних держав. Її суть полягає у досягненні інформаційної переваги, яка дозволяє впливати на поведінку громадян, політичної еліти, військових, формувати та моделювати громадську думку у вигідному для агресора руслі. Особливістю цієї війни є те, що вона не має чіткої лінії фронту, її операції майже не фіксуються, а виконавці залишаються невідомими. Інформаційна війна розширює простір ведення бойових дій у нематеріальній площині – сфері ідей, цінностей, переконань, де ключову роль відіграє не сила, а вплив [44].

Перші концепції інформаційної війни з’явилися у 1970-х роках. Американець Томас Рона в доповіді «Системи зброї та інформаційна війна» (1976) звернув увагу на вразливість інформаційної інфраструктури США, що водночас стала й основою економіки країни. Відтоді питання інформаційного протистояння почало активно розвиватися у військових колах. Було визнано: інформація є не лише ціллю, а й зброєю, здатною дестабілізувати державу без фізичного втручання [44].

Інформаційна війна складається з цілеспрямованих дій для досягнення переваги над супротивником через вплив на інформаційні системи й інформацію.

Її збитки мають переважно психологічний характер: деструкція свідомості, зміна поглядів, переконань, нав'язування нових цінностей. Особливо вразливою до таких атак є молодь та владна еліта. Основна мета – домогтися капітуляції або хаосу без єдиного пострілу, перепрограмувавши ментальний простір країни-жертви [41].

Інформаційна війна, як частина гібридного конфлікту, охоплює кілька рівнів. На емпіричному рівні розповсюджуються фейкові новини, перекручуються факти, створюються емоційні вкиди, що підмінюють об'єктивне сприйняття реальності. Концептуальний рівень пов'язаний із способами подачі, організації та інтерпретації інформації як вона виглядає, які смисли в неї закладено. Найнебезпечнішим є смисловий рівень, на якому відбувається глибинне переписування системи цінностей суспільства, нав'язування чужих ідеологем.

Інформаційна війна охоплює всі сфери від міжособистісної до міждержавної. Її мета – контроль над інформаційним простором, каналами комунікації та змістом повідомлень. Серед основних завдань інформаційного тиску: дезінформація населення, знищення архівів і баз даних, дестабілізація економіки, дискредитація політичного керівництва, послаблення міжнародного впливу, розпалювання міжнаціональної ворожнечі, просування чужих культурних цінностей, організація масових заворушень, підтримка опозиційних рухів тощо [41].

Одним із ключових інструментів такої війни є інформаційно-психологічна війна, що є органічною складовою гібридних конфліктів. Вона передбачає цілеспрямований вплив на свідомість, волю та емоції мас з метою змінити мотивацію, переконання, посіяти страх, безпорадність і невпевненість. У психологічній війні допускаються всі методи впливу, включаючи морально неприйнятні дії від поширення чуток до саботажу, провокацій, терору. Війна ведеться не лише проти зовнішнього ворога, а й проти власного населення – з метою його контролю та мобілізації в умовах внутрішніх і зовнішніх загроз [81].

Психологічна війна здійснюється через інформаційно-психологічні операції, що можуть бути інформаційно-технічними (вплив на телекомунікаційні системи, бази даних, управлінські процеси) або інформаційно-психологічними (вплив на особовий склад ЗС, населення, політичну еліту, інтелігенцію). Операції проводяться в мирний час, у фазі військового конфлікту та після його завершення. Вони спрямовані на ослаблення волі до спротиву, розкол в суспільстві, делегітимацію влади, дискредитацію політики держави в очах міжнародної спільноти.

У межах гібридної війни, психологічний тиск часто реалізується без відкритої агресії. Противник закликає до "мирного врегулювання", критикує військову політику країни-жертви, просуває альтернативні наративи, формує міжнародну думку на свою користь, підтримує внутрішні опозиційні сили, вдається до демонстрації сили, економічного тиску, культурної ізоляції (рис. 2.4).

Рис. 2.4.Основні методи інформаційно-психологічного впливу

Будь-яка ефективна ІПсО супроводжується зворотним зв’язком: ретельним моніторингом інформаційного середовища, оцінкою реакції цільової аудиторії, аналізом ефективності поширення ідеологем, коригуванням стратегії впливу.

Інформаційно-психологічна війна є не просто частиною гібридного протистояння вона є його ядром. Від її ефективності залежить не лише успіх військової кампанії, а й політична стабільність, громадянська єдність і навіть культурна ідентичність нації. У сучасних умовах захист інформаційного простору є таким же важливим, як і оборона територіальної цілісності держави [81].

Таким чином, інформаційна війна – це не просто сукупність фейкових повідомлень чи технічних атак. Це – системна стратегія довготривалого впливу, що може кардинально змінити політичну карту світу, зруйнувати державу без жодного пострілу, змусити народ добровільно здатися або змінити свій вибір, вважаючи це власним рішенням. Саме тому в умовах гібридної війни пріоритетами кожної демократичної держави мають бути інформаційна безпека, розвиток критичного мислення, медіаграмотності населення та стратегічна комунікація, яка здатна не лише оборонятись, а й давати відсіч агресору на кожному з трьох рівнів – емпіричному, концептуальному та смисловому.

РОЗДІЛ 3
ІНФОРМАЦІЙНІ СТРАТЕГІЇ В СУЧАСНИХ КОНФЛІКТАХ

3.1. Стратегії інформаційного впливу в міжнародних відносинах

Сьогодні, в часи активного розвитку цифрових технологій, інформація стала чи не найвпливовішою силою у міжнародних відносинах. Це вже не просто інструмент в дипломатичному арсеналі, а, скоріше, спосіб говорити, переконувати, захищатися і навіть атакувати. Держави дедалі частіше вдаються до інформаційного впливу, щоб не просто донести свою позицію, а змінити ставлення інших: схилити до співпраці, сформувати потрібну думку, посіяти сумнів або, навпаки, зміцнити довіру. Це своєрідна гра словами, емоціями, образами та символами.

Коли інформація миттєво перетинає океани, а соціальні мережі стирають кордони, стає зрозумілим: впливати на інше суспільство сьогодні можна без єдиного пострілу. Саме тому інформаційна взаємодія набуває особливої ваги – іноді як спосіб знайти спільну мову і розв'язати складне питання, а іноді – як форма боротьби, де кожне повідомлення, та кожен заголовок чи твіт можуть мати далекосяжні наслідки. Все це робить інформаційний простір не менш важливим за територіальний.

Одну з найважливіших стратегій в цьому контексті відіграє публічна дипломатія, яка ґрунтується на концепції так званої «м’якої сили». Це не про тиск чи загрози, а про тонкий і тривалий процес формування позитивного іміджу країни через відкриту комунікацію, культурні обміни, академічне партнерство, роботу зі ЗМІ та залучення громадянського суспільства. Такі дії спрямовані на те, щоб інші держави добровільно орієнтувалися на цінності та моделі поведінки, які пропонує ця країна, і навіть симпатизували їй. Мета – не нав’язати, а надихнути, не примусити, а зацікавити, створивши привабливий образ, який має вплив як на політичному рівні, так і на рівні суспільної свідомості в глобальному контексті [2, с.212].

Інформаційно-психологічні операції сьогодні – це не просто набір технічних дій, це, скоріше, цілеспрямовані спроби вплинути на людську

свідомість, викривити уявлення про реальність і сформувати викривлену картину світу. За допомогою розповсюдження дезінформації, фейкових новин, спотворених фактів і перекрученої логіки противник намагається змінити сприйняття конкретних подій або осіб, маніпулюючи емоціями, страхами та сумнівами. Така інформаційна агресія може проявлятись у вигляді навмисного «шуму» в інформаційному просторі, підміни понять або посіву недовіри – все це спрямовано на послаблення суспільної єдності, деструкцію віри в інститути влади та дискредитацію окремих людей або, навіть, держав [28, с.60].

Поки на перший погляд все залишається стабільним, в цифровому вимірі точиться невидима, але надзвичайно небезпечна війна. Кібератаки – це вже давно не сюжет для фантастичних фільмів, а щоденна реальність, у якій за лічені хвилини можуть бути паралізовані державні сервіси, медіаплатформи, енергетичні мережі чи інші життєво важливі системи. Ідеться не лише про спробу зламати програмне забезпечення чи викрасти дані – мова про реальний вплив на добробут, стабільність і безпеку цілих країн [28, с.60].

Коли інформація перестає бути доступною або спотворюється, а особисті й державні дані опиняються під загрозою, це б’є не тільки по технологіях – це влучає в серце довіри громадян до держави, у здатність функціонувати в кризовий момент. Саме тому країни по всьому світу дедалі активніше переглядають підходи до захисту: вкладають у новітні технології, впроваджують сучасні протоколи безпеки, готують фахівців, які здатні діяти на випередження. А ще – об’єднуються, бо протистояти цим загрозам поодинці вже неможливо. Кіберпростір не знає кордонів, і лише спільна відповідь на виклики може забезпечити захист у світі, де невидимі атаки мають цілком відчутні наслідки.

Варто зауважити, що в наш час, коли інформаційний простір стає ареною нових викликів і загроз, співпраця між країнами в питаннях інформаційної безпеки набуває особливого значення. Жодна держава вже не може самотужки впоратися з потужними хвилями дезінформації, кібератак або цілеспрямованих спроб вплинути на громадську думку. Тому держави все частіше об’єднують свої зусилля – діляться досвідом, спільно напрацьовують дієві підходи до захисту

цифрового простору, шукають нові способи виявлення й нейтралізації інформаційних загроз. Але мова йде не лише про технічні рішення чи цифрові бар'єри. Насамперед це про людей – про те, як захистити суспільства від маніпуляцій, як навчити критично мислити, розрізняти правду і навмисне спотворення фактів. В центрі цих міжнародних зусиль – турбота про безпеку, яка починається з довіри: до інформації, джерел, партнерів тощо. І саме ця довіра, разом із відкритим діалогом і солідарністю, є найміцнішим щитом проти сучасних інформаційних загроз.

Все це було б неможливо без зростання рівня інформаційної грамотності населення. Вміння критично мислити, аналізувати джерела, відокремлювати правду від вигадки – це вже не просто навички, а необхідність сучасного громадянина. Саме освітні ініціативи, доступ до якісної інформації та свідоме споживання контенту допомагають формувати стійкість до зовнішніх впливів і зберігати здорове інформаційне середовище в суспільстві [28, с.60].

Тобто, сучасна інформаційна безпека охоплює широкий спектр підходів – від тонких інструментів впливу на свідомість до технічно складних кібератак. Кожен із цих підходів має свою мету: хтось прагне створити привабливий образ, хтось – посіяти хаос і недовіру, інші ж зосереджені на зламі критичних систем або, навпаки, на їх захисті. Саме тому варто розглядати інформаційну боротьбу не лише як конфлікт між правдою і брехнею, а як складну систему цілей, інструментів і контрдиверсійних дій [48, с.76].

Для кращого розуміння цієї системи доцільно звернутися до узагальненої таблиці 3.1, яка відображає ключові напрямки інформаційного впливу та протидії, приклади застосовуваних інструментів і кінцеві цілі, яких прагнуть досягти різні сторони в умовах гібридного протистояння.

Ознайомлення з цією структурованою інформацією допомагає і систематизувати знання про методи інформаційного впливу, і усвідомити, наскільки важливим є активне формування власної інформаційної стійкості на індивідуальному й національному рівнях [42, с.87].

Таблиця 3.1

Основні напрями та інструменти інформаційного впливу і протидії

Напрям	**Приклади інструментів**	**Кінцева мета**
М’яка сила	Культурна дипломатія, академічні програми, пропаганда на ЗМІ	Формування позитивного іміджу, лобіювання
Інформаційні війни	Дезінформація, фейкові новини, соціальні мережі	Дестабілізація, зміна громадської думки
Кібервплив	Кібератаки, шантаж, втручання в інфраструктуру	Порушення роботи систем, шантаж
Контрдиверсія	Виявлення і спростування фейків, медіаграмотність	Захист власного інформаційного простору

Джерело: складено автором

Сьогодні ми живемо в епоху, коли інформація поширюється швидше, ніж будь-коли раніше. Новини, думки, зображення – все це може облетіти пів світу за лічені секунди, залишаючи помітний слід у свідомості мільйонів людей. Наше інформаційне середовище стало не просто динамічним – воно пульсує в режимі реального часу, змінюється щодня, щогодини, а іноді й щохвилини.

Цей новий етап інформаційного розвитку має одну суттєву особливість – у ньому взаємодіють найрізноманітніші гравці. Це не тільки державні установи з їхніми офіційними заявами, а й приватні компанії, громадські організації, активісти, блогери, користувачі соцмереж і навіть ті, хто ховається за анонімними акаунтами. Всі вони творять той самий простір, у якому ми щодня живемо, приймаємо рішення, формуємо ставлення до світу.

Традиційні медіа вже давно втратили монополію на вплив. Їхнє місце поділили нові джерела – соціальні платформи, алгоритми, які підбирають контент під наші вподобання, штучний інтелект, що генерує тексти та зображення, а також армії ботів, які можуть створити ілюзію суспільного настрою чи посилити потрібний інформаційний сигнал. Все це робить сучасний

інформаційний ландшафт неймовірно складним і водночас вразливим до маніпуляцій. І саме тому так важливо розуміти, хто, як і навіщо формує повідомлення, які ми щодня бачимо у своїх стрічках [2, с.212].

Для України виклики інформаційної війни давно вже не є чимось далеким чи теоретичним. Ми живемо з цим щодня, у прямому сенсі – на передовій боротьби за правду, гідність і власну незалежність у світі, де слово й зображення можуть завдати не меншої шкоди, ніж зброя. Інформація стала для нас не лише інструментом впливу – вона перетворилась на справжній щит і водночас меч, якими ми захищаємося від атак і водночас даємо відсіч.

В умовах повномасштабної війни українське суспільство навчилося бути уважним, стійким і згуртованим у медійному полі. Держава, волонтерські спільноти, журналісти, освітяни, айтішники – усі разом формують живу, адаптивну систему реагування на інформаційні загрози. Ми не просто викриваємо фейки – ми навчаємо одне одного, як розпізнавати брехню, як зберігати холодний розум перед навалою маніпуляцій і як відстоювати власну інформаційну безпеку. Цей досвід болючий, але унікальний. Він робить нас сильнішими, об’єднує і змушує шукати нові, дієві відповіді на виклики, які народжуються щодня у цифровому просторі [28, с.60].

Отже, інформаційний вплив в сфері міжнародних відносин є надзвичайно багатогранним і охоплює цілий комплекс дій – від ненасильницьких, м’яких методів, таких як культурна дипломатія, обмін цінностями, формування позитивного іміджу держави, до більш агресивних форм, таких як кібератаки, дезінформаційні кампанії та повномасштабні інформаційні війни.

В сучасному світі, де інформація має вагу реальної зброї, важливим завданням кожної держави стає побудова ефективної системи захисту від таких загроз. Ця система не може бути одновимірною: вона вимагає одночасного розвитку на кількох рівнях. Передусім ідеться про створення надійної інфраструктури кібербезпеки, але не менш важливою є і підтримка освітніх ініціатив, спрямованих на формування критичного мислення громадян – здатності розпізнавати маніпуляції, протистояти пропаганді та робити свідомий

вибір. Крім того, лише у співпраці з міжнародною спільнотою, через обмін досвідом, спільне напрацювання стандартів безпеки та єдину інформаційну політику, можливо ефективно протидіяти глобальним викликам у сфері інформаційної безпеки.

3.2. Роль соціальних медіа в інформаційній складовій гібридної війни

В реаліях сучасної війни, в тому числі і в контексті протистояння України перед країною-агресором Росією, соціальні медіа перетворилися на щось значно більше, ніж просто платформи для обміну новинами чи думками. Вони стали своєрідним фронтом, де щодня відбувається боротьба не просто за факти, а за людські серця та розум. Сьогодні тут не просто поширюють інформацію про повсякденне розмірене буття та вигадані факти на кшталт «чупакабри», сьогодні тут формують уявлення про реальність, створюють наративи, у яких одні постають героями, інші ж – ворогами.

Сьогодні кожне слово в дописі, кожен кадр у відео чи навіть звичайний коментар під публікацією можуть мати вагу, яку раніше приписували лише офіційним заявам чи гучним політичним виступам. Все, що ми читаємо чи бачимо в цифровому просторі, здатне впливати на наше сприйняття світу: надихати на дії (часом, навіть ворожі), вселяти впевненість, посіяти сумнів або ж змусити людину по-новому подивитися на те, що здавалося беззаперечно істинним.

В віртуальному середовищі, яке давно стало частиною нашої реальності, точиться постійна боротьба – не за території, а за думки, переконання та емоції. І від того, хто зуміє достукатися до серця і свідомості, часто залежить не менше, ніж від того, хто переможе у збройному протистоянні. Адже саме тут вирішується, кому люди вірять, кого підтримують, за ким ідуть – і це формує нову, дуже реальну мапу впливу у світі.

Рисунок 3.1. Аспекти впливу інформаційних медіа

Соціальні мережі перетворилися на зручний інструмент для тих, хто прагне маніпулювати масами. Тут народжуються і миттєво розлітаються фейкові новини, влучні, але оманливі заголовки, спеціально сконструйовані емоційні повідомлення. Вони спрямовані на те, щоб викликати злість, страх або зневіру. За лічені хвилини сумнівна інформація може охопити тисячі або мільйони людей, вплинути на суспільні настрої, посіяти недовіру до уряду, армії чи міжнародних партнерів. Часто це робиться цілеспрямовано – для дестабілізації, роз'єднання суспільства, ослаблення тилу [5, с.124].

Одне з найнебезпечніших явищ сучасного інформаційного світу – це не лише зміст певного повідомлення, а те, з якою неймовірною швидкістю й масштабом воно може поширитися. Соціальні мережі стерли просторові межі, й те, що було створене, наприклад, у російському пропагандистському цеху, вже за кілька хвилин може з’явитися на екранах користувачів у будь-якому куточку світу – від Європи до Латинської Америки. І це не просто фоновий інформаційний шум: такі меседжі здатні змінювати думки, настрої, формувати викривлену картину реальності – як у власному суспільстві, так і за його межами.

В цьому новому цифровому середовищі соціальні медіа вже давно перестали бути майданчиком лише для спілкування чи розваг. Вони

перетворилися на справжній фронт – не символічний, а цілком реальний, зі своїми атаками, обороною і жертвами. І те, наскільки кожен з нас уміє розпізнати маніпуляцію, критично оцінити побачене, зупинитися і подумати, – часто має набагато більше значення, ніж здається. Адже в гібридній війні зброєю може стати навіть допис чи коментар. І виграє в ній той, хто не втрачає здатності думати самостійно та мислити критично [17, с.52].

В сучасних умовах гібридної війни соціальні мережі вже давно перестали бути просто місцем для спілкування чи обміну новинами – вони стали справжнім полем бою. Але тут не лунають вибухи, не видно танків чи безпілотників. Тут воюють інакше: через слова, емоції, зображення, які здатні проникати глибоко в свідомість і поступово змінювати сприйняття світу.

Ті, хто намагається розхитати суспільство зсередини, діють хитро й вивірено. Вони не кричать – вони нашіптують. Вкидають неправдиву інформацію так, щоб вона здавалася правдоподібною, розпалюють недовіру до влади, до армії, до сусідів, до власної країни. І роблять це не поодинці: за ними стоять цілі мережі – тисячі фейкових профілів, підставних осіб, автоматизованих ботів, які вдень і вночі працюють над тим, щоб зруйнувати відчуття стабільності, посіяти тривогу, викликати злість або байдужість.

Їхня ціль – не просто дезорієнтувати. Вони хочуть, щоб люди почали сумніватися в очевидному, відверталися від правди, перестали вірити одне одному. Щоб реальність стала розмитою, а будь-яка інформація – підозрілою. Це тиха, але дуже небезпечна війна за свідомість, і вона точиться просто зараз, в стрічках новин, в коментарях під дописами, в заголовках, які ми щодня бачимо [80, с.164].

В світі, де неправда здатна поширюватися зі швидкістю блискавки, де кожен пост чи заголовок може викривити реальність, народжується інша, дуже жива і справжня сила – людська солідарність. Попри всі ризики й виклики, цифровий простір сьогодні – це не просто поле для інформаційних атак, це місце, де з'являється надія, де з маленьких людських вчинків виростає щось значно більше. Соціальні мережі стали не просто засобом спілкування, а інструментом

дії: вони здатні миттєво згуртувати незнайомих людей довкола спільної мети, показати правду там, де її намагаються приховати, донести голос тих, хто його давно втратив, чи простягнути руку допомоги туди, де її найбільше чекають.

В Україні ця здатність об'єднувати вже давно перетворилася на щось більше, ніж просто активність в інтернеті – вона стала важливою частиною нашої сили, частиною національного імунітету. Щодня тисячі людей – журналісти, волонтери, аналітики, лікарі, вчителі, студенти, пенсіонери – кожен по-своєму і кожен по-людськи роблять те, що підсилює нас усіх. Хтось розвінчує фейки, хтось ділиться корисною інформацією, хтось підтримує словом, а хтось – дією, хтось збирає донати на потреби армії. І в цій буденній, але дуже щирій взаємопідтримці народжується те, що не дає інформаційній темряві охопити нас повністю. Це тиха, майже непомітна робота серця й розуму, яка насправді є основою нашої спільної стійкості [5; 18].

Сьогодні соціальні мережі вже давно вийшли за межі простої розваги чи способу підтримувати зв'язок із близькими. Вони стали простором, у якому розгортаються події не менш значущі, ніж на реальних фронтах. Все, що з'являється в стрічці – від емоційного відео до короткого, але влучного допису – може стати тригером для хвилі емоцій, роздумів або дій. Іноді один пост здатен розбудити сумління, викликати обурення або, навпаки, подарувати надію тисячам, а то й мільйонам людей по всьому світу. Все це відбувається блискавично, у режимі реального часу, коли кожне слово й кожен кадр мають значення.

І в цьому стрімкому потоці інформації все частіше визначається не лише громадська думка, а й політичні рішення, настрій суспільства, хід перемовин і навіть напрямки дій міжнародних інституцій. Тому нині межа між війною в класичному розумінні та боротьбою за уми і серця людей практично зникає.

Інформаційні кампанії стали настільки впливовими, що іноді добре продумане повідомлення, сказане вчасно й в потрібному тоні, може завдати більшого удару, ніж найпотужніша зброя. І ця реальність вимагає від нас усвідомлення, що ми всі, хай навіть несвідомо, беремо участь у цьому новому

вимірі сучасних конфліктів – там, де слово стало зброєю, а правда й маніпуляція ведуть щоденну боротьбу за перевагу [17,с.52].

Це змушує замислитися над дуже тонкою, але надзвичайно важливою гранню: соціальні медіа сьогодні можуть стати як джерелом надії, так і інструментом руйнування. У руках людей, які вміють мислити стратегічно, вони перетворюються на потужну зброю – здатну або підірвати довіру, посіяти страх, внести розбрат у суспільство, або ж навпаки – об'єднати, підтримати, пробудити відчуття причетності до чогось більшого. Ці платформи мають здатність поширювати правду, викривати несправедливість, давати голос тим, кого не чують. Але з тією ж швидкістю і впевненістю вони можуть транслювати відверту неправду, фальсифіковані факти, створювати уявну реальність, у якій складно відрізнити справжнє від вигаданого.

Все це говорить про одне: ми живемо в час, коли контроль над інформацією перестав бути суто технічним питанням – це вже питання безпеки, довіри, гуманності. Це не просто змагання за кількість переглядів чи лайків. Це боротьба за світогляд, за те, як мільйони людей бачитимуть події, інших людей і самих себе. В цій боротьбі вирішується набагато більше, ніж виграш у політичному чи ідеологічному протистоянні. Йдеться про те, яким буде наше «завтра» – чи буде воно побудоване на розумінні та співпереживанні, чи на страхові, агресії та маніпуляції. І саме ми, користувачі цих медіа, щодня робимо свій вибір у цьому інформаційному лабіринті.

3.3. Інформаційні атаки та їх вплив на державні інституції та громадянське суспільство

Інформаційні атаки сьогодні перетворилися на одну з найнебезпечніших загроз для держав і суспільства. Особливої актуальності та загрози вони набувають в умовах гібридної війни, коли межа між відкритим протистоянням і прихованим впливом майже стерлася. Ці атаки не завжди супроводжуються вибухами чи вистрілами, але їхні наслідки можуть бути не менш руйнівними – особливо коли мішенню стають не лише інституції, а й свідомість людей.

Коли інформаційний простір заповнюється неправдою, викривленими фактами, маніпулятивними повідомленнями та навмисною дезінформацією, першою жертвою стає довіра – той крихкий, але життєво необхідний фундамент, на якому тримається зв'язок між державою та її громадянами. Люди починають сумніватися не лише у конкретних рішеннях чи заявах, а й у самій спроможності влади діяти чесно і ефективно. З кожною новою фейковою новиною чи навмисно спотвореним повідомленням у свідомості громадян проростає зневіра: в слова, в обіцянки, в наміри [64, с.151].

Цей процес особливо небезпечний тим, що відбувається поступово, майже непомітно. Розгубленість, роздратування, втома від суперечливої інформації перетворюються на підозру до всього, що йде «згори» – будь то нові закони, ініціативи, чи навіть щоденні рішення, необхідні для керування країною. Коли викривлена інформація перетворюється на норму, навіть щирі дії держави починають сприйматися як частина змови або маніпуляції. І в моменти, коли суспільство особливо вразливе – під час війни, економічної кризи чи соціального конфлікту – ця недовіра може буквально паралізувати державне управління, зробити його нездатним діяти рішуче, бо кожен крок наштовхується на спротив, підозру або ігнорування.

Уряди, які опиняються в такій ситуації, фактично ведуть боротьбу не лише з викликами реального світу, а й з невидимим ворогом – руйнівною силою інформаційного впливу. І ця боротьба – не лише про політику чи комунікацію. Це боротьба за відновлення взаєморозуміння, за право бути почутими, за збереження довіри, без якої неможлива ані демократія, ані стабільне, здорове суспільство [64, с.152].

Сьогодні інформаційна агресія дедалі частіше виходить за межі маніпуляцій у ЗМІ чи соціальних мережах і набуває конкретної, технічної форми. Йдеться про кібератаки – цілеспрямовані удари по цифровій інфраструктурі держави, які можуть паралізувати її роботу буквально в одну мить. Це не сюжет фантастичного фільму й не далека перспектива – це вже наша реальність.

Достатньо одного добре спланованого вторгнення в державні системи, аби перестали працювати реєстри, заблокувалися бази даних, порушився доступ до зв'язку чи електронних сервісів, на які щодня покладаються мільйони людей [30, с.30].

Подібні атаки вражають не лише абстрактні урядові структури – їх наслідки безпосередньо відчувають звичайні громадяни. Наприклад, хтось не може вчасно записатися до лікаря, отримати соціальні виплати чи зареєструвати дитину до школи, або ж навіть отримати довгоочікувану посилку з «Нової пошти». Порушення банківських операцій або енергетичних систем може позбавити людей елементарного – світла, тепла, доступу до грошей. І в такі моменти стає особливо зрозуміло: наш цифровий світ надзвичайно вразливий, а технічна безпека – це не лише про «фахівців у серверній», а й про спокій кожної окремої людини.

Технічна складова інформаційної агресії – це ще одна форма тиску, яка має на меті посіяти хаос, недовіру, відчуття безпорадності. І в умовах сучасної гібридної війни ми не можемо дозволити собі бути легковажними. Захист кіберпростору має стати такою ж звичною справою, як охорона кордонів, бо в ньому точиться справжня, хоч і невидима, битва за стабільність, безпеку і наше з вами майбутнє [30, с.30].

Найпідступнішою формою інформаційного впливу залишаються саме інформаційно-психологічні операції. Їхня мета – не просто ввести людей в оману, а значно глибша й болючіша: викликати внутрішній хаос, підірвати емоційну рівновагу, посіяти паніку та паралізуючий страх. Це атаки, спрямовані не на об’єкти інфраструктури, а безпосередньо на свідомість людини – її здатність розрізняти правду, довіряти, діяти зважено. Такі впливи ретельно вибудовуються, використовують слабкі місця – напругу, втому, інформаційну перевантаженість, емоційне виснаження.

Найвразливішими суспільства стають саме в моменти кризи або небезпеки – коли люди шукають опору, відповіді, чітких орієнтирів. У такі періоди кожне слово, кожен заголовок може або заспокоїти, або вкинути в паніку. Тоді

інформаційно-психологічні атаки особливо небезпечні: вони цілеспрямовано розмивають відчуття реальності, сіють недовіру до державних інституцій, до армії, до одне одного. Вони змушують людей відчувати себе розгубленими, безсилими, ніби світ навколо розвалюється і немає на що спертися.

Насправді ж у цей момент справжнє поле бою – не екрани чи мережі, а наш внутрішній стан, наша здатність зберігати холодний розум, бути уважними, співчутливими й об'єднаними. Саме в нашій свідомості вирішується, чи зможемо ми протистояти цій новій формі агресії, яка не використовує зброю в класичному розумінні, але завдає не менш серйозної шкоди. І тому перемога починається там, де зберігається гідність, людяність, взаємна підтримка – навіть у найскладніші часи [9].

Сьогодні ми живемо в епоху, коли інформаційний простір проникає в кожен куточок нашого життя – у розмови з друзями, стрічки в соцмережах, родинні обговорення за вечерею. І саме в цьому просторі, непомітно для більшості, на громадянське суспільство здійснюється постійний, іноді майже невловимий, але дуже потужний тиск. Він не має вигляду явного примусу чи заборон – натомість, діє через емоції, через сумніви, через багатоголосся, що часто перетворюється на какофонію.

Соціальні мережі, які донедавна здавалися зручним місцем для вільного обміну думками, підтримки зв'язку й спільного пошуку істини, все частіше стають майданчиком, де розгортаються цілеспрямовані маніпуляції. Це не просто поодинокі фейки або випадкові помилки – це складна, добре продумана інформаційна кампанія, що має на меті розхитати емоційний і моральний стан суспільства. Людям нав'язують суперечливі версії подій, загострюють болючі теми, змушують сумніватися в очевидному, шукати ворогів там, де їх немає, і втрачати довіру навіть до тих, хто вчора ще здавався близьким.

В такому середовищі особливо небезпечною стає поступова втрата внутрішньої злагоди. Замість того щоб разом шукати відповіді, люди починають сперечатися, не чуючи одне одного. Колись єдине поле суспільного діалогу розбивається на фрагменти, між якими вже не пролітає міст довіри. Виникають

невидимі стіни – між поколіннями, між громадами, навіть всередині сімей. І що більше таких інформаційних бар'єрів, то складніше підтримувати відчуття спільності, необхідне для руху вперед.

Це не абстрактна загроза. Це щоденна реальність, у якій ми всі живемо, і яка вимагає пильності, емпатії й великої внутрішньої сили, щоб не дозволити себе роз'єднати [26].

Ще однією тривожною ознакою такого впливу є поступова втрата довіри – до ЗМІ, до державних інституцій, до офіційних заяв. Коли інформаційний простір заповнюють протилежні, суперечливі версії подій, навіть найбільш добросовісні громадяни починають сумніватися у правдивості всього, що чують і бачать. В критичні моменти, коли потрібно діяти спільно – під час надзвичайних ситуацій, війни чи епідемій – така втрата довіри може мати серйозні наслідки: люди починають ігнорувати офіційні рекомендації, піддаються паніці або, навпаки, впадають у байдужість [9, с.225].

Не можна також оминути увагою психологічний бік цієї проблеми. Постійний потік тривожних новин, повідомлень про загрози, зраду, небезпеку створює відчуття тривоги, невпевненості й навіть безнадії. Багато хто просто не витримує цього тиску – емоційного та інформаційного – і поступово втрачає здатність критично мислити, зосереджуватися, сприймати реальність збалансовано. Це позначається як на особистому благополуччі, так і на загальному стані суспільства.

Зрештою, коли суспільство розділене, кожна його частина починає жити у своєму інформаційному світі, де свої «правди», «герої» й «вороги». Діалог між цими частинами стає майже неможливим, адже втрачається спільна основа для розуміння. Такий стан речей не просто шкодить – він блокує будь-які спроби єднатися, взаємодіяти, будувати щось спільне. І саме в цьому – головна небезпека інформаційних атак: вони непомітно розмивають фундамент довіри, на якому тримається громадянське суспільство [9, с.225].

Інформаційні атаки – це не просто фоновий шум сучасного світу. Вони працюють тихо, але влучно, й нерідко миттєво змінюють атмосферу в

суспільстві. Те, що сьогодні здається лише окремою публікацією чи новиною, вже завтра може спровокувати недовіру до влади, підірвати віру в національні інституції, розхитати емоційний стан людей і навіть викликати хвилю протестів або суспільну напругу. Найнебезпечніше – це не швидкий вплив, а ті глибокі, приховані зміни, які залишаються надовго. В свідомості громадян проростає сумнів, з'являється відчуття тривоги, розгубленості, а іноді – відчуження від держави та одне від одного [30, с.30].

Все це лише підкреслює, наскільки важливо сьогодні мати ефективну, продуману політику в сфері інформаційної безпеки. Це вже не технічне питання – це про довіру, про відповідальність, про здатність держави не тільки відбивати зовнішні інформаційні удари, а й створювати умови, в яких суспільство стійке до маніпуляцій. Йдеться про формування інформаційної культури: коли люди вміють розрізняти правду і фейк, не піддаються паніці, критично осмислюють те, що бачать і чують, і зберігають внутрішній орієнтир [64, с.152].

Насправді, мета інформаційного тиску – не просто посіяти хаос. Це спроба розламати те, що тримає країну разом: довіру, солідарність, усвідомлення спільної мети. І саме тому протидія має бути всеохопною – від кіберзахисту до шкільної освіти, від незалежних медіа до щирого діалогу між владою й суспільством. Найефективніша оборона – це коли люди залишаються єдиними, мислять тверезо й розуміють, за що вони стоять.

3.4. Аналіз інформаційних операцій в українському контексті (на прикладі конфлікту на Сході України)

Інформаційні операції, що стали невіддільною частиною гібридної війни, яку Росія веде проти України, – це одна з найнебезпечніших і найпідступніших форм впливу. Їхня мета – не лише спотворити факти чи використати медіа у своїх інтересах. Йдеться про щось набагато глибше: це системна, холоднокровна боротьба за людську свідомість. За те, як ми відчуваємо, як мислимо, кому віримо і як розуміємо світ навколо. Це війна, яка ведеться не на полі бою, а в

душах і серцях людей – і саме тому вона така небезпечна. В ній намагаються підірвати саме поняття правди, посіяти сумніви, зламати довіру одне до одного, до держави, до реальності. І хоча ці атаки невидимі, їхні наслідки відчутні глибоко всередині кожного, хто зіштовхується з потоком брехні, напівправд і навмисно викривлених сенсів.

Одним з найпомітніших проявів цієї війни є потужна дезінформаційна атака. Російські медіа, контрольовані державою, систематично створюють паралельну реальність: транслюють фейкові новини, спотворюють хід подій, використовують постановочні відео та голослівні заяви, які мають створити враження розгубленості й зради в українській армії та керівництві. Вигадки про нібито втечу українських лідерів, капітуляцію, паніку в ЗСУ – все це подається як незаперечна істина, тоді як насправді це – елементи продуманої інформаційної атаки. Мета зрозуміла: посіяти страх, зневіру, викликати сумніви навіть у найстійкіших.

На сході України, зокрема в перші роки конфлікту, активно використовувалися методи психологічного тиску. Через підроблені «свідчення», псевдорозслідування, сфабриковані документи, які потім поширювались у медіа, намагалися деморалізувати не лише військових, а й цивільне населення. Ці інформаційні вкиди часто мали одну мету – підірвати довіру до української влади, викликати обурення, посіяти ворожнечу, зупинити бажання захищати свою державу.

Одним із перших і найбільш резонансних прикладів в 2014 році стало поширення через російські телеканали, такі як RT та «Россия 24», історії про «розіп'ятого хлопчика» в Слов'янську. Цей емоційно навантажений і абсолютно вигаданий сюжет, який нібито ілюстрував «жорстокість українських військових», був спрямований на виклик у глядачів почуття обурення та ненависті до української армії. Попри повну відсутність доказів і спростування цього випадку численними журналістами й правозахисниками, сюжет довго циркулював у медіапросторі, виконуючи свою функцію – створювати образ ворога та виправдовувати дії Росії на Донбасі.

Іншим вектором інформаційної атаки стало послідовне знецінення діяльності Збройних Сил України. Через проросійські Telegram-канали, фейкові акаунти в соцмережах і навіть постановочні відео за участі т.зв. «ополченців», українських військових намагалися змалювати як агресорів або аморальних мародерів. Подібні повідомлення часто супроводжувалися візуальними матеріалами – іноді зняті на інших війнах або навіть в інших країнах, вони подавалися як «докази» злочинів ЗСУ. Така практика сприяла поширенню страху, підозри та розчарування серед частини населення, особливо в прифронтових зонах.

Значну частину інформаційної війни складали цілеспрямовані психологічні атаки на цивільне населення. У 2014–2015 роках, під час активної фази бойових дій на Донбасі, через підконтрольні Росії інформаційні ресурси активно поширювалися апокаліптичні прогнози про «розпад України», «економічний крах» і «повне занепадання соціальних систем». Ці меседжі були спрямовані на формування серед громадян відчуття безпорадності й недовіри до влади, стимулюючи внутрішню еміграцію, політичну апатію та відчуження [83].

Соціальні мережі та цифрові канали стали ще одним фронтом. Тут працюють цілі фабрики тролів і ботів, які день у день нав'язують потрібні меседжі, намагаючись впливати не лише на українців, а й на іноземну аудиторію. Але в цьому ж цифровому просторі розгорнулася й боротьба за правду: українські журналісти, волонтери, військові та просто небайдужі громадяни докладають величезних зусиль, щоб не дати фейкам прижитися. Створюються ініціативи, які розвінчують неправдиву інформацію, розповідають світу про реальні події, показують голоси людей, які не можуть мовчати [30, с.30].

В 2022–2023 роках, з початком повномасштабного вторгнення, ці наративи трансформувалися в нову форму – через соцмережі поширювалися фейки про «неминучу здачу Києва», «відсутність підтримки з боку Заходу» або «знищення всієї інфраструктури». Боти закликали населення залишити міста, розповсюджували псевдоінструкції з евакуації чи навіть погрози від імені окупаційних структур.

Окремий напрям – це кіберфронт. Тут ворог діє цинічно і жорстко: атаки на державні сайти, злам інформаційних порталів, спроби блокування доступу до українських джерел в Криму – все це робиться, щоб посіяти паніку, порушити комунікацію, унеможливити доступ до правдивої інформації. Замість реальних новин людям нав'язують сконструйовану картину, яка має утримати їх в інформаційній ізоляції.

Одним із гучних прикладів стала атака на українські телекомпанії у 2022 році, коли в прямому ефірі на декількох телеканалах з’явилися проросійські посили, які не мали жодного відношення до редакційних політик мовників. Такі дії були спрямовані не стільки на інформування, скільки на дезорієнтацію – глядач, стикаючись із протилежними повідомленнями, губився в реальності. Додатково проводилися атаки на акаунти в Telegram українських військових, журналістів та посадовців, що дозволяло агресору викрадати інформацію, стежити за переміщеннями та навіть поширювати дезінформацію від імені жертв зламу.

Російська дезінформація не обмежувалася відкритою пропагандою. Її найнебезпечнішим проявом стало створення псевдоукраїнських медіа-ресурсів і Telegram-каналів, які стилізувалися під об’єктивні або навіть патріотичні джерела, але фактично працювали на поширення кремлівських наративів. Такі ресурси як «Голос Правди», «Украина.ру» або популярні Telegram-канали на кшталт «Резидент», «Легітимний» системно публікували викривлену або відверто неправдиву інформацію про внутрішньополітичні процеси в Україні, військові події чи міжнародну підтримку. Їхні повідомлення часто були подані у формі «інсайдів», що створювало ілюзію достовірності й викликало довіру в аудиторії, не підготовленої до критичного аналізу джерел [21].

Окрім звичних форм дезінформації, Росія активно використовувала тактику «інформаційного замінування». Це особливий тип операцій, коли в інформаційне поле свідомо вкидається панічна новина, наприклад про «евакуацію всього Києва», «тривале знеструмлення всієї країни» або «масову мобілізацію дітей». Такі фейки, поширювані в пікові моменти – наприклад, під

час масованих обстрілів енергосистеми, – викликали миттєвий ажіотаж, скуповування товарів, блокування доріг, паніку в лікарнях і школах. В такий спосіб створювався ефект внутрішнього хаосу без єдиного пострілу, але з масштабними наслідками для стабільності.

На тимчасово окупованих територіях інформаційна ситуація ще складніша. Там системно знищувалися українські джерела інформації, блокувалися телерадіоканали, а натомість насаджувалася однобока, проросійська пропаганда. Людей позбавляли вибору – їм лишали лише одну, зрежисовану версію подій. Так формувалося викривлене бачення світу, де Росія – «визволитель», а Україна – «загроза» [43, с.309].

Тактика, з якою працює Росія в інформаційному просторі, націлена на досягнення результатів не тільки в моменті. Так, на рівні тактичному їй вдалося створити певний інформаційний тиск, розпалити ворожнечу, мобілізувати частину населення під свої гасла. Але на стратегічному рівні – тобто в очах світу – ця брехня все частіше дає тріщини. І хоча інформаційна боротьба триває, саме правда, як показує досвід останніх років, має найміцнішу витривалість [43, с.309].

Наведені приклади засвідчують, що інформаційна війна в українському контексті не є абстрактною чи другорядною – вона має глибоко людське обличчя. Вона про страх і віру, про вибір між правдою і зручним обманом, про боротьбу за свідомість кожного, хто вмикає новини, гортає стрічку в смартфоні або читає коментар під дописом. Росія побудувала багаторівневу систему інформаційного тиску, де кожна людина – не просто глядач, а потенційний учасник і ціль.

Зважаючи на події на Сході України, інформаційні операції давно перестали бути лише сухими повідомленнями чи пропагандою в звичному розумінні. Це складне й багатошарове явище, яке охоплює цілу систему дій, ретельно спланованих для того, щоб впливати на людей – на їхні думки, емоції, сприйняття реальності. Такий вплив нерідко поглиблює сам конфлікт, розпалюючи недовіру, страх і ненависть. Для досягнення своїх цілей

використовуються як традиційні засоби – наприклад, ЗМІ чи листівки, – так і сучасні цифрові інструменти: соціальні мережі, боти, фейкові сайти. Це не просто «інформаційна війна» в загальному розумінні, а цілеспрямований психологічний тиск, який відчувають на собі як військові, так і звичайні люди, часто навіть не усвідомлюючи, що стали об’єктами зовнішнього впливу.

РОЗДІЛ 4. ПРОТИДІЯ ІНФОРМАЦІЙНИМ ЗАГРОЗАМ

4.1. Методи протидії інформаційним операціям

Протидія інформаційним операціям в нашій країні здійснюється через багатогранний і скоординований підхід, який охоплює як технічні, правові, так і гуманітарні та стратегічні заходи. В центрі цієї боротьби – захист національного інформаційного простору та забезпечення інформаційної безпеки громадян.

Моніторинг інформаційного простору – це щоденна невидима, але надзвичайно важлива робота, яка нагадує складну багаторівневу операцію. Вона передбачає не просто фонове спостереження за новинами, а цілеспрямоване, аналітичне відстеження всього, що відбувається в медіа, соціальних мережах, блогах, форумах, коментарях під дописами та на інших інформаційних платформах. Цей процес дозволяє виявляти потенційно небезпечні інформаційні вкиди ще до того, як вони почнуть впливати на суспільну думку чи дестабілізовувати ситуацію в країні [40, 111].

В центрі цього процесу – спеціалісти з інформаційної безпеки, аналітики, ІТ-фахівці, які працюють як у державних структурах, так і в незалежних експертних групах. Вони користуються складними програмними системами, зокрема й тими, що працюють на базі ШІ. Такі системи здатні за лічені секунди «просіювати» тисячі повідомлень, виявляючи ключові слова, тональність, підозрілі джерела, повторювані наративи або синхронізовані інформаційні кампанії. Це дозволяє не просто зафіксувати факт появи фейку, а зрозуміти, хто стоїть за його запуском, з якою метою, та які групи він намагається вразити.

Окрема увага приділяється виявленню ботів та фейкових акаунтів у соціальних мережах – тих «мовчазних солдатів» інформаційної війни, які розганяють неправдиві повідомлення, створюють ілюзію «народного обурення», або навпаки – імітують підтримку ворожих ідей. За допомогою спеціалізованих інструментів, таких як Botometer або Graphika, ці акаунти аналізуються й маркуються. Виявлення подібної активності дозволяє не тільки блокувати джерела дезінформації, а й відстежувати цілу мережу, що стоїть за ними [82, с.127].

Та в цій роботі важливий не лише алгоритм, а й людина – із її інтуїцією, досвідом і розумінням контексту. Саме тому аналітики часто працюють у тандемі з експертами з медіа, соціологами, психологами, які допомагають розпізнати неочевидні маніпуляції або нові інформаційні інфекції – ті, які несе в собі зміст, що на перший погляд виглядає невинно, але прицільно вражає психіку й підсвідомість аудиторії.

Ще одним важливим напрямом у боротьбі з інформаційними атаками є цілеспрямоване виявлення й нейтралізація джерел, з яких системно поширюється дезінформація, мова ворожнечі або відверта ворожа пропаганда. Це не просто технічне блокування сайтів чи окремих акаунтів – це робота, яка часто відбувається на стику технологій, права та національної безпеки [40, с.111].

В сучасних умовах інформаційної війни подібні ресурси функціонують під виглядом звичайних новинних каналів, популярних Telegram-сторінок чи навіть блогів, які видають себе за «незалежні голоси правди». В реальності ж за ними нерідко стоять організовані групи, що мають на меті підірвати довіру до держави, розхитати суспільну єдність або створити хаос шляхом поширення фейків, маніпуляцій і страху.

Реакція держави на такі загрози чітка й скоординована. Завдяки запровадженню санкцій та рішень РНБО припинено діяльність цілої низки проросійських медіа, які роками формували викривлену реальність для мільйонів глядачів. В співпраці з інтернет-провайдерами блокується доступ до небезпечних Telegram-каналів, що транслюють фейки, конспірологічні теорії та антивоєнну риторику, створену в інтересах агресора. Це – приклад того, як сучасна держава може діяти рішуче, але водночас в рамках закону, щоб захистити свій інформаційний суверенітет [85, с.49].

Великий обсяг роботи виконується і в сфері кібербезпеки. Спеціалісти кіберполіції разом з правоохоронцями займаються виявленням та знешкодженням ботоферм і цілих ботнетів – автоматизованих мереж фейкових акаунтів, які здатні створювати ілюзію масової підтримки або незадоволення, впливати на суспільні настрої та навіть втручатися в політичні процеси.

За всіма цими діями стоїть розуміння простої, але важливої істини: інформаційна безпека – це не про цензуру чи обмеження свободи слова. Це – про відповідальність. Про захист людей від навмисного обману. Про те, щоб кожен громадянин міг отримувати правдиву, перевірену інформацію та не став заручником маніпуляцій. І поки точиться війна, ця інформаційна гігієна є такою ж необхідною, як і захист фізичних кордонів країни.

Правова відповідь держави в сфері інформаційної безпеки – це тверда, але виважена реакція на спроби дестабілізувати суспільство через брехню, маніпуляції та пропаганду. В цьому контексті право вже давно перестало бути лише інструментом реагування – воно стало активною частиною оборони, щитом, який допомагає зупиняти інформаційні атаки на ранніх етапах [40, с.111].

Коли мова йде про поширення фейків, заклики до розпалювання ворожнечі чи підрив довіри до держави – це не просто неприпустимі прояви безвідповідальності. Це дії, які мають чітке юридичне визначення і тягнуть за собою конкретну відповідальність. Кримінальний кодекс України передбачає покарання за такі злочини. Наприклад, статті, що стосуються порушення рівноправності громадян або свідомого поширення неправдивої інформації, дають можливість відкривати кримінальні справи, виносити судові рішення й обмежувати діяльність осіб або груп, які свідомо шкодять державі через слово.

Такими заходами охоплені як громадяни України, так і іноземці, які займаються інформаційною диверсією на нашій території. До них застосовуються санкції, їм забороняється в'їзд, а в окремих випадках навіть ініціюються міжнародні розслідування. Цей інструментарій дозволяє не лише захищати інформаційний простір, а й формувати чітке розуміння: кожне слово, кожна дія в інформаційній війні має свою вагу – і за неї доведеться відповідати.

Особливо небезпечними є так звані інформаційні агенти – ті, хто під прикриттям журналістики чи «альтернативної думки» свідомо працює в інтересах агресора. Держава має право та обов'язок обмежувати їхню діяльність, зокрема шляхом закриття доступу до ресурсів, які порушують національну безпеку або сіють розбрат у суспільстві.

Окремим, надзвичайно важливим напрямом у боротьбі з дезінформацією є системна та щира взаємодія з громадськістю. Адже саме люди – кожен окремо і всі разом – є мішенню інформаційних атак, але водночас і головним бар'єром, здатним їм протистояти. Тому надзвичайно важливо не лише боротися з фейками після того, як вони вже з'явилися, а й формувати у суспільстві навички, які дозволяють розпізнавати неправду з перших секунд, не піддаватися на провокації та обирати перевірені джерела [45, с.83].

Цю роботу ведуть не лише державні установи. У ній активно задіяні незалежні медіа, громадські організації, журналісти, фактчекери, волонтери, освітяни та навіть блогери. Наприклад, такі платформи, як Український кризовий медіа-центр, оперативно реагують на інформаційні загрози, спростовують фейки та дають людям чіткі орієнтири у складному потоці новин. Вони публікують аналітичні матеріали, проводять розслідування, створюють інфографіку, що допомагає розібратися, де реальна подія, а де навмисно зрежисований обман.

Паралельно з цим в Україні все більше уваги приділяється просвітницькій роботі – проводяться лекції, тренінги, шкільні уроки, онлайн-курси з медіаграмотності. Це знання, які ще десять років тому здавалися факультативними, сьогодні стали життєво необхідними. Бо людина, яка вміє розпізнати маніпуляцію, – це вже не просто глядач чи читач. Це активний учасник інформаційного спротиву.

Все це – не тимчасові заходи, а частина нової культури інформаційної стійкості. Культури, в якій громадянин не лише споживає інформацію, а й критично її аналізує, перевіряє, ділиться лише тим, що має вагу й підтвердження. І саме така культура – один із найсильніших щитів у гібридній війні.

Формування дієвої системи інформаційної безпеки – це не разова кампанія, а довготривалий процес, що вимагає глибоких змін на всіх рівнях: від освітніх програм у школах до стратегічних рішень на рівні держави. В його основі лежить розуміння того, що найнадійніший захист – це не лише технічні бар'єри, а насамперед свідоме, критично мисляче суспільство, здатне самостійно розпізнавати загрози [46].

Одним із ключових кроків на цьому шляху стало впровадження медіаграмотності в навчальні програми. Сьогодні вже у школах діти вчаться не просто читати новини, а ставити до них запитання, перевіряти джерела, розуміти, хто і з якою метою створив той чи інший контент. У вищих навчальних закладах дедалі частіше з'являються окремі курси з інформаційної безпеки та цифрової гігієни, що готують молодь до життя в епоху, де інформація стала головною зброєю.

Зміцнення інформаційної інфраструктури – це основа цифрової безпеки держави, особливо в умовах війни, коли атаки відбуваються не лише на полі бою, а й у кіберпросторі. Інформаційні системи, які забезпечують життєдіяльність країни, – державні реєстри, ресурси урядових структур, канали комунікації – мають бути захищені так само ретельно, як стратегічні об'єкти на мапі [22, с.20].

В сучасних реаліях кіберзахист – це не просто встановлений антивірус. Це ціла система: складна, багаторівнева, постійно оновлювана. Вона включає сучасні програмні рішення – міжмережеві екрани, системи виявлення вторгнень (IDS/IPS), багатофакторну автентифікацію, аналітичні платформи для відстеження підозрілої активності. Усі ці інструменти працюють разом, як злагоджений організм, щоб вчасно виявити й нейтралізувати кіберзагрозу, навіть коли вона ще не встигла завдати шкоди.

Проте навіть найкраща система не буде ефективною без людей, які нею управляють. Тому в Україні системно організовуються навчання й спеціалізовані тренінги з кіберзахисту для ІТ-фахівців, працівників державних установ, аналітиків. Це дозволяє підтримувати високий рівень обізнаності та оперативного реагування, адже кожен кібератакувальний інцидент – це виклик, який потребує швидкого і фахового рішення.

Окрема роль у забезпеченні кіберстійкості відведена міжнародній співпраці. Україна активно взаємодіє з глобальними компаніями, партнерами з ЄС і НАТО, обмінюється даними про нові види загроз, отримує технічну допомогу, долучається до спільних кібернавчань. У світі, де хакерські атаки вже давно не мають кордонів, така співпраця стає життєво необхідною.

Завдяки цим зусиллям державні цифрові системи України залишаються доступними, надійними та захищеними навіть у найскладніші моменти – коли одночасно ведеться війна, лунають сирени й ширяться інформаційні атаки. Це – тиха, але рішуча оборона, яка щодня стоїть на сторожі цілісності інформаційного простору й безпеки мільйонів громадян.

Міжнародна співпраця в сфері інформаційної безпеки сьогодні є не просто додатковим ресурсом – це життєво важливий елемент національної стійкості, без якого неможливо ефективно протистояти сучасним гібридним загрозам. Інформаційні атаки не мають кордонів, і ворожі кампанії часто охоплюють одночасно десятки країн. Тому лише спільними зусиллями, через об'єднання досвіду, знань і ресурсів можна створити дієвий фронт спротиву [40, с.111].

Україна вже має потужну підтримку на цьому напрямі. Зокрема, співпраця з НАТО у сфері кібербезпеки дозволяє не лише вчитися у партнерів, а й вносити свій внесок у формування колективної безпеки. Це включає як участь у спільних проєктах, так і залучення до регулярних навчань, що моделюють реальні сценарії інформаційних атак. Такі практики допомагають державам не лише бути готовими до надзвичайних ситуацій, а й налагоджувати ефективну комунікацію в умовах кризи.

Одним із важливих інструментів є обмін розвідувальною інформацією. Йдеться не лише про фактичні дані щодо джерел дезінформації, ботоферм або технічних атак, а й про аналіз наративів, які поширюються ворогом у різних країнах. Це дозволяє оперативно реагувати на інформаційні кампанії ще до того, як вони досягнуть максимальної шкоди, і передбачати сценарії подальших атак.

Велике значення мають і міжнародні конференції, круглі столи, обміни між фахівцями – не як формальності, а як середовище, в якому народжуються нові підходи до інформаційного захисту. Саме під час таких зустрічей розробляються загальні стандарти, протоколи взаємодії, а також інструменти, які можна адаптувати до реалій конкретної держави [51, с.57].

Таким чином, Україна вже сьогодні є не лише об'єктом допомоги, а й активним гравцем у світовій інформаційній спільноті. Вона ділиться своїм

унікальним досвідом – адже за останні роки пройшла крізь безпрецедентну хвилю інформаційного тиску – і водночас зміцнює власну безпеку через міжнародну солідарність. Бо в інформаційній війні, як і в будь-якій іншій, перемога – це справа спільна. І тільки в союзі з іншими країнами можна ефективно захистити правду, свободу слова та національний суверенітет.

4.2. Роль державних інституцій та міжнародних організацій у боротьбі з інформаційною агресією

В умовах інформаційної війни, яка ведеться не лише на полі бою, а й у цифровому просторі, роль державних інституцій та міжнародних організацій набуває критичного значення. Їхня участь у протидії інформаційній агресії є ключовою як на рівні окремої держави, так і в глобальному контексті. В основі цієї боротьби лежить злагоджена система дій, чітка міжвідомча координація, постійне удосконалення нормативно-правової бази та активна міжнародна співпраця (рис.4.1).

З боку держави цю боротьбу очолюють ключові установи, зокрема Рада національної безпеки і оборони (РНБО), Служба безпеки України (СБУ), Міністерство оборони, Державна служба спеціального зв’язку, Міністерство цифрової трансформації та Національна рада з питань телебачення і радіомовлення. Вони несуть відповідальність за формування та впровадження стратегій інформаційної безпеки, здійснюють щоденний моніторинг інформаційного простору, виявляють загрози, аналізують ризики та оперативно реагують на ворожу пропаганду та дезінформаційні кампанії [14, с.19; 60; 67, с.36; 68, с.108].

Рисунок 4.1. Роль державних інституцій [46]

Окрему увагу держава приділяє формуванню законодавчої бази, яка дозволяє вводити санкції проти медіа та осіб, що поширюють шкідливу інформацію, а також блокувати доступ до фейкових платформ. Такі заходи спрямовані не на обмеження свободи слова, а на захист інформаційного суверенітету країни [60].

Водночас не менш важливою є підтримка незалежних засобів масової інформації та розвиток критичного мислення серед громадян, що досягається шляхом надання дотацій незалежним медіа, створення англомовних ресурсів, орієнтованих на світову аудиторію, на кшталт UkraineWorld.org, а також реалізації освітніх ініціатив, спрямованих на підвищення рівня медіаграмотності [69, с.108, с.108].

Інформаційна безпека також неможлива без надійного захисту інфраструктури: держава інвестує у зміцнення кіберзахисту, модернізує IT-системи органів влади, готується до можливих кібератак і підвищує стійкість критичних систем до зовнішніх втручань [72, с.214].

В цій боротьбі держава активно співпрацює з громадянським суспільством, експертним середовищем та міжнародними партнерами. Важливим стає обмін досвідом, проведення спільних навчань, реалізація просвітницьких програм та підтримка ініціатив, що сприяють підвищенню обізнаності громадян про загрози інформаційного характеру. Така взаємодія формує стійкий щит перед обличчям сучасних гібридних викликів.

В свою чергу, міжнародні організації відіграють також надзвичайно важливу роль у зміцненні інформаційної безпеки України, сприяючи як захисту держави від дезінформаційних атак, так і розвитку демократичного інформаційного середовища (рис.4.2). Україна активно співпрацює з Європейським Союзом, НАТО, ООН, ОБСЄ та іншими впливовими структурами, які надають не лише технічну, а й експертну допомогу. Завдяки такій взаємодії вдається координувати заходи кіберзахисту, розробляти та впроваджувати міжнародні стандарти протидії фейковим наративам і підвищувати стійкість держави до інформаційних впливів [69, с.108].

Рисунок 4.2. Роль міжнародних організацій

Окрему цінність мають міжнародні проєкти, освітні ініціативи та дослідницькі програми. Спільні тренінги для журналістів, аналітиків і держслужбовців, обмін досвідом, впровадження передових практик із медіагігієни та фактчекінгу, а також можливість поширювати правдиву інформацію через глобальні англомовні платформи сприяють зміцненню позицій України на інформаційному фронті. Важливим чинником в цьому процесі є партнерство з провідними світовими медіа, яке дозволяє транслювати об'єктивну інформацію про події в Україні за кордоном і розширювати підтримку міжнародної аудиторії [28].

Однією з дієвих відповідей на інформаційну агресію з боку Росії стало запровадження санкцій. Країни Заходу в межах спільної політики запроваджують обмеження для російських пропагандистських каналів, блокують доступ до ворожих інформаційних ресурсів та вживають заходів для ліквідації мереж дезінформаційних впливів на своїх територіях. Це не просто ускладнює агресору поширення неправдивого контенту, а формує чітку позицію щодо неприпустимості маніпуляцій у глобальному медіапросторі [69, с.108].

В центрі всіх цих зусиль – ідея міжнародної солідарності. Підтримка України в інформаційній сфері з боку партнерів – це не лише прояв політичної дружби, а й стратегічно важливий фактор стабілізації ситуації як всередині країни, так і в ширшому регіональному контексті. Така солідарність дозволяє швидко й ефективно реагувати на нові виклики та агресивні інформаційні операції [28, с.60].

Із зазначеного можна зробити висновок, що протистояти інформаційній загрозі можливо лише завдяки тісній співпраці між державою, громадянським суспільством і міжнародною спільнотою. Комплексний підхід, що поєднує правові механізми, санкції, розвиток незалежних медіа, посилення медіаграмотності населення та широке міжнародне партнерство, є запорукою успішної боротьби з дезінформацією. Лише поєднання внутрішніх реформ і потужних зовнішніх зв'язків здатне створити надійний щит проти сучасних інформаційних викликів.

4.3. Створення інформаційної безпеки в умовах гібридної війни

В реаліях сучасної гібридної війни, коли за кожним словом в медіа може стояти стратегічний розрахунок, а інформація використовується як зброя не менш небезпечна, ніж ракети чи танки, питання інформаційної безпеки стає життєво важливим для кожного з нас. Більше не можна розглядати інформаційний простір лише як нейтральне середовище для вільного обміну думками чи дискусій – сьогодні це арена щоденної боротьби, де визначається, наскільки ми, як суспільство, здатні зберегти єдність, критичне мислення та віру в свою державу.

Інформаційна війна не обмежується фейковими новинами чи пропагандою – вона проникає в кожен дім через стрічку новин, соцмережі, навіть повсякденні розмови. Її мета – посіяти страх, сумнів, зневіру, роз'єднати суспільство, підірвати довіру до інституцій, розмити межі між правдою і маніпуляцією. У такому середовищі наша моральна стійкість стає не менш важливою, ніж обороноздатність на фронті. І саме тому інформаційна безпека – це не лише компетенція спеціалістів чи державних структур, це щоденна відповідальність кожного громадянина [21; 41].

Від здатності суспільства розпізнавати загрози, не піддаватися паніці, вчасно фільтрувати джерела і критично ставитися до повідомлень, залежить не лише атмосфера в суспільстві, а й стратегічна стійкість цілої країни. Кожен фейк, як невидимий снаряд, може влучити в серце нашої єдності – і навпаки, кожен свідомий крок у бік правди, кожен акт інформаційної грамотності – це щит, що захищає нашу демократію, наші родини, наше майбутнє [34, с.150].

Надійна інформаційна безпека – це не просто набір технічних заходів, а живий, постійно діючий процес, який потребує злагодженої взаємодії між різними структурами, рівнями управління і навіть окремими людьми. В нашій реальності, коли інформація стала не лише джерелом знань, а й інструментом впливу, маніпуляцій і навіть зброєю, першочерговим завданням є пильне, безперервне спостереження за тим, що відбувається в інформаційному просторі.

Це спостереження – не абстрактна функція, а щоденна кропітка праця спеціалістів, які аналізують медіа, моніторять соціальні мережі, перевіряють підозрілі повідомлення, відстежують появу фейкових наративів або спроби запустити інформаційні атаки. Вони першими помічають тривожні сигнали – будь-то раптовий сплеск ворожої пропаганди, організована хвиля коментарів, які сіють паніку, чи навіть замаскована кібератака.

Цю роботу виконують не лише державні установи, які мають відповідні повноваження та інструменти. До цієї боротьби залучені також волонтери, експертні аналітичні центри, незалежні журналісти, технічні фахівці, які створюють складні алгоритми для автоматичного виявлення дезінформації. Вони працюють із сучасними цифровими технологіями, зокрема й тими, що базуються на штучному інтелекті, що дозволяє реагувати на загрози швидше та точніше [34].

Це поєднання людської пильності, фахової експертизи та інноваційної техніки створює надійний захисний бар'єр – своєрідний інформаційний щит України. Щит, що не лише відбиває атаки, а й зміцнює довіру суспільства до правдивої, верифікованої інформації. Всі ці люди – державні аналітики, айтішники-волонтери, фактчекери, військові інформаційного фронту – це невидимі бійці, які щодня працюють для того, щоб ми могли читати новини без страху бути ошуканими, щоб наше суспільство залишалося єдиним, згуртованим і сильним.

Однак моніторинг – лише частина справи. Не менш важливою є здатність держави швидко й адекватно реагувати. Для цього необхідно мати чітко виписані й дієві законодавчі та адміністративні механізми, що дозволяють своєчасно блокувати ворожі ресурси, притягати до відповідальності осіб, які поширюють дезінформацію, і впроваджувати санкції проти медіа, що працюють на країну-агресора. Лише за наявності правового інструментарію можлива ефективна протидія інформаційним злочинам.

Водночас важливою залишається й стратегічна комунікація: суспільство має отримувати правдиву, вчасну й чітку інформацію від легітимних джерел.

Побудова ефективної системи державних комунікацій – це не просто передача новин, а створення механізму довіри, який допомагає уникнути паніки, розвінчати фейки та сформувати єдиний інформаційний фронт.

Інформаційна безпека неможлива без належного захисту кіберпростору. Кожен державний орган, бізнесова структура, громадська організація – це потенційна мішень для хакерських атак. Тому впровадження сучасних стандартів кіберзахисту, регулярний аудит систем, підвищення кваліфікації фахівців у цій галузі – все це є невід'ємними елементами захисту цифрової держави.

Окрему роль відіграє освіта. Формування критичного мислення, уміння розпізнавати фейки, розуміння механізмів інформаційних маніпуляцій має починатися ще зі школи. Підвищення рівня медіаграмотності серед усіх верств населення – це довготривала, але вкрай необхідна інвестиція в стійкість держави [34, с.150].

І нарешті, жодна країна не може протистояти таким викликам наодинці. Обмін досвідом із партнерами, участь у міжнародних ініціативах, інтеграція у європейські та світові безпекові структури створюють передумови для колективного захисту. В світі, де загрози не мають кордонів, лише скоординовані дії можуть гарантувати стабільність і безпеку.

На практиці забезпечення інформаційної безпеки в умовах гібридної війни потребує цілеспрямованих і багаторівневих дій з боку держави, громадянського суспільства та міжнародних партнерів. Одним із важливих напрямів є впровадження державних програм моніторингу й швидкого реагування на інформаційні загрози. Наприклад, діяльність Центру стратегічних комунікацій та інформаційної безпеки дозволяє своєчасно виявляти фейки, дезінформацію та інші інформаційні атаки, надаючи суспільству перевірену та достовірну інформацію.

Одним із ключових напрямів захисту інформаційного простору України в умовах гібридної війни стало цілеспрямоване блокування проросійських медіаресурсів, а також запровадження санкцій проти платформ і джерел, які

свідомо займаються інформаційним терором. Йдеться не просто про обмеження доступу до певних сайтів чи каналів – це передусім про захист людей від систематичного психологічного впливу, від маніпуляцій, брехні та паніки, які можуть роз'їдати суспільну довіру зсередини.

Такі ресурси часто маскуються під звичайні новинні портали чи блогерські канали, але їхня мета – посіяти розбрат, спровокувати страх, змусити українців сумніватися в власній державі, її спроможності захищати та діяти в інтересах громадян. Через спотворену інформацію вони намагаються підірвати впевненість в спільній меті, змусити відчути розпач або байдужість.

Рішення про блокування таких джерел – це не прояв цензури, а життєво необхідний крок, який дозволяє захистити наш інформаційний простір як тил. Адже в сучасній війні інформація – це не просто дані, це зброя. І коли ця зброя в руках агресора, вона може бути не менш небезпечною за ракети.

Кожне таке блокування – це ще один акт турботи про ментальне здоров'я українців, про єдність, про збереження правди як основи нашого національного спротиву. Саме тому ці заходи спрямовані не на заборони заради заборон, а на створення безпечного середовища, в якому кожен може отримувати перевірену інформацію, бути впевненим у завтрашньому дні та залишатися частиною сильної, згуртованої спільноти.

Однією з найважливіших складових захисту інформаційного простору сьогодні стає саме просвітницька діяльність, адже вона звертається не до систем і технологій, а до найголовнішого – до людини. В сучасному світі, де ми щодня отримуємо величезний потік новин, повідомлень і коментарів, здатність розпізнавати правду від брехні, не піддаватись емоційним маніпуляціям і зберігати критичне мислення стає не просто навичкою, а життєво необхідною умовою інформаційної безпеки [30, с.30].

В Україні вже кілька років поспіль з великим натхненням та відповідальністю реалізуються різноманітні державні та громадські ініціативи («Медіаграмотність для кожного», Проекти ГО «Детектор медіа», «StopFake», «Інтерньюз-Україна» тощо), мета яких – навчити кожного громадянина бути

свідомим і уважним споживачем інформації. Це не просто абстрактні ідеї чи теоретичні знання, а живі, практичні навички, які кожен може застосувати у повсякденному житті. Вони допомагають розпізнавати маніпуляції, уникати дезінформації, критично оцінювати джерела та зберігати ясність думки в умовах надлишку інформації.

Ці програми відкривають двері до розуміння медіапростору для дуже широкого кола людей – від дітей у школах, які лише починають пізнавати світ і активно формують свої уявлення про нього, до дорослих, які працюють у державних структурах і приймають рішення, що впливають на життя мільйонів. Вони створюють простір, де люди навчаються не боятися інформації, а впевнено користуватися нею, бути активними учасниками суспільства, здатними захистити себе та своїх близьких від впливу фейків та маніпуляцій.

Такі ініціативи – це, перш за все, про довіру: довіру до правди, до суспільства і один до одного. Вони підтримують дух відповідальності й солідарності, допомагаючи будувати міцне, обізнане та стійке суспільство, яке не просто пасивно сприймає інформацію, а свідомо формує свою точку зору і діє на її основі. Цей процес є одним із фундаментів, на яких тримається сучасна демократична Україна, особливо в умовах викликів і загроз, які постали перед нашою країною.

Ці ініціативи мають неймовірно важливе значення не лише через те, що вони надають людям знання, а ще й тому, що вони поступово змінюють глибинне ставлення кожного з нас до інформації, яку ми отримуємо і передаємо далі. Завдяки цим програмам люди починають усвідомлювати: те, що ми читаємо, дивимося, обговорюємо та поширюємо – це не просто випадкові слова чи картинки, а справжня сила, яка може впливати на наші думки, рішення і навіть долі. Вони вчаться ставити собі важливі питання: хто стоїть за цією новиною? Яка її справжня мета? Чи не намагаються мене використати або маніпулювати моєю свідомістю? Це не просто формальності – це початок внутрішнього діалогу, який допомагає розпізнавати правду серед інформаційного шуму. Саме такі прості, але дуже глибинні запитання поступово створюють нову

інформаційну культуру – культуру, в якій кожен бере на себе відповідальність за те, як він споживає і поширює інформацію. Це культура, що не дозволяє бути байдужим або легковірним, а навпаки виховує уважність, критичність і свідомість. І саме завдяки цьому суспільство стає більш захищеним від маніпуляцій, здатним зберігати свою ідентичність, свободу і єдність у складних викликах сучасності.

Особливо цінним і надзвичайно важливим є те, що в основі цих програм лежить глибока повага до людської гідності – до кожної особистості, її права на правдиву інформацію, на вибір, на свободу думки. Це не просто технічні заходи чи сухі інструкції, а живе прагнення будувати суспільство, яке ґрунтується на довірі до фактів, взаємоповазі і чесності. Адже тільки у світі, де люди можуть спиратися на перевірену інформацію і критично мислити, можна побудувати справжню силу – силу, що не руйнується під впливом ворожих наративів, пропаганди та маніпуляцій.

Інформаційна гігієна перестає бути чимось абстрактним, далеким і незрозумілим, вона стає невід'ємною частиною повсякденного життя кожного з нас. Так само, як ми щодня дбаємо про своє здоров'я, ми починаємо дбати про «здоров'я» свого інформаційного простору – очищати його від брехні, перевіряти джерела, не піддаватися емоційним маніпуляціям. Це стає звичкою, такою ж природною і необхідною, як миття рук або дотримання правил дорожнього руху, які зберігають наше життя і безпеку [27, с.3].

Це фундаментальна, невидима на перший погляд робота, результат якої не проявляється миттєво. Але саме вона створює міцну основу для довгострокової стійкості нашого суспільства. Коли кожен починає усвідомлювати свою роль і відповідальність за інформацію, яку споживає і поширює, національна безпека перестає бути виключно прерогативою армії чи державних інституцій. Вона перетворюється на справу всього народу – на спільне зусилля мільйонів громадян, які разом захищають правду, свободу і майбутнє своєї країни. Саме таке суспільство стає незламним, живучим і готовим протистояти будь-яким викликам сучасності.

Міжнародна співпраця в питаннях інформаційної безпеки для України сьогодні – не просто важливий напрям, а життєва необхідність. У той час як наша держава щодня стикається з новими формами гібридної агресії, партнерство з міжнародними союзниками стає міцною опорою в цьому нерівному протистоянні. Особливо потужну підтримку Україна отримує від структур НАТО, Європейського Союзу, USAID та інших авторитетних міжнародних організацій.

Ці партнери не обмежуються лише формальними заявами – вони беруть безпосередню участь у створенні надійного цифрового щита для України. Завдяки спільним проєктам вдається не тільки впроваджувати найсучасніші технології захисту, а й адаптувати міжнародний досвід до наших реалій. Участь зарубіжних експертів, які допомагають розбудовувати систему кіберзахисту, підвищувати кваліфікацію українських фахівців, консультувати в кризових ситуаціях – це приклад справжньої солідарності, яка рятує не лише інформаційний фронт, а й реальні життя.

Співпраця виходить далеко за межі технічних рішень – вона базується на довірі, спільних цінностях і розумінні того, що демократичні країни мають триматися разом перед обличчям авторитарної загрози. Обмін досвідом, спільні тренінги, підтримка українських ініціатив, розробка нових моделей реагування – усе це поступово формує в Україні систему, здатну не лише відбивати атаки, а й діяти на випередження.

Така міжнародна взаємодія – це ще й потужний сигнал агресору: Україна не самотня. За нею стоїть глобальна спільнота, яка визнає її право на правду, свободу і незалежність. І цей союз, заснований на взаємоповазі й спільному прагненні до миру, робить нашу країну сильнішою – не лише в цифровому вимірі, а й у моральному сенсі.

У підсумку можна сказати, що інформаційна безпека в умовах війни – це не лише реакція на ворожі атаки, а передусім створення цілісної, стійкої та динамічної системи, здатної як захищатись, так і попереджати нові виклики. Вона об’єднує технологічні інструменти, освітні ініціативи, потужну

законодавчу базу та широку міжнародну підтримку. Саме така стратегія дозволяє не лише захищати національний суверенітет, а й будувати демократичне, стійке суспільство, здатне зберігати правду і свободу в умовах сучасних викликів.

ВИСНОВОК

Отже, в ході проведеної роботи нами були виконані усі поставлені завдання, в результаті чого було зроблено наступні висновки:

Передусім, ми ґрунтовно охарактеризували теоретичні основи гібридної війни як одного з найнебезпечніших викликів сучасності. Було доведено, що гібридна війна – це не лише поєднання класичних форм збройної боротьби з нетрадиційними, а й цілісна стратегія багатовекторного тиску, де інформаційна складова відіграє ключову роль. Такий тип війни порушує звичні уявлення про фронт, адже він проходить не лише на лінії зіткнення, а в медіапросторі, свідомості людей, у кожному смартфоні, в соціальних мережах і навіть у розмовах за кухонним столом.

Другим кроком стало осмислення ролі інформаційної складової в системі гібридних впливів. Було проаналізовано, як інформаційна зброя впливає на політичну стабільність, громадську думку, моральний дух суспільства, рівень довіри до інституцій. Особлива увага приділялася психологічному впливу, який часто проявляється не у вигляді прямої брехні, а через витончені маніпуляції, перекручування фактів, подачу фейкових наративів у «зручній» для агресора формі. Такий вплив має накопичувальний ефект і працює на розмивання єдності, деморалізацію, розпалювання внутрішніх конфліктів.

Третє завдання дозволило виявити основні інструменти інформаційної агресії. До них належать фейки, пропаганда, діпфейки, дезінформація, створення паралельної інформаційної реальності, інфікування соціальних мереж ботами та тролями, підміна понять і цінностей. Це не лише технічні чи технологічні засоби – це ретельно розроблені механізми впливу на людські емоції, страхи, надії та уявлення про світ. Найнебезпечнішим є те, що людина часто навіть не усвідомлює, що стає об’єктом впливу, і в цьому – головна сила інформаційної зброї.

У рамках четвертого завдання було детально проаналізовано особливості застосування інформаційної зброї в умовах російсько-української війни. Це – безпрецедентний випадок інформаційної агресії, яка триває паралельно з

воєнними діями, використовуючи всі доступні засоби – від телеканалів до Telegram-ботів. Було висвітлено, як РФ використовує медіа для деморалізації українців, поширення паніки, дискредитації ЗСУ, спроб роз'єднати суспільство. Водночас, не менш важливою є і протидія: волонтерські OSINT-ініціативи, державні кампанії з медіаосвіти, діяльність Центру протидії дезінформації, застосування мемів як форми контрпропаганди – все це свідчить про те, що Україна не лише захищається, а й вчиться діяти на випередження.

Нарешті, п’ятим завданням було розроблення практичних підходів до захисту інформаційного простору. Було запропоновано систему заходів, що охоплює як технічні рішення (моніторинг, кіберзахист, блокування деструктивних ресурсів), так і гуманітарні: підвищення медіаграмотності, розвиток критичного мислення, просвітницькі ініціативи, міжсекторальну взаємодію держави, бізнесу та громадянського суспільства. Особливої ваги набуває міжнародна співпраця – Україна активно залучає партнерів з НАТО, ЄС, USAID для побудови стійкої системи інформаційної безпеки. Однак головний ресурс протидії – це люди: обізнані, уважні, відповідальні громадяни, які не дозволяють обманути себе й уміють відрізняти істину від нав’язаного образу.

У підсумку можна стверджувати, що інформаційна складова гібридної війни стала не просто елементом сучасного конфлікту, а його центральною віссю. Від здатності держави і суспільства розпізнавати загрози, швидко на них реагувати, зберігати єдність і спиратись на правду залежить не лише перебіг війни, а й майбутнє демократії, національного суверенітету й свободи слова. Україна вже сьогодні демонструє приклад того, як можливо вистояти у найнебезпечнішій війні – війні за свідомість. І саме ця боротьба, попри її невидимість, визначає, яким буде світ завтра.

Використані джерела

1. Авдєєнко Є. І., Головко О. В., Івасів О. М. та ін. Інформаційна війна: сутність, методи та захист / ред. Є. І. Авдєєнко. Київ : Видавничий дім «Ін Юре», 2018. 532 с.

2. Анісімович-Шевчук О. Інформаційно-комунікативні впливи у сучасних міжнародних відносинах: теоретичний аспект. *Вісник Львівського університету.* Серія філос.-політолог. студії. 2023. Випуск 49, с. 211-218. URL: https://doi.org/10.30970/PPS.2023.49.27 (дата звернення: 30.07.2025)

3. Арістова І. В. Державна інформаційна політика: організаційно-правові аспекти / за заг. ред. О. М. Бандурки. Харків : Університет внутрішніх справ, 2016. 366 с.

4. Афанасьєв І. Ю., Новохатько Л. М., Сінько А. С. Інформаційно-комунікаційна діяльність та аналітика під час російсько-української війни (на прикладі соціальних мереж). *Communications and Communicative Technologies*. 2023. № 23. С. 156–163.

5. Батрименко О.В. Роль соціальних медіа у російсько-українській інформаційній війні. *Політологічний вісник Київського національного університету ім. Т. Шевченка.* 2022. № 89. С. 124-131. URL: https://doi.org/10.17721/2415-881x.2022.89.124-132 (дата звернення: 30.07.2025)

6. Беленчук І. В. Фейки та їх використання російськими масмедіа в умовах інформаційної війни. Магістерські студії. Херсон : ХДУ, 2021. Вип. 21. С. 203–205.

7. Богуш В. М. Інформаційна безпека держави. Київ : МК-Прес, 2005. 432 с.

8. Бондарсук О. В. Відображення у дискурсі ЗМІ пропагандистських кампаній. *Political science*. 2013. № 12 (104). С. 56–66.

9. Булгакова К. В. Інформаційна війна під час воєнного стану: вплив та наслідки для суспільства. С.255-259. URL: https://er.knutd.edu.ua/bitstream/123456789/26142/1/PRPSZISPU_2023_%D0%A0255-259.pdf (дата звернення: 30.07.2025)

10. Валюшко І. О. Основні виклики і загрози в епоху інформаційних війн. *Науковий вісник Дипломатичної академії України*. Зовнішня політика і дипломатія: традиції, тренди, досвід. Частина ІІ. Серія «Політичні науки». 2016. С. 157–162.

11. Васильчук Г. М., Маклюк О. М., Бессонова М. М. Феномен пропаганди та антипропаганди у сучасному світі: історико-політологічний дискурс. Запоріжжя : Інтер-М, 2018. 386 с.

12. Війна Росії проти України: хронологія кібератак. Дослідницька служба Європейського парламенту. 2022. URL: https://www.europarl.europa.eu/RegData/etudes/BRIE/2022/733549/EPRS_BRI(2022)733549_XL.pdf (дата звернення: 13.03.2025).

13. Владлєнова І. В., Кальницький Е. А. Особливості інформаційної війни як засобу вирішення соціально-політичних конфліктів: філософський аналіз. *Психолого-педагогічні проблеми в освітньому процесі* : зб. наук. ст. Харків : Харків. нац. пед. ун-т ім. Г. Сковороди, 2012. 75 с.

14. Галіпчак В. Д. Державно-правовий механізм інформаційної безпеки України в умовах російської агресії // *Науковий журнал «Політикус»*. 2023. Вип. 5. С. 19–24. DOI: http://politicus.od.ua/5_2023/3.pdf (дата звернення: 30.07.2025)

15. Горбань Ю. О. Інформаційна війна проти України та засоби її ведення. Вісник НАДУ. 2015. Вип. 1. URL: http://visnyk.academy.gov.ua/wpcontent/uploads/2015/04/20.pdf (дата звернення: 13.03.2025).

16. Горбулін В. П. Світова гібридна війна: український фронт. Київ : Нац. ін-т стратег. дослідж., 2017. 496 с.

17. Гуцуляк Д.М. Роль інформаційно-медійних технологій як інструменту гібридної війни. *Вчені записки ТНУ імені В. І. Вернадського. Серія: Філологія. Журналістика.* Том 35 (74) № 3 2024. Частина 2. С.52 – 58. URL: https://www.philol.vernadskyjournals.in.ua/journals/2024/3_2024/part_2/11.pdf (дата звернення: 30.07.2025)

18. Данько Ю. А. Соціальні мережі як інструмент інформаційної війни РФ проти України: особливості та механізми протидії // *Сучасне суспільство. 2023.* Вип. 2 (27). URL: https://doi.org/10.34142/24130060.2023.27.2.05 (дата звернення: 30.07.2025)

19. Додонов А. Г., Горбачик Е. С., Кузнєцова М. Г. Сучасні технології та проблеми інформаційної безпеки. Інформаційні технології та безпека : зб. наук. пр. Київ : Ін-т проблем реєстрації інформації НАН України, 2006. 259 с.

20. Доктрина інформаційної безпеки України : затв. указом Президента України від 8 лип. 2009 р. № 14/2009. URL: http://zakon.rada.gov.ua/laws/show/514/2009 (дата звернення: 13.03.2025).

21. Єрмоленко В. Слова та війни: Україна в боротьбі з російською пропагандою : аналіт. вид. / Інтерньюз-Україна. Київ : К.І.С., 2017. URL: https://issuu.com/internews-ukraine/docs/words_and_wars_ukr (дата звернення: 13.03.2025).

22. Залєвська І. І., Удренас Г. І. Інформаційна безпека України в умовах російської військової агресії // *Південноукраїнський правничий часопис. Проблеми становлення правової демократичної держави*. 2022. № 1–2. С. 20–26. DOI: https://doi.org/10.32850/sulj.2022.1-2.4 (дата звернення: 30.07.2025)

23. Запорожець О. Ю. Феномен гібридної війни у сучасних міжнародних відносинах. International relations, part «Political sciences». 2017. №16. URL: http://journals.iir.kiev.ua/index.php/pol_n/index (дата звернення: 13.03.2025).

24. Іваницька Б. Основні методи пропаганди в російському інтернет ЗМІ pravda.ru. *Вісник Нац. ун-ту «Львівська політехніка»*. Серія: Журналістські науки. 2018. № 896. С. 46–58.

25. Іжутова І. Мартін Лібікі: «Що таке інформаційна війна?». Військо України. 2014. URL: http://viysko.com.ua/texnologiji-voyen/martin-libikishhotake-informacijna-vijna (дата звернення: 13.03.2025).

26. Інформаційні атаки в соціальних мережах: дослідження впливу російської дезінформації через рекламу в Facebook [Електронний ресурс] / Центр стратегічних комунікацій та інформаційної безпеки. Київ, 2024. URL:

https://spravdi.gov.ua/wp-content/uploads/2024/04/informaczijni-ataky-v-soczialnyh-merezhah.-doslidzhennya-vplyvu-rosijskoyi-dezinformacziyi-cherez-reklamu-v-facebook.pdf (дата звернення: 30.07.2025).

27. Кондратюк М. О. Інформаційна війна та роль мас-медіа в міжнародних конфліктах. *Вісник Харківської державної академії культури*. 2013. Вип. 41. С. 3–11.

28. Конончук В., Ржевська Н. Інформаційна війна та її вплив на міжнародні дипломатичні процеси: досвід України. *Universum*. 2023. № 3. С. 60–64. URL: https://archive.liga.science/index.php/universum/article/view/604 (дата звернення: 30.07.2025)

29. Копаль О. С., Павленко Ю. В. Інформаційна війна: проблеми та перспективи. Київ : НАДУ, 2015. 192 с.

30. Кривцов В. Ю. Інформаційні заходи оборони держави в сучасних умовах // *Теорія та історія держави і права. Філософія права. Часопис Київського університету права.* 2023. № 1. С. 30–33.

31. Кулеба Д. Війна за реальність. Як перемагати у світі фейків, правд і спільнот. Київ : #книголав, 2022. 384 с.

32. Леонтьєва Л. Є. Пропаганда як інформаційно-психологічний складник політичних процесів. Львів : Львів. нац. ун-т ім. І. Франка, 2004. 298 с.

33. Лизанчук В. Журналістська правда і постправда в контексті гібридної війни Російської Федерації проти України. *Вісник Львівського університету.* Серія: Журналістика. 2019. Вип. 45. С. 323–334.

34. Ліпкан В. А., Максименко Ю. Є., Желіховський В. М. Інформаційна безпека України в умовах євроінтеграції. Київ : КНТ, 2006. 280 с.

35. Магда Є. Виклики гібридної війни: інформаційний вимір. *Наукові записки Інституту законодавства Верховної Ради України.* 2014. № 5. С. 138–142.

36. Магда Є. М. Гібридна війна: сутність і структура феномену. *Міжнародні відносини*. Серія: Політичні науки. 2014. № 4. URL:

http://journals.iir.kiev.ua/index.php/pol_n/article/viewFile/2489/2220 (дата звернення: 13.03.2025).

37. Малик Я. Інформаційна війна і Україна. *Науковий вісник*. 2015. Вип. 15. URL: http://www.lvivacademy.com/vidavnitstvo_1/visnyk15/fail/Malyk.pdf (дата звернення: 13.03.2025).

38. Малькова Т. В. Маси. Еліта. Лідер. Харків : Яуар, 2015. 232 с.

39. Мельник О. В. Інформаційна війна: теоретико-методологічні аспекти. URL: https://journals.iir.kiev.ua/index.php/npi/article/view/215/195 (дата звернення: 13.03.2025).

40. Новицький В. Я. Стратегічні засади забезпечення інформаційної безпеки в сучасних умовах // *Інформація і право.* 2022. № 1 (40). С. 111–118. URL: https://orcid.org/0000-0001-7386-1221 (дата звернення: 30.07.2025)

41. Ожеван М. А., Шевченко О. В. Війна інформаційна. Українська дипломатична енциклопедія : у 2 т. Київ : Знання України, 2004.

42. Онопрійчук А. Підходи та методи інформаційного протиборства в Російсько-Українській війні. Політ. Сучасні проблеми науки. Міжнародні відносини : тези доп. XXII міжнар. наук.-практ. конф. здобувачів вищ. освіти і молодих учених (Київ, 2022). Київ : НАУ, 2022. 142 с.

43. Павлюх М. В. Методи та засоби російсько-української інформаційної війни (2014–2022): міфи і риторика пропаганди // *Протидія агресії РФ в умовах інформаційної війни: виклики та загрози : колективна монографія* / за заг. ред. І. І. Мазура, Т. В. Матюшиної. Київ: ДКС-Центр, 2023. С. 309–318. URL: https://doi.org/10.30525/978-9934-26-223-4-127 (дата звернення: 13.03.2025).

44. Патлашинська І. В. Сучасна російсько-українська інформаційна війна: завдання, методи та особливості використання. *Регіональні студії*. 2022. № 84. URL: http://www.regionalstudies.uzhnu.uz.ua/archive/28/15.pdf (дата звернення: 13.03.2025).

45. Пащенко А. Методи та складові сучасної інформаційної війни, вивчення її впливу на свідомість та поведінку людей // Психолого-педагогічні проблеми сучасної школи: зб. наук. праць. 2023. Вип. 2 (10). С. 83–90. URL:

https://library.udpu.edu.ua/library_files/probl_sych_school/2023/2/11.pdf (дата звернення: 30.07.2025)

46. Петрик В. І. Сутність інформаційної безпеки держави, суспільства і особи. URL: http://justinian.com.ua/article.php?id=3222 (дата звернення: 13.03.2025).

47. Петрик В. М., Бедь В. В., Присяжнюк М. М. та ін. Інформаційно психологічне протиборство: підручник. Київ: ПАТ «ВІПОЛ», 2018. 386 с.

48. Пєвцов Г. В. Інформаційна безпека у воєнній сфері: проблеми, методологія, система забезпечення: монографія. Харків: Цифрова друкарня № 1, 2013. 272 с.

49. Політологічний енциклопедичний словник / уклад. Л. М. Герасіна, В. Л. Погрібна, І. О. Поліщук та ін.; ред. М. П. Требін. Харків: Право, 2015. 32 с.

50. Почепцов Г. Г. Сучасні інформаційні війни. Київ: Видавничий дім «Києво-Могилянська академія», 2015. 498 с.

51. Прибутько П. С. Інформаційні впливи: роль у суспільстві та сучасних воєнних конфліктах. Київ: Паливода А. В., 2007. 252 с.

52. Присяжнюк М. Аналіз засобів ведення інформаційної боротьби з використанням інформаційних технологій, форм і способів їх застосування. *Вісник Київського національного університету імені Тараса Шевченка*. Сер. Військово-спеціальні науки. 2007. № 14. С. 31–48.

53. Притула А. М. Пропаганда – компонент гібридної війни: шляхи протидії засобами кримінального права. *Юридична наука*. 2015. № 3. С. 113–122.

54. Пропаганда vs контрпропаганда у медіа просторі: минуле, сучасне, майбутнє: матеріали міжнар. наук.-практ. конф. (Запоріжжя, 12 лютого 2018 р.). Запоріжжя: Інтер-М, 2018. 406 с. URL: https://istznu.org/index.php/journal/article/view/243/192 (дата звернення: 13.03.2025).

55. Радковець Ю. І. Ознаки технологій «гібридної війни» в агресивних діях Росії проти України. *Наука і оборона*. 2014. № 3. С. 45–55.

56. Рак О. А., Шпот С. І., Бардас І. В. Інформаційна війна: фактори, причини, наслідки / за ред. О. А. Рака. Київ: Ін Юре, 2017. 62 с.

57. Рибак М. І., Атрохов А. В. До питання про інформаційні війни. *Наука і оборона*. 2018. № 2. С. 65–77.

58. Рижиков М. М. Міжнародна інформаційна безпека: сучасні виклики та загрози. Київ: Центр вільної преси, 2015. 916 с.

59. Рижков М. Інформаційна війна // *Політична енциклопедія* / Ю. Левенець, Ю. Шаповал та ін. Київ: Парламентське видавництво, 2011. С. 298.

60. Ряполов А. П. Гібридна агресія проти України як виклик модернізації правової політики у сфері інформаційної безпеки // Адміністративне право і процес; фінансове право; інформаційне право. URL: https://doi.org/10.5281/zenodo.15253981 (дата звернення: 30.07.2025)

61. Саєнко О. Г. Інформаційна війна як прояв інформаційного протиборства. *Зб. наук. праць Військового інституту КНУ ім. Т. Шевченка*. 2008. Вип. 12. 147 с.

62. Сампан І. «Манафорт» для Пушиліна. Як Росія рятує рейтинг глави «ДНР» та збирає резервістів. 2020. Цензор.НЕТ. URL: https://censor.net/ua/b3203445 (дата звернення: 01.03.2025).

63. Синчак Б. Прямоефірна інформаційна війна та російсько-українська війна 2022-го на медійному плацдармі // *Український інформаційний простір.* 2022. № 2(10). С. 88–97.

64. Скочиляс-Павлів О. Правові механізми забезпечення інформаційної безпеки в Україні. *Вісник Національного університету «Львівська політехніка».* Серія: Юридичні науки. 2024. № 2 (42). С. 151–157. URL: https://science.lpnu.ua/sites/default/files/journal-paper/2024/jul/35421/skochilyas-pavlivvisnik2.pdf (дата звернення: 30.07.2025)

65. Слюсаревський М. М. Термінологічний словник російсько-української війни. Київ: НАПН України, 2022. 20 с.

66. Смолій В. О., Романова О. Г. Інформаційна війна в Україні: проблеми та виклики. Київ: НАДУ, 2016. 213 с.

67. Солодка О. М. Пріоритети удосконалення інформаційної безпеки України // *Інформація і право*. 2015. С. 36–42.

68. Сопілко І. М. Інформаційна війна проти України та правові засоби протидії злочинним діям. Проблеми формування та реалізації державної політики у сфері інформаційної безпеки України // Юридичний вісник. 2022. № 3 (64). С. 108–114. URL: https://orcid.org/0000-0002-9594-9280 (дата звернення: 30.07.2025)

69. Стичинська А. Б. Інформаційна агресія Російської Федерації: виклики та подолання // Політична культура та ідеологія. 2024. № 1. С. 108–112. URL: https://orcid.org/0000-0002-0519-43051 (дата звернення: 30.07.2025)

70. Стратегія національної безпеки України. URL: http://zakon2.rada.gov.ua/laws/show/389/2012 (дата звернення: 13.03.2025).

71. Стругацький В. Маніпулятивні практики на тлі гібридної війни: філософський аналіз. Київ: ФОП Халіков Р. Х., 2018. 166 с.

72. Твердохліб Ю. Державна політика України щодо забезпечення інформаційно-психологічної безпеки // Вісник Львівського університету. Серія філософсько-політологічні студії. 2019. Вип. 23. С. 214–223. URL: http://fps-visnyk.lnu.lviv.ua/archive/23_2019/33.pdf (дата звернення: 30.07.2025)

73. Ткач В. Ф. Спецпропаганда як інформаційний складник гібридної війни Росії проти України. Київ: Національний інститут стратегічних досліджень, 2016. 109 с.

74. Ткач Д. І. Розвиток інформаційного суспільства: у 10 т. Т. 10: Інформаційно-комунікаційні аспекти міжнародної та національної безпеки: колективна монографія / за наук. ред. Ун-ту економіки та права «КРОК». Київ, 2013. 342 с.

75. Толубко В. Б. Підготовка і ведення інформаційної боротьби в Збройних Силах України: навч. посіб. Київ: НАОУ, 2004. 280 с.

76. Трофименко О. Г., Дубовой Я. В. Еволюція поглядів на інформаційні війни в епоху інформаційного суспільства // Порівняльно-аналітичне право. 2017. № 1. С. 189–192.

77. Цуканова О. В. Інформаційні війни: вплив на суспільство. URL: http://www.sworld.com.ua/konfer34/800.pdf (дата звернення: 13.03.2025).

78. Чирва Р. Інформаційна війна – зброя, страшніша за ядерну. *Профспілкові вісті.* 2014. № 13. С. 2–14.

79. Чистоклетов Л. Г. Інформаційно-психологічні впливи як невід'ємна складова парадигми інформаційної безпеки // Наук. вісник Львів. держ. ун-ту внутр. справ. 2012. 192 с.

80. Чорняк Р. А. Гібридні війни як різновид інформаційних війн XXI ст. // Інформаційні технології і системи в документознавчій сфері. 2024. Червень. С. 164–167. URL: https://jitas.donnu.edu.ua/article/view/15971/15871 (дата звернення: 30.07.2025)

81. Шевчук П. Інформаційно-психологічна війна Росії проти України: як їй протидіяти // *Демократичне врядування.* 2014. Вип. 13. URL: http://lvivacademy.com/visnik13/zmist.html (дата звернення: 13.03.2025).

82. Шпига П. С. Основні технології та закономірності інформаційної війни // Проблеми міжнародних відносин. 2014. Вип. 8. 339 с.

83. Шуляк Н. Інформаційні війни в інтеграційних процесах // Міжнародні інтеграційні процеси: історичний досвід, сучасні виклики та перспективи. 46 с.

84. Яковлєва Н. І. Пропаганда як складова політичної комунікації: автореф. дис. ... канд. політ. наук: 23.00.02 / Київ. нац. ун-т ім. Т. Шевченка. Київ, 2010. 18 с.

85. Bondarsuk O. V. Reflection in the discourse of the media of propaganda campaigns // Political science. 2013. No. 12 (104). P. 49–53. URL: http://example.com (дата звернення: 13.03.2025).

86. Cold War in Space: Reconnaissance Satellites and US-Soviet Security Competition. URL: https://doi.org/10.4000/ejas.20427 (дата звернення: 13.03.2025).

87. Fake News and Information Warfare: An Examination of the Political and Psychological Processes From the Digital Sphere to the Real World. URL: https://www.researchgate.net/publication/348129387 (дата звернення: 13.03.2025).

88. Ivanytska B. Basic methods of propaganda in Russian Internet media pravda.ru // Journal of Lviv Polytechnic National University. Series: Journalistic Sciences. 2018. No. 896. P. 54–58. URL: http://example.com (дата звернення: 13.03.2025).

89. Strategic Information Warfare: A New Face of War. RAND Corp, 2014. URL: http://www.rand.org/pubs/monograph_reports/MR661/index2.html (дата звернення: 13.03.2025).

90. The Ethics of Cyberweapons in Warfare. URL: https://faculty.nps.edu/ncrowe/ethics_of_cyberweapons_09.htm (дата звернення: 13.03.2025).