Кам’янець-Подільський національний університет імені Івана Огієнка
Історичний факультет
Кафедра політології та філософії

Дипломна робота

бакалавра

з теми: ІНФОРМАЦІЙНІ ВІЙНИ СУЧАСНОСТІ: ЗАСОБИ ТА МЕХАНІЗМИ ВЕДЕННЯ

Виконала:
студентка P1B23z групи
спеціальності 052 Політологія
заочної форми навчання
ХАРЧУК Олександра

Науковий керівник:
Грубі Т. В., в.о. завідувача кафедри
політології та філософії
кандидат соціологічних наук, доцент

Рецензент:

_____

Кам’янець-Подільський
2026

ЗМІСТ

ВСТУП…… 3

РОЗДІЛ 1. ТЕОРЕТИКО-МЕТОДОЛОГІЧНІ ЗАСАДИ ДОСЛІДЖЕННЯ ІНФОРМАЦІЙНИХ ВІЙН…… 8

1.1. Сутність та еволюція поняття «інформаційна війна» в політологічному дискурсі……8

1.2. Класифікація засобів ведення інформаційних війн: традиційні, цифрові та когнітивні інструменти……..16

1.3. Стратегічні комунікації та публічна дипломатія в системі інформаційного протистояння……...23

Висновки до розділу 1……28

РОЗДІЛ 2. МЕХАНІЗМИ РЕАЛІЗАЦІЇ ІНФОРМАЦІЙНОГО ВПЛИВУ В СУЧАСНИХ ЗБРОЙНИХ КОНФЛІКТАХ……..30

2.1. Цикли, фази та операційні моделі ведення інформаційних війн……30

2.2. Інституційні та правові механізми протидії інформаційним загрозам у світовій практиці ……...36

2.3. Особливості інформаційної агресії проти України та стратегії національної протидії……45

Висновки до розділу 2……50

ВИСНОВКИ……..52

СПИСОК ВИКОРИСТАНИХ ДЖЕРЕЛ……..56

ВСТУП

Актуальність дослідження поняття інформаційної війни залишається одним із найбільш дискусійних у сучасній політології. У науковому середовищі відсутній консенсус щодо його сутності: чи це окреме явище, технологія в межах гібридних конфліктів, чи атрибут будь-якого протистояння. Ця концептуальна невизначеність набуває гостроти в інформаційну епоху, коли доступ до знань і контроль над комунікацією стають визначальними ресурсами влади.

Відсутність єдиного розуміння інформаційної війни ускладнює не лише теоретичний аналіз, а й оцінку реальних загроз. З одного боку, без чіткого визначення неможливо розмежувати інформаційну війну, пропаганду, психологічну операцію чи кібератаку. З іншого, практика демонструє, що такі дії вже детермінують наслідки схожі за своїми масштабами зі збройними конфліктами.

Для України, яка з 2014 року, а після повномасштабного вторгнення 2022 р. з особливою інтенсивністю перебуває в стані гібридної війни з російською федерацією, інформаційне протистояння стало критичним виміром національної безпеки. Загрози в цій сфері мають специфічний характер. Поряд із фізичним знищенням інфраструктури противник здійснює системний вплив на масову свідомість українців. Основним інструментом тут виступає дезінформація, зокрема поширення фейкових відомостей про оточення, втрату управління чи нестачу ресурсів. Це провокує панічні настрої та підриває довіру до владних інституцій і військового командування. Додатковими засобами інформаційних атак є скоординовані дії в соціальних мережах із використанням ботоферм, дипфейків та автоматично згенерованого контенту, спрямовані на розхитування внутрішньої стабільності й створення штучних розколів між різними соціальними групами населення. Кібератаки на критичну інфраструктуру, а також фейкові новини про евакуацію чи здачу міст є складовими інформаційно-

психологічних операцій, кінцевою метою яких виступає зниження волі населення до спротиву.

Окремим фронтом інформаційної війни є міжнародна аудиторія. За допомогою наративів про недемократичність України, високий рівень корупції чи неспроможність до контрнаступальних дій противник прагне зменшити обсяги військової, фінансової та політичної підтримки з боку країн-партнерів.

Незважаючи на значну кількість наукових праць з цієї проблематики [16, 23, 34 та інш.], системний аналіз засобів (традиційні медіа, цифрові платформи, когнітивні атаки, технології штучного інтелекту) і механізмів (цикли ведення інформаційної війни, фазові моделі, операційні схеми, а також інституційні та правові механізми протидії) залишається недостатньо вивченим. Потребують більш глибокого аналізу технології впливу в межах інформаційної війни і способи ефективного реагування на них.

Український досвід протидії інформаційній агресії, включаючи діяльність Центру протидії дезінформації, волонтерські кіберініціативи, програми підвищення медіаграмотності населення та системи психологічної підтримки військовослужбовців й цивільного населення є унікальним. Його вивчення дозволить не лише адаптувати наявні теоретичні моделі, а й сформувати дієві практики протидії інформаційним викликам і загрозам. Саме це й зумовило вибір теми дослідження: «Інформаційні війни сучасності: засоби та механізми ведення».

Метою дослідження є аналіз засобів та механізмів ведення інформаційної війни як інструменту сучасної геополітики та ефективних напрямів протидії інформаційній агресії в умовах російсько-української війни.

Для досягнення зазначеної мети сформовано **такі завдання дослідження**:

– визначити теоретико-методологічні засади дослідження інформаційних війн та систематизувати їх понятійний апарат.

– розкрити структурно-функціональні характеристики механізмів реалізації інформаційного впливу в сучасних збройних конфліктах.

– проаналізувати інституційні та правові механізми протидії інформаційним загрозам у міжнародній практиці.

– дослідити специфіку інформаційної агресії проти України та охарактеризувати стратегії національної протидії в умовах російсько-українського протистояння.

Об'єктом дослідження є інформаційні війни сучасності. **Предметом дослідження** є засоби та механізми ведення інформаційних війн, механізми протидії їм.

Методологічні засади дослідження базуються на комплексному міждисциплінарному підході. Діалектичний метод застосовувався для дослідження інформаційної війни в динаміці її розвитку та внутрішніх суперечностей, зокрема для аналізу взаємодії між суб'єктом агресії та об'єктом впливу як безперервного процесу «дії-протидії» і «виклику-відповіді».

Системний метод дозволив проаналізувати інформаційну агресію як цілісну систему скоординованих дій, підпорядкованих досягненню єдиної стратегічної мети. Метод аналізу та синтезу застосовувався для виокремлення структурних складових інформаційної війни.

Контент-аналіз і дискурс-аналіз використовувалися для дослідження наративного виміру інформаційних війн, виявлення стійких пропагандистських конструктів, тематичних домінант та образно-символічних патернів у масивах медіатекстів. Порівняльний метод дозволив порівняти інституційні та правові механізми протидії інформаційним загрозам у різних державних контекстах. Метод кейс-стаді забезпечив поглиблений аналіз конкретних інформаційних кампаній, зокрема в контексті російсько-української війни та інституційних практик ЄС і НАТО.

Практичне значення дослідження результати дослідження можуть слугувати теоретичною базою для подальшого вивчення інформаційно-психологічних механізмів впливу в умовах гібридної війни.

Узагальнені в роботі засоби та механізми ведення інформаційної війни доцільно використовувати при виконанні науково-дослідних проєктів здобувачами вищої освіти, а також у межах навчальних дисциплін «Інформаційна безпека», «Стратегічні комунікації», «Міжнародні конфлікти сучасності».

Окремі положення роботи можуть бути застосовані викладачами для підготовки семінарських занять з курсів «Гібридні війни», «Психологія масових комунікацій», «Політична психологія», «Політична конфліктологія». Крім того, матеріали дослідження можуть використовуватися в роботі студентських наукових гуртків.

Апробація результатів дослідження: Результати дослідження були апробовані в статтях «Цифрові технології та пропаганда у сучасних інформаційних війнах» й опубліковані у збірнику Філософ-і-Я: наукові розвідки студентів Кам'янець-Подільського національного університету імені Івана Огієнка : наук. журнал / гол. ред. А.В. Найчук. Кам'янець-Подільський: Кам'янець-Подільський національний університет імені Івана Огієнка, 2025. Випуск 10 (3), «Дезінформація та інформаційно-психологічні операції у соціальних мережах як механізми сучасних інформаційних війн: український кейс і практики протидії» у збірнику Філософ-і-Я: наукові розвідки студентів Кам'янець-Подільського національного університету імені Івана Огієнка : наук. журнал / гол. ред. А.В. Найчук. Кам'янець-Подільський: Кам'янець-Подільський національний університет імені Івана Огієнка, 2025. Випуск 10 (4) та науковій конференція студентів і магістрантів за підсумками НДР у 2025-2026 н. р. (8-9 квітня 2026 р., м. Кам'янець-Подільський).

Структура роботи. Робота складається зі вступу, двох розділів, висновків до кожного розділу, загальних висновків, списку використаних джерел.

РОЗДІЛ 1. ТЕОРЕТИКО-МЕТОДОЛОГІЧНІ ЗАСАДИ ДОСЛІДЖЕННЯ ІНФОРМАЦІЙНИХ ВІЙН

1.1. Сутність та еволюція поняття «інформаційна війна» в політологічному дискурсі

Сучасний стан розвитку світової політики характеризується суттєвим зростанням ролі інформаційно-комунікаційних технологій як інструменту досягнення геополітичних цілей. Інформація, яка традиційно розглядалася як допоміжний ресурс у XXI ст. перетворилася на самостійний чинник влади та стратегічний актив, контроль над яким визначає позиції держав у системі міжнародного впливу.

Для розуміння сутності інформаційної війни необхідно, перш за все, визначити зміст базових категорій «війна» та «інформація». Остання, згідно із Законом України «Про інформацію», визначається як будь-які відомості та/або дані, які можуть бути збережені на матеріальних носіях або відображені в електронному вигляді [41]. В межах суспільних наук, інформацію розглядають не лише як сукупність даних, але як ресурс влади, засіб комунікації та інструмент впливу на прийняття політичних рішень [54, с. 534].

Поняття «війна» у класичному розумінні передбачає збройне протистояння між державами або соціальними групами з метою досягнення політичних цілей. Одним із варіантів сучасного протистояння є гібридна війна, яка поєднує традиційні збройні методи з невійськовими засобами, серед яких переважають інформаційно-психологічні операції [9, с. 6].

Історична еволюція поняття «інформаційна війна» свідчить про те, що сам термін з’явився значно пізніше, ніж відповідні явища. Елементи інформаційного протистояння простежуються ще в античні часи. Так, Сунь-Цзи у трактаті

«Мистецтво війни» наголошував на важливості обману, дезінформації та психологічного впливу на противника як складових перемоги [51, с. 28]. Він стверджував, що найвищим мистецтвом є не здобуття перемоги у ста боях, а підкорення ворога без бою, що досягається, зокрема, через маніпуляцію його сприйняттям реальності [3, с. 38].

У Давній Греції риторика та публічні промови використовувалися як засоби переконання громадян і формування суспільної думки на користь певних політичних рішень, що також можна розглядати як ранню форму інформаційного впливу [3, с. 40]. Фараони Стародавнього Єгипту активно використовували міфотворчість для легітимації своєї влади та створення сакрального образу правителя, що дозволяло зміцнювати соціальну ієрархію та нейтралізувати потенційних опонентів [3, с. 42].

Середньовіччя стало періодом інституціоналізації інформаційного впливу. У XVII ст. Ватикан створив «Конгрегацію пропаганди віри» (Sacra Congregatio de Propaganda Fide), яка фактично стала першим історично зафіксованим центром підготовки та проведення інформаційно-психологічних операцій. Завданням цієї інституції було поширення католицького впливу через контрольовану комунікацію з населенням інших країн [7, с. 137]. Подібна діяльність Ватикану не була випадковою чи безпідставною: ще за століття до створення Конгрегації теоретичне підґрунтя для маніпулювання суспільною свідомістю та утримання влади через контроль над інформацією заклав італійський мислитель Нікколо Макіавеллі у праці «Державець» [29, с. 75].

Технічний прогрес XIX століття, зокрема поява телеграфу, телефону, а згодом радіо, створив принципово нові можливості для швидкого поширення інформації. Наполеон Бонапарт одним із перших усвідомив силу друкованого слова у військових кампаніях. Його штаб супроводжувала похідна друкарня, яка видавала газети з метою пропаганди серед населення окупованих територій та деморалізації ворога. Він практикував випуск фейкових газет, зокрема, у Парижі

видавався псевдоанглійський часопис, який повністю контролювався імператором. Таким чином, ще до офіційного введення терміну «інформаційна війна» сформувався досить потужний арсенал методів і засобів інформаційного впливу, які згодом були систематизовані та розвинуті у XX ст.

Цей період був переломним у становленні інформаційної війни як самостійного феномену. Перша світова війна продемонструвала ефективність масштабних пропагандистських кампаній. Так, у 1917 році в США був створений Комітет публічної інформації, який організував мережу з 75 тисяч доповідачів, що виголосили понад 755 тисяч промов для 400 мільйонів слухачів про необхідність вступу країни у війну. У 1927 році вийшла книга Гарольда Лассвелла «Техніка пропаганди у світовій війні», яка стала першим системним науковим дослідженням інформаційно-психологічного аспекту воєнних конфліктів. Г. Лассвелл визначив пропаганду як особливий вид зброї, яка впливає на моральний стан ворога та виокремив основні стратегічні цілі пропагандистського впливу: створення ненависті до ворога, формування дружніх відносин із союзниками, збереження нейтралітету третіх країн та деморалізація противника [62, с. 54].

Друга світова війна стала полігоном для масштабного застосування інформаційно-психологічних операцій. Всі країни-учасниці конфлікту створили спеціалізовані структури для ведення пропаганди. У Великій Британії з 1941 року діяв підрозділ політичної війни (Political Warfare Executive), який займався підготовкою та поширенням дезінформації серед військ та цивільного населення.

США у 1942 році заснували Управління військової інформації (Office of War Information), яке проводило інформаційно-роз'яснювальні заходи щодо ролі Америки у війні, спрямовані на підняття бойового духу на фронтах та формування позитивного образу союзників у нейтральних країнах [60, с. 778]. На противагу цьому, особливо відомою стала радіопередача «Токійська троянда» - серія японських пропагандистських радіо-передач, спрямованих на

деморалізацію американських військовослужбовців, яка велася дикторкою Івако Хірано [67, с. 52].

Саме в роки Другої світової війни остаточно сформувалося розуміння пропаганди як важливої складової загальної військової стратегії. Були розроблені та апробовані принципи ведення психологічних операцій: використання правдивих фактів для створення довіри до джерела інформації, адаптація повідомлень до психологічних особливостей цільової аудиторії, поєднання «білої» та «чорної» пропаганди, систематичність та безперервність інформаційного впливу [64, с. 272].

Після закінчення Другої світової війни та початку Холодної війни інформаційне протистояння набуло глобального характеру. Сполучені Штати та Радянський Союз розгорнули масштабні пропагандистські кампанії, спрямовані на формування сприятливого образу своїх політичних систем та дискредитацію опонента. У 1949 році Міністерство оборони США підготувало низку документів, які визначали принципи, завдання та засоби ведення інформаційних протистоянь, зокрема «Ведення операцій психологічної війни» (1949), «Ведення психологічної війни» (1955), «Психологічні операції» (1979) [7, с. 138].

Варто зазначити, що офіційне введення терміну «інформаційна війна» у науковий обіг дослідники пов’язують із різними датами та іменами. Частина авторів посилається на звіт Томаса Рона «Системи зброї та інформаційна війна», підготовлений для Пентагону у 1976 році. У цьому документі вперше зверталася увага на вразливість інформаційної інфраструктури США як у воєнний, так і в мирний час. На думку інших дослідників термін вперше з’явився у 1967 році в книзі Аллена Даллеса «Таємна капітуляція», присвяченій таємним сепаратним переговорам між США, Великобританією та рейхсфюрером СС Гіммлером.

Широкого вжитку він набув після операції «Буря в пустелі» (1991 р.), де інформаційні технології вперше були використані як засіб ведення бойових дій: активно застосовувалися розповсюдження листівок для деморалізації іракських

військ, трансляція пропагандистських радіопередач, демонізація образу Саддама Хусейна (його іменували «дияволом», «арабо-мовним Гітлером»), використання лжесвідків для формування негативного образу іракської армії, а також організація роботи журналістів таким чином, щоб американський глядач не бачив жахливих сцен із театру воєнних дій [7, с. 139]. Саме після цього конфлікту інформаційна війна стала розглядатися як самостійна форма протиборства поряд із традиційними військовими діями.

Сьогодні дефініція «інформаційна війна» визначається по-різному, що пояснюється багатозначністю англійського терміну «information warfare» та належністю авторів до різних наукових шкіл. У західній політології поширеним є визначення, запропоноване дослідниками Оксфордського університету: інформаційна війна - це процес використання інформаційно-комунікаційних технологій з наступальною або оборонною метою для негайного вторгнення, підриву або контролю над ресурсами опонента [73, с. 461]. Американські автори Крістофер Вайт, Тревор Тралл та Браян Мазанець пропонують більш вузьке визначення: навмисне маніпулювання або використання інформації однією стороною щодо противника для впливу на вибір та рішення, які він приймає, з метою отримання військової або стратегічної вигоди [75, с. 15].

Українське законодавство у «Стратегії інформаційної безпеки України» визначає інформаційну війну як форму ведення інформаційного протистояння між різними суб’єктами (державами, неурядовими, економічними та іншими структурами), яка передбачає проведення комплексу заходів з нанесення шкоди інформаційній сфері конкуруючої сторони і захисту власної інформаційної сфери [49]. Згідно інших дефініцій, інформаційна війна - це форма ведення інформаційного протистояння між різними суб’єктами (державами, неурядовими, економічними та іншими структурами), яка передбачає проведення комплексу з нанесення шкоди інформаційній сфері конкуруючої сторони і захисту власної інформаційної безпеки.

Вітчизняні дослідники О. Данильян та О. Дзьобань трактують інформаційну війну як «цілеспрямований вплив на суспільну свідомість противника для досягнення інформаційної переваги, політичних чи військових цілей (у разі інформаційної війни між окремими державами) шляхом заподіяння шкоди інформації та інформаційним системам супротивника» [12, с. 22].

Вітчизняними дослідниками систематизовано існуючі підходи до визначення даного феномену:

– інформаційна війна є сукупністю політико-правових, соціально-економічних та психологічних дій, що передбачають захоплення інформаційного простору та витіснення ворога з інформаційної сфери;

– це найгостріша форма протистояння в інформаційному просторі, що характеризується безкомпромісністю та високою інтенсивністю;

– це спосіб підтримки та ведення військових дій із використанням сучасних електронних засобів;

– Інформаційна війна ототожнюється з кібернетичною війною, тобто є протистоянням між технічними системами [57, с. 328].

Важливою складовою наукового аналізу є виокремлення різних типів інформаційних війн, залежно від сфери застосування та цілей: психологічна війна (вплив на свідомість та психіку населення і військових), кібервійна (протистояння у кіберпросторі), мережева війна (конфлікт між мережевими структурами), ідеологічна війна (боротьба на рівні цінностей та наративів) та радіоелектронна боротьба (придушення систем зв’язку та телекомунікацій) [20, с. 45]. Кожен із цих типів має власні засоби, методи та механізми реалізації, однак у реальних конфліктах вони, як правило, застосовуються в комплексі.

Військово-стратегічний підхід до розуміння інформаційної війни представлений у працях Джона Аркілли, Девіда Ронфельдта та Джеймса Деріана, які визначають її як вид військового конфлікту, що є або самостійною формою

протиборства, або частиною розширеного набору військових дій, що утворюють мережеві та кібервійни. При цьому наголошують на тому, що домінування в інформаційній війні забезпечується за рахунок комп'ютеризації військової техніки та формування мережевої організації збройних сил, а також через руйнування інформаційних систем противника, що позбавляє його здатності отримувати, обробляти та використовувати необхідну інформацію [60, с. 775].

Особливий науковий інтерес становить конфліктологічний підхід, який розглядає інформаційну війну через призму військово-політичного протистояння. Річард Шафранський визначає досліджуваний феномен як збройні дії проти частини системи знань і переконань противника, що мають на меті прихований деструктивний вплив на прийняття політичних рішень контрагентом [69]. Автор наголошує, що чим потужнішими є технологічні можливості та комунікативна сфера держави, тим більш вразливою вона є в інформаційній війні. Цей парадоксальний висновок підкреслює асиметричний характер сучасного інформаційного протистояння: високотехнологічні держави, залежні від складних інформаційних систем, стають більш вразливими до точкових інформаційних атак, ніж країни з менш розвиненою інфраструктурою [69].

Аналіз наукової літератури дозволяє виокремити кілька базисних ознак інформаційної війни: вона ведеться безперервно, не обмежуючись періодом збройного протистояння, пронизує всі сфери суспільного життя від політики до культури і може тривати десятиліттями. Її головною метою є не фізичне знищення супротивника, а вплив на його свідомість, цінності та моделі прийняття рішень. Інформаційна війна характеризується високим рівнем асиметрії: порівняно невеликі ресурси можуть призвести до значних політичних та соціальних наслідків. До того ж, вона тісно інтегрується з іншими формами протиборства, зокрема військовими, економічними, дипломатичними, утворюючи складний гібридний комплекс.

Погоджуємося із позицією вітчизняного дослідника А. Фісуну щодо необхідність комплексного підходу до визначення інформаційної війни. Це відкритий або прихований цілеспрямований інформаційний вплив, який одна сторона здійснює на іншу або сторони діють взаємно, використовуючи систему методів і засобів для впливу на людей, їхню психіку та поведінку, а також на інформаційні ресурси та системи [54, с. 538].

Важливим аспектом сучасного наукового дискурсу є розрізнення понять «інформаційна війна», «інформаційне протиборство» та «інформаційна агресія». Якщо інформаційна війна передбачає активну, цілеспрямовану діяльність із нанесення шкоди інформаційній сфері противника, то інформаційне протиборство є більш широким поняттям, що охоплює всі форми конкуренції в інформаційному просторі, включаючи оборонні дії та захист власних інформаційних ресурсів [20, с. 94]. Інформаційна агресія, своєю чергою, є крайньою формою інформаційної війни, що характеризується відкритим, наступальним характером дій та прагненням завдати максимальної шкоди інформаційному суверенітету держави-жертви [34, с. 120].

Отже, еволюція поняття «інформаційна війна» в науковій думці демонструє перехід від сприйняття її як допоміжного інструменту підтримки воєнних дій до визнання самостійною, а в окремих випадках визначальною формою сучасного військового протистояння. В умовах глобалізації та цифрової трансформації інформаційна війна дедалі частіше розгортається у кіберпросторі, охоплюючи не лише урядові та військові структури, а й широкі верстви населення, що робить її одним із головних викликів національній та міжнародній безпеці XXI ст.

1.2. Класифікація засобів ведення інформаційних війн: традиційні, цифрові та когнітивні інструменти

Сучасна система засобів ведення інформаційних війн є складним, багаторівневим утворенням, що постійно еволюціонує під впливом

технологічного прогресу та трансформації суспільних комунікацій. Для ефективного аналізу досліджуваного феномену необхідно визначити класифікацію інструментів інформаційного впливу, яка б враховувала як історично сформовані, так і новітні засоби.

До традиційних засобів ведення інформаційної війни, належать друковані ЗМІ (газети, журнали, бюлетені), радіо, телебачення, а також інформаційні агентства. Сучасний інформаційний простір використовується провідними світовими державами у військових та політичних конфліктах як з метою оптимізації функціональних спроможностей власних безпекових і оборонних структур, так і для створення нових засобів реалізації власних геополітичних інтересів, зокрема й інформаційної зброї [45, с. 13].

Друковані ЗМІ, попри суттєве зменшення тиражів, залишаються важливим інструментом впливу в регіонах з обмеженим доступом до Інтернету або серед старших вікових груп населення. До того ж вони можуть розповсюджуватися на окупованих територіях або в зонах бойових дій, де Інтернет-зв’язок відсутній або заблокований. Історично листівки були одними з перших масових засобів інформаційно-психологічного впливу: їх скидали з літаків, розповсюджували через агентурну мережу та залишали на території противника [7, с. 139].

Радіомовлення зберігає своє значення як засіб інформаційної війни завдяки низькій вартості приймачів, можливості прийому сигналу на великих територіях (включно з важкодоступними районами) та анонімності слухання. Радіо було головним інструментом пропаганди під час Другої світової війни та Холодної війни, і сьогодні воно активно використовується для мовлення на території противника через короткохвильові станції, які неможливо повністю заглушити. Наприклад, російські радіостанції «Спутник» та «Радио Sputnik» ведуть мовлення багатьма мовами світу, поширюючи проросійські наративи.

Водночас міжнародні мовники, такі як «Радіо Свобода» та «Голос Америки», продовжують вести мовлення в країнах з авторитарними режимами.

Телебачення, незважаючи на поширення інтернет-комунікацій, залишається потужним інструментом формування масової свідомості, особливо серед старших вікових груп населення. Як зазначає О. Дяченко, блогосфера формується як національний сегмент інформаційного простору, однак традиційні медіа все ще є привабливими з точки зору рекламодавців, а аудиторія комерційної реклами продовжує дивитися розважальні програми на телебаченні [15, с. 23]. В умовах гібридного конфлікту традиційні медіа використовуються як для поширення офіційних наративів, так і для прихованої пропаганди. Особливу роль відіграють медіа-скандали та медіатизація політики, які готують ґрунт для інформаційних війн сучасності [40, с. 99].

Інформаційні агентства (Reuters, Associated Press, Agence France-Presse, ТАСС, Сіньхуа тощо) є традиційними й надзвичайно впливовими акторами інформаційного простору. Вони формують первинний потік новин, який потім тиражується іншими ЗМІ. Контроль над інформаційними агентствами або вплив на їхню роботу дозволяє задавати тон висвітленню подій у глобальному масштабі.

Цифрові засоби інформаційної війни стали домінуючими у XXI ст. До цієї категорії належать Інтернет-платформи, соціальні мережі, месенджери, блоги, а також спеціалізоване програмне забезпечення для ведення кібероперацій. Як підкреслюють дослідники, «нові медіа» (англ. new media) є інтерактивними електронними виданнями, що комбінують формати подання інформації, а їхнім контентом може бути відео, онлайн-радіо, телевізійна трансляція, анімація, звукове оформлення та власне. До їх основних характеристик відносять: можливість зворотного зв’язку, прозорість, контент, який зосереджений на певній групі користувачів (User Generated Content), дискусії в коментарях, відсутність цензури (у більшості демократичних країн), зменшення ролі гейткіперів

(професійних редакторів, які відбирають новини) та низький фінансовий поріг входження [50, с. 133].

Соціальні мережі (Facebook, Twitter, Telegram, TikTok, Instagram) стали головним полем битви за свідомість мас. В. Яковлєв характеризує цифрову дезінформацію, яка використовує технології «впливу нано-інфлюенсерів», «бджолиного рою», «шкарпеткових ляльок» (найпростіші з них називаються «бібабо»), спін-докторінгу тощо, як новий пропагандистський стиль соціальних мереж, які неодноразово доводили свою ефективність, і саме тому вони є невід'ємною частиною сучасних інформаційних війн [58, с. 36-37].

Блоґи та блоґери стали новими суб'єктами інформаційного простору, які часто мають більшу довіру аудиторії, ніж традиційні журналісти. Як зазначає О. Дяченко, актуальною тенденцією в рамках розвитку україномовного інформаційно-комунікаційного простору є становлення блогів, які виступають як його важливий сегмент, і формування повноцінної україномовної блогосфери [15, с. 23]. Блоги, не будучи ЗМІ за своєю комунікативною природою, демонструють свою ефективність на політичних майданчиках шляхом активної праці з масовою аудиторією. Все частіше вони використовуються для соціалізації та консолідації своєї аудиторії (майбутнього електорату) і є потужним інструментом для освіти політичних віртуальних спільнот та соціальних мереж [15, с. 24].

Месенджери (Telegram, WhatsApp, Signal, Viber) становлять особливу категорію цифрових засобів інформаційної війни через закритість комунікації, шифрування повідомлень та можливість створення великих груп і каналів. Так, Telegram став ключовою платформою для поширення пропаганди під час російсько-української війни завдяки анонімності адміністраторів каналів, відсутності ефективної модерації та можливості публікувати великі обсяги контенту.

Окремою групою є спеціалізоване програмне забезпечення для ведення кібероперацій, яке включає комп'ютерні віруси, троянські програми, логічні

бомби, програми-шпигуни та інші види шкідливого програмного забезпечення (malware). Як слушно зазначає О. Левченко, інформаційна зброя може бути класифікована як така, що впливає на інформаційні ресурси, мережі та системи державного та військового управління (інформаційно-технічна зброя), та така, що впливає на психічну сферу, свідомість, підсвідомість, морально-психологічний стан соціальних груп та суспільства в цілому (інформаційно-психологічна зброя) [27, с. 142]. При цьому, кібератаки можуть використовуватися як для прямого знищення інформаційних систем (наприклад, атака на енергомережу), так і для викрадення та публікації компрометуючої інформації (злам + злив).

Боти (автоматизовані акаунти) та мережі тролів (скоординовані групи, що пишуть коментарі від реальних осіб) є важливими інструментами маніпулювання громадською думкою в цифровому просторі. Вони можуть генерувати тисячі повідомлень за хвилину, створюючи тренди, зміщуючи порядок денний та пригнічуючи альтернативні думки. Тролі, своєю чергою, імітують реальних користувачів, ведуть дискусії, поширюють дезінформацію та провокують конфлікти.

Алгоритми соціальних мереж, що базуються на машинному навчанні, самі по собі можуть ставати засобами інформаційної війни, навіть без свідомого втручання. Системи персоналізації контенту створюють «фільтрувальні бульбашки» та «ехо-камери», де користувач бачить переважно ту інформацію, яка підтверджує його існуючі переконання. Це робить його більш вразливим до маніпуляцій, оскільки альтернативні точки зору виключені з його інформаційного поля. У поєднанні з таргетингом (точним націлюванням реклами на певні групи за інтересами, демографією та поведінкою) алгоритми дозволяють надсилати переконливі повідомлення саме тим, хто сприйме їх найкраще.

Швидко набирають популярності технології штучного генерування контенту (deepfake, синтез голосу, генерація текстів), що дозволяє створити надзвичайно переконливі фальшиві матеріали, які майже не можливо відрізнити

від реальних. Deepfake-відео можуть демонструвати політиків, із недостовірними промовами чи компрометуючими діями. Це руйнує саму основу довіри до візуальних доказів, оскільки глядач більше не може бути впевнений, що бачить реальність. Не зважаючи на те, що створення якісних deepfake вимагає значних технічних ресурсів, технологія швидко дешевшає та стає доступнішою, що в майбутньому може призвести до епідемії синтетичної дезінформації [66, с. 23].

Когнітивні засоби інформаційної війни спрямовані безпосередньо на свідомість, підсвідомість, систему цінностей та моделі прийняття рішень особистістю. Аналітичний центр НАТО визначає когнітивну війну як змагання за здатність змінювати світогляд конкретних груп населення, спрямоване на управління світоглядом людей, їхніми інтересами та цінностями [66, с. 18]. До цієї групи засобів належать наративи (цілісні історії, що пояснюють світ), фрейми (способи подання інформації, які акцентують одні аспекти та ігнорують інші), меми (одиниці культурної інформації, що швидко поширюються), а також пропагандистські кліше та ідеологеми.

Наративи є найбільш потужним когнітивним засобом, оскільки вони не просто передають інформацію, а організовують її в осмислену історію, яка резонує з існуючими цінностями та позиціями аудиторії. Вдало сконструйований наратив може пояснити складні події, запропонувати чіткий план дій. У контексті інформаційної війни вони часто будуються навколо дихотомій «ми - вони», «добро - зло», «жертва - агресор», наприклад, можуть легітимізувати військове вторгнення (наратив «денацифікації» України), виправдовувати репресії чи дестабілізувати політичний режим.

Фреймінг (рамкування) - це техніка подання інформації таким чином, що певні аспекти проблеми опиняються в центрі уваги, а інші залишаються в тіні. Зміна фрейму може кардинально змінити сприйняття однієї й тієї ж події. Наприклад, військову операцію можна фреймувати як «акт агресії», «миротворчу місію», «боротьбу з тероризмом» або «захист прав людини».

Меми - це одиниці культурної інформації, що швидко поширюються в інтернеті, часто у формі зображень із текстом, відеороликів або фраз. На відміну від традиційної пропаганди, меми сприймаються як легкий, розважальний контент, тому вони легко долають захисні бар'єри аудиторії та ефективно поширюють певні ідеї на підсвідомому рівні. Мем може висміяти політичного лідера, дискредитувати військову операцію або, навпаки, підняти бойовий дух та сформувати відчуття єдності. Вірусне поширення мемів робить їх одним із найбільш ефективних і водночас найменш контрольованих засобів когнітивної війни.

Пропагандистські кліше та ідеологеми - це стандартизовані фрази, гасла та концепти, які багаторазово повторюються в медіа, аби створити стійкі асоціації. Наприклад, «глибинна держава», «ліберальний фашизм», «руський мир», «колективний Захід» та інші. Ці кліше виконують роль маркерів приналежності до певного табору та демонізують опонентів, позбавляючи необхідності раціональної аргументації. Уповільнене, але систематичне насаджування ідеологем може змінювати мову політичного дискурсу та впливати на світогляд навіть тих, хто вважає себе критичним спостерігачем.

Психологічні операції (PSYOP) посідають особливе місце в класифікації засобів інформаційної війни, оскільки вони інтегрують традиційні, цифрові та когнітивні інструменти в єдину стратегічну кампанію. Психологічні операції - це ретельно сплановані й здійснювані дії, які використовують різні методи комунікації та інші засоби впливу, спрямовані на визначену аудиторію, з метою формування її сприйняття, настроїв і поведінки для досягнення політичних і військових завдань. Особливістю PSYOP є їхня цілеспрямованість, систематичність та адаптація до психологічних особливостей конкретної аудиторії.

Дослідження, проведене А. Бакіровим та І. Сулейменовим, присвячене комплексному аналізу сучасних форм інформаційної війни в контексті

цифровізації та глобального взаєповпливу [2] розглядає фундаментальні його засади. Серед ключових інструментів інформаційного впливу дослідники називають дезінформацію, використання ботнетів, дипфейки, меметичні стратегії і підкреслюють, що розуміння когнітивних механізмів сприйняття інформації є критично важливим для розробки ефективних стратегій захисту від маніпуляцій.

Українські дослідники Петро Шпига та Роман Рудник систематизували існуючі підходи до визначення інформаційної війни, виокремивши чотири основні концепції, які фактично відображають різні групи засобів.

Перший підхід трактує інформаційну війну як сукупність політико-правових, соціально-економічних та психологічних дій, що передбачають захоплення інформаційного простору та витіснення ворога з інформаційної сфери.

Другий підхід визначає її як найгострішу форму протистояння в інформаційному просторі, що характеризується безкомпромісністю та високою інтенсивністю.

Третій підхід розглядає інформаційну війну як спосіб підтримки та ведення військових дій із використанням сучасних електронних засобів.

Четвертий підхід ототожнює інформаційні війни з кібернетичними війнами - протистоянням між технічними системами [57, с. 328].

О. Левченко пропонує більш детальну класифікацію, виокремлюючи такі види інформаційно-психологічної зброї: пропагандистська (поширення ідей через ЗМІ), психофізична (вплив на фізичний стан людей), нейролінгвістична (використання технік НЛП), психотропна (застосування хімічних засобів), психотронна (використання генеруючих пристроїв), психогенна (провокування психічних розладів) та психоаналітична (глибинна терапія свідомості) [27, с. 144].

Насамкінець зауважимо, що комплексне застосування різних засобів інформаційної війни дозволяє досягнути максимального ефекту впливу: традиційні медіа використовуються для легітимації наративів та охоплення

старшого покоління, соціальні мережі - для швидкого поширення контенту та роботи з молоддю, а когнітивні інструменти - для сформованих на рівні масової свідомості установок.

1.3. Стратегічні комунікації та публічна дипломатія в системі інформаційного протистояння

У сучасній системі інформаційного протистояння дедалі більшого значення набувають не окремі розрізнені заходи інформаційного впливу, а цілісна, скоординована діяльність держави з управління комунікаціями на стратегічному рівні. Стратегічні комунікації є комплексом заходів в інформаційній сфері, спрямованим на забезпечення національних інтересів, що включають не лише зв'язки з громадськістю, але й заходи публічної дипломатії, військово-цивільної співпраці, а також інформаційно-психологічні операції [43].

Термін «стратегічні комунікації» є узгодженим зі стандартною термінологією НАТО та вже офіційно використовується в нормах українського законодавства, зокрема, він був введений до нової редакції Воєнної доктрини України [43]. Як зазначає Р. Шихуцький, у контексті гібридних загроз та повномасштабної війни проти України інформаційний простір є базисним фактором сучасного протистояння, а комунікація еволюціонує із допоміжного інструменту в стратегічний ресурс національної безпеки, що формує легітимність рішень, мобілізує суспільну підтримку та впливає на міжнародну репутацію держави [70, с. 225].

Стратегічні комунікації, на відміну від традиційних комунікаційних кампаній, характеризуються довгостроковим плануванням, міжвідомчою координацією, орієнтацією на досягнення конкретних політичних цілей та інтеграцією від публічної дипломатії до інформаційних операцій.

Публічна дипломатія є ключовою складовою стратегічних комунікацій, що відповідає за комунікацію з іноземними аудиторіями, формування позитивного іміджу держави, просування національних інтересів та створення сприятливого міжнародного середовища. На відміну від традиційної, яка передбачає закриті переговори між офіційними представниками держав, публічна дипломатія орієнтована на безпосередню комунікацію з громадськістю, експертними колами, медіа та неурядовими організаціями інших країн.

У контексті інформаційної війни публічна дипломатія виконує низку важливих функцій:

– вона забезпечує поширення національних наративів серед міжнародної аудиторії;

– сприяє консолідації міжнародної підтримки, формуванню коаліцій та залученню союзників;

– формує умови для легітимації дій держави на міжнародній арені, особливо в умовах збройного конфлікту;

– допомагає поширювати правдиву інформацію про воєнні злочини та порушення міжнародного права.

Сучасні інструменти публічної дипломатії дедалі частіше використовуються не лише для інформування, але й для активного впливу на міжнародні наративи та протидії ворожій пропаганді. Особливу роль у цих процесах відіграють цифрові технології. Цифрова публічна дипломатія передбачає використання соціальних мереж, веб-платформ, подкастів, відеохостингів та інших інструментів для комунікації з міжнародною аудиторією. Це дозволяє долати традиційні медійні бар’єри, звертатися безпосередньо до громадян інших країн та оперативно реагувати на інформаційні виклики. Як показує практика російсько-української війни, цифрова публічна дипломатія

стала ключовим каналом донесення правдивої інформації про перебіг бойових дій, воєнні злочини та гуманітарну ситуацію.

Розкриття розвідувальних даних стало новим, потужним інструментом цифрової публічної дипломатії в умовах інформаційної війни. Як зазначає Л. Сіверт у своєму дослідженні на прикладі Taurus Scandal, де конфіденційна розмова високопоставлених німецьких військових офіцерів про потенційні поставки ракет Taurus в Україну була перехоплена та опублікована росією, що призвело до політичних та дипломатичних потрясінь у Німеччині та серед її союзників [56, с. 97].

Аналогічні процеси спостерігаються і в практиці США. Як зазначає дослідження, опубліковане в Ludovika University Press, розкриття розвідувальних даних як інструмент публічної дипломатії пережило значну еволюцію: від суто операційного інструменту до складного засобу стратегічної комунікації. Аналіз двох нещодавніх випадків - розкриття американських розвідувальних даних перед вторгненням Росії в Україну в 2022 р. та інцидент з китайським метеозондом у 2023 р., демонструють різні підходи до викриття розвідувальних даних: систематичне превентивне поширення в українському випадку та швидке антикризове реагування під час інциденту з метеозондом [68, с. 3]. Ці випадки є запитом щодо перегляду політики балансування операційної безпеки з потребами стратегічних комунікацій американського розвідувального співтовариства [68, с. 8].

Для більш глибокого осмислення характеру впливу держави у міжнародних відносинах використовують концепцію стратегічних наративів, в межах якої державну комунікацію розглядають як спробу внести порядок і запропонувати сенс у складний і суперечливий міжнародний ландшафт [71]. Це дозволило дослідникам переосмислити практику публічної дипломатії, розширити визначення її акторів, краще зрозуміти, як і чому держави комунікують. Крім того, термін «стратегічні наративи» (був введений у 2013 р.) відіграв важливу роль у

відкритті нових напрямів досліджень публічної дипломатії, включаючи аналіз диджиталізації дипломатії та «наративної війни», в якій державні наративи стикаються, детермінуючи фрагментований і позбавлений сенсу світ. Ці кризи включають анексію Криму 2014 р., війну проти ІДІЛ, пандемію COVID-19 2020 р., війни в Україні та Газі [71].

Україна, перебуваючи в стані війни, приділяє значну увагу розбудові системи стратегічних комунікацій. Як зазначає В. Петров, під час візиту Генерального секретаря НАТО Єнса Столтенберга до України в 2015 році було підписано ключовий документ - «Дорожню карту партнерства зі стратегічних комунікацій між РНБО України та Міжнародним секретаріатом НАТО», який передбачає активізацію співпраці та надає Україні доступ, перш за все, до інтелектуального потенціалу країн-членів НАТО в цій сфері [43]. Підписання цього документа стало своєрідним поштовхом, після чого було затверджено відповідний міжвідомчий план його реалізації.

У 2025 році Україна зробила важливий крок у розбудові інституційної спроможності протидії дезінформації на місцевому рівні. Як повідомляє Media Center Ukraine, було запущено нову навчальну програму, спрямовану на допомогу місцевим громадам у виявленні та протидії російській дезінформації [63]. Ця ініціатива належить Центру розвитку стратегічних комунікацій та регіональних досліджень (громадська організація, створена на базі академічної спільноти КНУ імені Тараса Шевченка). Місією центру є створення практичних інструментів для громад щодо виявлення та протидії маніпуляціям з боку ворожих акторів.

Як зазначає Жанна Паціора, директорка Центру, за підтримки Представництва НАТО в Україні, Центру протидії дезінформації при РНБО та Академії СБУ було розроблено чотиримодульну програму, що поєднує навчання та практичні вправи [63]. Вінета Кляйне, керівниця комунікацій Представництва НАТО в Україні, наголосила, що стійкість громад є однією із семи базових вимог до стійкості, встановлених НАТО, а стратегічні комунікації є частиною цієї

системи, базисом проти дезінформації, гібридних загроз, а також компасом, який скеровує суспільство за допомогою надійних, прозорих та заснованих на фактах наративів, укорінених у демократичних цінностях.

Стратегічні комунікації та публічна дипломатія тісно взаємопов'язані, проте не є тотожними поняттями. Публічна дипломатія є складовою стратегічних комунікацій, яка фокусується на зовнішній аудиторії та формуванні позитивного міжнародного іміджу держави. Стратегічні комунікації, в свою чергу, охоплюють як зовнішні, так і внутрішні комунікації, включаючи координацію повідомлень між різними гілками влади, військовими структурами, дипломатичними установами та іншими державними інституціями.

Успішна стратегічна комунікація вимагає узгодження трьох типів наративів: наративу ідентичності (хто ми є), наративу політики (чого ми прагнемо) та наративу системи (як влаштований світ). Усі вони мають бути внутрішньо узгодженими, послідовними в часі та адаптованими до різних цільових аудиторій. Публічна дипломатія відповідає, перш за все, за донесення цих наративів до іноземних аудиторій.

Підсумовуючи зауважимо на тому, що стратегічні комунікації є невід'ємною складовою сучасної системи національної безпеки, особливо в умовах гібридної війни. Вони забезпечують координацію дій різних державних інституцій, формування єдиного національного наративу та ефективну комунікацію як з внутрішньою, так і з зовнішньою аудиторією [70, с. 228].

Ефективна система стратегічних комунікацій вимагає не лише централізованої координації на рівні центральних органів влади, але й розбудови спроможностей на місцевому рівні, зокрема через навчання представників громад, посилення медіаграмотності населення та створення практичних інструментів для виявлення та протидії дезінформації. При цьому, успішне функціонування стратегічних комунікацій неможливе без використання сучасних технологій моніторингу інформаційного простору, серед яких: соціальний

моніторинг, аналітика різних даних та системи ШІ, які дозволяють в реальному часі відстежувати ворожі наративи та оперативно реагувати на них.

Висновки до розділу 1

Проведений у першому розділі аналіз теоретико-методологічних засад інформаційних війн дозволяє констатувати, що цей феномен є складним, багатовимірним явищем, яке не може бути описане в межах однієї наукової парадигми. Інформаційна війна саме на межі XX-XXI ст. набула якісно нових характеристик та перетворилася на автономний механізм досягнення політичних цілей, здатний детермінувати наслідки, цілком співмірні з ефектом від застосування конвенційної зброї.

Серед найбільш універсальних класифікацій засобів інформаційної війни переважає поділ на традиційні, цифрові та когнітивні. При цьому підкреслено, що найбільшої ефективності інформаційні кампанії досягають саме за умови поєднання всіх трьох груп засобів.

Стратегічні комунікації та публічна дипломатія виступають інтегративною рамкою, яка забезпечує координацію різних інформаційних заходів у межах єдиної державної політики. Наголошено на тому, що сучасне інформаційне протистояння вимагає не ситуативних реакцій на окремі ворожі випади, а системної, міжвідомчої скоординованої роботи, що поєднує моніторинг інформаційного простору, активну комунікацію та побудову суспільної стійкості через медіаграмотність.

РОЗДІЛ 2. МЕХАНІЗМИ РЕАЛІЗАЦІЇ ІНФОРМАЦІЙНОГО ВПЛИВУ В СУЧАСНИХ ЗБРОЙНИХ КОНФЛІКТАХ

2.1. Цикли, фази та операційні моделі ведення інформаційних війн

Інформаційна війна в сучасних збройних конфліктах перетворилася з допоміжного інструменту на самостійний вимір протиборства, здатний визначати перебіг і результат військово-політичного зіткнення ще до застосування традиційних засобів ураження. Як слушно зауважує І. Фещенко, така війна є «непомітною», що породжує легковажне ставлення до неї, однак саме ця якість робить її особливо небезпечною: вона не призводить безпосередньо до кровопролиття, але її руйнівний вплив на суспільну свідомість може бути не менш масштабним, ніж наслідки збройного нападу [53, с. 92]. Військова агресія росії проти України розпочалася саме з інформаційної війни, яка сьогодні продовжується паралельно із ескалацією бойових дій.

Будь-яка масштабна інформаційна війна розвивається не хаотично, а за певними циклами, що мають власну внутрішню логіку розгортання та завершення. У науковій літературі цю властивість описують через поняття «життєвого циклу інформаційного впливу», яке запропонували дослідники Б. Ван Нікерк та М. Махараджа [6, с. 45]. Цей цикл охоплює послідовні стадії:

– формування інформаційного приводу (або створення штучного приводу);

– його активне поширення в медійному просторі;

– фазу максимальної резонансності, коли повідомлення досягає цільових аудиторій і викликає заплановану реакцію;

– поступове скорочення інформаційних повідомлень після досягнення мети або втрати актуальності.

Теоретичним базисом для розуміння циклічності прийняття рішень в умовах інформаційного протиборства є так званий цикл Бойда (OODA – Observation–Orientation–Decision–Action), розроблений полковником ВПС США Джоном Бойдом. Хоча сама модель виникла у військовій авіації, її активно адаптують для планування інформаційно-психологічних операцій. Так, ряд дослідників підкреслюють, що використання цього циклу дозволяє приймати оптимальні рішення в умовах невизначеності, яка є невід'ємною характеристикою інформаційного середовища [35, с. 24]. Цикл Бойда можна описати за допомогою чотирьох кроків, які постійно повторюються: спостереження за ситуацією, орієнтування (осмислення побаченого через призму наявних знань і досвіду), прийняття рішення та дія. Перевага в інформаційній війні належить тому, хто проходить цей цикл швидше, ніж противник [35, с. 26].

Українська дослідниця О. Кундеус наголошує, що циклічність не є механічним автоматизмом, вона безпосередньо залежить від наявності чіткої стратегії та «картини успіху» як кінцевої мети. Без неї інформаційні цикли стають самоціллю, втрачають стратегічну спрямованість і швидко розчиняються в інформаційному просторі [26, с. 212].

Найбільш показовим прикладом для вивчення циклічності інформаційного впливу є російсько-українське протистояння, яке триває вже більше десяти років. російська федерація спершу розгорнула масштабну інформаційну війну проти євроінтеграційних прагнень України [10, с. 61]. Коли цей цикл не дав бажаного результату та не вдалося зірвати євроінтеграцію й консолідувати проросійську частину українського соціуму, кремль перейшов до наступного, гібридного, циклу, який включав анексію Криму та війну на Донбасі. Згодом, після чергового інформаційного циклу підготовки (2019-2021 рр.), згодом настала фаза повномасштабного вторгнення. Ці етапи ілюструють спіралеподібну природу інформаційної війни: кожен новий виток включає елементи попередніх, але на вищому рівні інтенсивності та з ширшим використанням технологічних засобів.

Г. Петришин пропонує розрізняти три виміри (простори), у яких одночасно розгортаються інформаційні цикли: внутрішній простір України (де противник прагне посіяти паніку, підірвати довіру до влади та розколоти суспільство), внутрішній простір рф (де пропаганда використовується для консолідації населення та легітимізації агресії) та світовий інформаційний простір (де москва намагається створити альтернативну картину подій, дискредитувати Україну та Захід) [34, с. 117]. У кожному з цих просторів одні й ті самі наративи набувають різних форм: наприклад, гасло «денацифікації» в українському просторі використовується для деморалізації, в російському – для мобілізації, а на Заході – для створення ілюзії «особливої операції» [34, с. 119].

Якщо цикли відображають повторювану динаміку окремих інформаційних кампаній, то фази інформаційної війни описують якісні зміни в її характері, масштабі та цілях інформаційного протистояння. Аналізуючи російсько-українську війну, дослідники виокремлюють чотири основні фази.

Перша фаза – латентна (підготовча). Вона охоплює тривалий період інформаційної підготовки до відкритої агресії, яка розпочалася значно раніше за 2014 р. Фактично інформаційна війна рф проти України стартувала одразу після розпаду СРСР і була спрямована на формування в українському суспільстві комплексу історичних міфів, образів «братнього народу», «спільної історичної долі», а також була фокусувалася на послабленні української державності, національної ідентичності та європейських інтеграційних прагнень [34, с. 119]. В межах реалізації цієї фази використовувалися інструменти історичної ревізії, ідеологічної диверсії, культурного впливу через так звану «м’яку силу», підтримка проросійськи орієнтованих політичних сил і медіа в Україні. Зазвичай такі дії спрямовані на маніпуляцію громадською думкою, формування стереотипів та перекручення фактів, пов’язаних із історією та політикою. Саме цей інструментарій був активно задіяний росією протягом 2000-х – початку 2010-х рр. для підриву української державності зсередини.

Друга фаза – відкритої інформаційної агресії та дезорієнтації. Вона розпочалася під час Революції гідності та особливо активізувалася після анексії Криму й війни на Донбасі. Як зазначає Ю. Данько, у цій фазі росія активізувала використання всіх доступних каналів: телебачення, Інтернет-ресурсів, соціальних мереж, месенджерів, кібератак на українські інформаційні системи та створення дезінформаційних мереж [13, с. 56]. Головними засобами стали Інтернет-ресурси, візуальні й звукові носії інформації, новинні портали, кіберхакерські атаки на інформаційні системи та інформаційні холдинги. У цей період сформувалися та активно поширювалися наративи про «громадянську війну» на Донбасі, «київську хунту», «руську весну» та інші міфологеми, покликані легітимізувати російське вторгнення та деморалізувати українське суспільство [34, с. 119]. В. Антонюк додає, що в цій фазі домінують короткі емоційно заряджені повідомлення, фейки, меми та панічні настрої («бійтеся», «не вірте владі», «не вірте ЗСУ») [1, с. 35].

Третя фаза – інформаційного супроводу бойових дій. Вона настала з початком повномасштабного збройного вторгнення 24 лютого 2022 р. У ній інформаційна війна тісно синхронізується з військовими операціями: дезінформація та пропаганда супроводжують удари по цивільній інфраструктурі, наступальні дії, обстріли та евакуацію населення, створюючи спотворену картину реальності, яка виправдовує чи приховує злочини агресора [53, с. 93]. Ключову роль в інформаційному протиборстві стали відігравати платформи соціальних мереж, месенджери, блоги, дезінформаційні мережі та технології штучного інтелекту. Останній дозволяє генерувати тисячі унікальних фейкових меседжів, адаптованих до різних соціальних груп, створювати глибинні фейки (deepfakes) та автоматизувати процеси поширення дезінформації в соціальних мережах [22, с. 112]. Синхронізація інформаційних кампаній із реальними військовими подіями (зокрема, з ударами по енергосистемі, ракетними атаками на цивільні об’єкти) стає визначальною рисою цього етапу протистояння [13, с. 58].

Четверта фаза – постконфліктного врегулювання та закріплення результатів у масовій свідомості. Вона є гіпотетичною для поточного конфлікту, однак її необхідно враховувати в будь-якій стратегії інформаційної безпеки. Навіть після завершення активних бойових дій інформаційна війна не припиняється – вона переходить у приховану форму, спрямовану на закріплення потрібних наративів, формування історичної пам'яті на умовах агресора, підрив довіри до власних інституцій та створення умов для майбутніх впливів. В ній домінуватимуть наративи про «примирення» на умовах агресора, «спільну історію» та «необхідність забути минуле» [1, с. 36].

Важливо зауважити, що усі ці фази не завжди чітко відокремлені; досить часто вони накладаються, переплітаються та взаємодіють, детермінуючи складний, багатошаровий інформаційний шум. Проте їхнє виокремлення дозволяє системно аналізувати закономірності застосування інструментів інформаційного впливу та розробляти адекватні заходи протидії на кожному етапі конфлікту [10, с. 62].

Якщо цикли та фази описують загальну логіку розгортання інформаційної війни, то операційні моделі – це конкретні алгоритми, технології та методи, за допомогою яких реалізується інформаційний вплив на цільову аудиторію. Найбільш ґрунтовну класифікацію операційних моделей для соціальних мереж (які стали головним полем битви після 2014 р.) запропонував Ю. Данько [13].

Перша модель – мережеві атаки. Вона створює своєрідну завісу з фіктивних повідомлень, що детермінують конфлікти між учасниками соціальної мережі [13, с. 60]. Через фейкові акаунти, групи, бот-мережі запускається велика кількість контенту, який дезорієнтує аудиторію, створює ілюзію стихійної дискусії або широкої підтримки певних поглядів. У 2022-2024 рр. цю модель використовували для масового поширення фейків про «зраду командирів», про втечу українських військових, про нестачу зброї в ЗСУ через анонімні Telegram-канали та фейкові акаунти [13, с. 61].

Друга модель – із залученням добровільних (або примусових) користувачів. Вона передбачає активне використання проплачених або ідейних агентів («тролів») для написання коментарів, постів, які критикують або підтримують певні дії та висвітлюють їх під потрібним кутом [13, с. 62]. Відмінність від попередньої моделі – у створенні симуляції «живої» активної участі реальних людей. У контексті війни її використовували для формування негативного ставлення до мобілізації, військової допомоги Заходу, українських біженців у Європі, а також для поширення паніки серед цивільного населення.

Третя модель – тотального блокування. Вона розглядає можливість блокування користувачів, якщо їхні дії порушують спокій або ображають інших [13, с. 63]. У російській практиці це реалізується як чистка коментарів під провладними дописами, блокування сторінок українських медіа та громадських організацій під приводом боротьби з «екстремізмом». Всі три моделі рідко діють окремо: вони комбінуються, чергуються залежно від фази конфлікту та специфіки соціальної платформи.

Особливого значення у цьому контексті набуває досвід України, яка після 2014 р. створила досить ефективну систему стратегічних комунікацій, а після 2022 р. значно її вдосконалила. І. Іжутова наголошує, що український досвід є унікальним у зв’язку із тим, що вперше в історії стратегічні комунікації країни, що обороняється, були інтегровані у військове планування на рівні оперативних штабів [17, с. 49]. Це означає, що аналіз циклів, фаз і операційних моделей перестав бути суто академічним: він безпосередньо впливає на боротьбу в інформаційному просторі. А знання про те, на якій фазі перебуває чергова модель мережевої атаки, дозволяє українським центрам протидії дезінформації не просто спростовувати брехню постфактум, а випереджати її, запускаючи власні наративи за тими самими операційними моделями [17, с. 50].

Отже, інформаційна війна має виражені цикли, які можуть бути різного масштабу: від коротких (окремі інформаційні операції тривалістю від кількох

годин до кількох днів) до довгих (багаторічні інформаційні кампанії, спрямовані на зміну світогляду цілих поколінь).

Інформаційна війна розгортається одночасно в межах кількох якісно різних фаз: латентна фаза підготовки, фаза інформаційної агресії, інформаційного супроводу бойових дій та постконфліктного закріплення результатів у свідомості мас [1, с. 34-36], при цьому кожна із них має власний набір домінантних методів інформаційно-психологічного впливу.

На операційному рівні інформаційний вплив реалізується через конкретні операційні моделі, такі як мережеві атаки, використання добровільних або проплачених агентів впливу та техніки блокування небажаного контенту. Ці моделі постійно модифікуються з урахуванням нових технологій, насамперед ШІ [22, с. 118].

Успішна протидія інформаційній війні вимагає комплексного підходу, який включає створення системи стратегічних комунікацій, аналітичний моніторинг інформаційного простору, нейтралізацію дезінформаційних каналів, а також активне формування власних наративів, які конкурують з наративами противника [17, с. 48].

2.2. Інституційні та правові механізми протидії інформаційним загрозам у світовій практиці

Міжнародний досвід переконливо свідчить, що інституційні та правові механізми протидії інформаційним загрозам розвиваються у двох основних напрямах. Перший охоплює національне законодавство та спеціалізовані інституції окремих країн, другий – систему колективних інструментів і стандартів, напрацьованих на рівні міжнародних організацій (ООН, ЮНЕСКО, ОБСЄ, Ради Європи, Європейського Союзу, НАТО) в межах їхньої компетенції. Світова спільнота активно розробляє та впроваджує правові й інституційні

механізми стримування дезінформації, оскільки її цілеспрямоване поширення становить загрозу не тільки національній безпеці окремих держав, а й стабільності міжнародних відносин загалом.

Перші спроби міжнародно-правового регулювання інформаційної сфери були реалізовані ще в межах Організації Об'єднаних Націй, однак тривалий час вони зосереджувалися переважно на свободі вираження поглядів, а не на протидії дезінформації як такій. Після 2014 р., коли постала проблема російського втручання в інформаційні простори інших держав, акцент змістився на необхідність розробки колективних механізмів виявлення, моніторингу та нейтралізації ворожих інформаційних впливів. Важливу роль у цьому відіграє ЮНЕСКО, яка координує глобальні ініціативи з розвитку медіаграмотності та захисту свободи медіа в умовах зростання гібридних загроз. ЮНЕСКО послідовно застосовує багатосторонній підхід до врегулювання викликів в інформаційній сфері [74, с. 5].

Особливе місце в системі міжнародних механізмів протидії інформаційним загрозам посідає Організація з безпеки і співробітництва в Європі (ОБСЄ). Її представник з питань свободи медіа – інституція, яка не тільки моніторить стан дотримання свободи слова в державах-учасницях, але й розробляє рекомендації щодо захисту медіа від маніпулятивних впливів. ОБСЄ послідовно виступає за те, щоб заходи протидії дезінформації не використовувалися як інструмент політичної цензури, а відповідали принципам пропорційності та транспарентності. Вагомим внеском даної інстиутції у зміцнення інформаційної безпеки в регіоні стала програма підтримки України, яка включає тренінги для журналістів із розпізнавання фейків, розвиток медіаграмотності населення та надання експертно-юридичної допомоги українським медіа у виробленні механізмів захисту від тиску через інформаційні атаки.

Серед регіональних організацій найбільш розвинену систему правових інституцій протидії інформаційним загрозам започаткував Європейський Союз.

Останнє було зумовлено як високим рівнем інтеграції держав-членів у спільний інформаційний і цифровий простір, так і масштабом викликів, пов'язаних із дезінформаційними операціями росії на території ЄС.

Ключовим елементом європейської інституційно-правової бази протидії інформаційним загрозам став «Акт про цифрові послуги» (Digital Services Act, DSA), що набув чинності у 2022 р. Він зобов'язує великі онлайн-платформи (Very Large Online Platforms, VLOP) активно протидіяти поширенню незаконного контенту та дезінформації на своїх майданчиках. Його мета – створити максимально безпечний цифровий простір для громадян ЄС, де їхні фундаментальні права захищені, а платформи несуть відповідальність за ті процеси, які відбуваються в співтоваристві. У межах імплементації DSA Європейська комісія у січні 2025 р. затвердила інтеграцію Кодексу практики протидії дезінформації (Code of Practice on Disinformation) [23, с. 8]. Кодекс, що об'єднує понад 30 підписантів, включаючи глобальні технологічні компанії, рекламні асоціації та неурядові організації, вимагає від платформ системного моніторингу дезінформаційних загроз, політики модерації контенту та звітів про заходи протидії інформаційним атакам. Крім того, в квітні 2024 р. було ухвалено «Європейський акт про свободу медіа» (European Media Freedom Act, Regulation 2024/1083), який посилює захист медіа від політичного втручання та закладає загальні рамки для медіапослуг на внутрішньому ринку ЄС.

Інституційну основу для протидії інформаційним загрозам на трансатлантичному рівні формує НАТО. Альянс стикається з інформаційними загрозами з моменту свого заснування у 1949 р., однак після незаконної анексії Росією Криму у 2014 р. ці загрози набули безпрецедентного масштабу, що змусило Альянс значно активізувати діяльність у відповідному напрямі [66, с. 11]. Основним інституційним інструментом протидії інформаційним викликам є «Центр передового досвіду НАТО з питань стратегічних комунікацій» (StratCom COE) у Ризі, який тісно співпрацює з державами-членами Альянсу і партнерами,

з метою усвідомлення інформаційних загроз та ефективного протистояння [66, с. 17]. Одним із базисних інструментів НАТО є проактивна комунікація: Альянс спілкується з авдиторією різними каналами, подаючи фактичну, достовірну, своєчасну та актуальну інформацію [66, с. 5-7]. Цей підхід ґрунтується на позиції, що своєчасне доведення об'єктивних, перевірених фактів блокує можливість противника заповнювати інформаційний вакуум фейками та маніпуляціями. Відзначимо, що після початку повномасштабної війни НАТО суттєво посилило координацію з Україною та країнами-партнерами в інформаційній сфері, зокрема через регулярні консультації з питань обміну даними про дезінформаційні кампанії та надання технічної допомоги у розбудові національних інституцій протидії [66, с. 21].

На рівні національного законодавства країни Європи також демонструють значну варіативність підходів до інституційного та правового забезпечення протидії інформаційним загрозам. Одним із лідерів у сфері правового регулювання дезінформації стала Німеччина, яка з 2018 р. запровадила Мережевий закон, який зобов'язує соціальні мережі, що мають понад 2 мільйони зареєстрованих користувачів видаляти «незаконний» контент протягом 24 годин до 7 днів. У разі систематичного недотримання цих вимог платформам загрожують штрафи до 50 мільйонів євро [57, с. 326]. Закон охоплює 22 категорії кримінальних правопорушень, включно з наклепом, мовою ворожнечі, публічними образами та підбурюванням до насильства. Він також передбачає запровадження прозорих механізмів подання скарг, оприлюднення рішень про видалення контенту та зберігання видаленого контенту щонайменше десять тижнів для надання доказів під час судових розглядів. У 2021 р. закон було доповнено положеннями про апеляційні процедури, обов'язкове інформування федеральної поліції про певні види кримінального контенту, а також розширено наглядові повноваження Федерального офісу юстиції [57, с. 327].

Німецька модель детермінувала жваву дискусію експертів: з одного боку, вона продемонструвала, що законодавче регулювання діяльності цифрових платформ може бути досить ефективним, з іншого, викликала занепокоєння щодо надмірного адміністративного тиску на свободу висловлювань. Як продемонструвала практика, через необхідність уникати величезних штрафів платформи часто видаляють контент, який технічно не є незаконним, але може бути сприйнятий як такий у разі помилкової класифікації, відсоток такого потенційно законного контенту сягає від 87,5 до 99,7% [57, с. 328]. Та не зважаючи на критику, німецька практика стала зразком для подібних законів у багатьох країнах світу та сформувала базис глобальної фрагментації підходів до регулювання онлайн-контенту.

Своєрідний шлях протидії інформаційним викликам обрала й Франція, яка зосередила увагу на захисті виборчих процесів. Після низки дезінформаційних кампаній під час президентських виборів 2017 р. та з огляду на зростання загроз напередодні майбутніх виборчих циклів, французький парламент ухвалив низку законодавчих актів, спрямованих на блокування іноземного втручання. Зокрема було надано судовим органам право в надзвичайному порядку вимагати від онлайн-платформ видаляти або блокувати контент, визнаний дезінформацією в період виборчої кампанії. Одночасно запроваджено нові правила транспарентності політичної реклами в Інтернеті, які зобов’язують платформи розкривати джерела фінансування та механізми таргетингу.

Велика Британія пішла шляхом системного регулювання онлайн-безпеки та прийняла у жовтні 2023 р. Закон про онлайн-безпеку, згідно якого платформи зобов’язані впроваджувати системи і процеси, спрямовані на зниження ризиків використання їхніх сервісів для незаконної діяльності, та оперативно видаляти незаконний контент, коли він з’являється. Імплементацію закону здійснює незалежний регулятор Ofcom, який наділений широкими повноваженнями для оцінки дотримання платформами вимог безпеки. Повноваження регулятора

поширюються на сервіси, зареєстровані за межами країни, якщо вони мають значну кількість британських користувачів, Велика Британія є їхнім цільовим ринком або існує матеріальний ризик заподіяння шкоди таким користувачам.

Британський підхід вирізняється розмежуванням відповідальності залежно від масштабу платформи: вимоги до безпеки є пропорційними таким факторам, як ризик заподіяння шкоди фізичним особам, а також розмір і спроможність кожного провайдера [75, с. 19-21]. Такий підхід дозволяє покладати найсуворіші зобов'язання на глобальних гігантів, водночас не створюючи надмірного адміністративного тягаря для малих і середніх сервісів.

Країни Східної Європи та Балтії, які мають безпосередню межу з росією або розташовані в безпосередній близькості від неї, напрацювали власні підходи до інституційної протидії інформаційним загрозам. Так, Польща, яка систематично стикається з російськими дезінформаційними кампаніями – від інформаційних атак довкола повені 2024 р. до багаторічних спроб посилити напругу в польсько-українських відносинах – створила потужну інституційну систему протидії [31, с. 8]. Державна політика Республіки Польща з протидії дезінформації ґрунтується на системному моніторингу інформаційного простору в координації з союзниками по НАТО та ЄС [31, с. 13]. Польська влада активно використовує механізми звернення до наднаціональних органів, зокрема, з вимогою до Європейської комісії розпочати провадження проти TikTok через масове поширення ШІ контенту, який закликає до виходу Польщі з ЄС. Така практика демонструє, що дедалі більше держав розглядають інструменти колективної дії як невід'ємну частину національної стратегії інформаційної безпеки.

Країни Балтії – Литва, Латвія та Естонія усвідомили критичну важливість інформаційної безпеки ще на початку 2000-х рр., коли вони стали об'єктом системних російських інформаційних впливів. Їхній досвід є особливо цінним, оскільки балтійські країни мають значні російськомовні меншини, що робить їх

особливо вразливими до маніпуляцій російськими державними медіа. Ці держави активно імплементують європейський Акт про цифрові послуги та національні закони про інформаційну безпеку, які суттєво обмежують мовлення російських пропагандистських каналів (зокрема, Sputnik, Russia Today, NTV-Мир тощо) [52, с. 103].

Латвія використовує механізм державного моніторингу інформаційних операцій росії, які мають чітку мету – дискредитувати НАТО та послабити довіру до Північноатлантичного альянсу в країнах-членах. Литва, своєю чергою, систематично викриває російські дезінформаційні кампанії, як-от спроби створити наратив про «сепаратизм у Клайпеді» – ключовому морському порту та місці розташування терміналу скрапленого природного газу. Естонія, Латвія та Литва повністю прийняли «Гаазьке зобов'язання», яке передбачає витрати щонайменше 3,5% ВВП на оборону, з яких 1,5% спрямовується на протидію гібридним загрозам включно з інформаційними [52, с.104].

Особливе місце в світовій практиці займає підхід Фінляндії, яка протягом багатьох років очолює європейські рейтинги з медіаграмотності. Фінська модель є системною та довгостроковою: медіаграмотність інтегрована не у вигляді окремого предмету в освітні програми, а як наскрізна тема, що пронизує викладання всіх дисциплін від початкової школи до вищої освіти [30]. Такий системний підхід формує стійку здатність населення критично оцінювати інформацію та розпізнавати дезінформацію на індивідуальному рівні, знижуючи ефективність будь-яких зовнішніх пропагандистських впливів.

Ефективність фінської моделі підтверджується міжнародними індексами: Фінляндія незмінно визнається країною з найвищим рівнем медіаграмотності в Європі, а навички, необхідні для виявлення онлайн-обманів, включені в національну програму підготовки вчителів [30].

Україна має власний досвід у системі протидії інформаційним викликам, особливо після 2014 р. У грудні 2021 р. Указом Президента України №685/2021

було затверджено «Стратегію інформаційної безпеки України на період до 2025 року», яка визначила концептуальні засади державної політики в цій сфері. Вона ґрунтується на інтеграції України до європейського цифрового простору та спрямована на досягнення трьох ключових цілей: забезпечення всебічного розвитку української культури та утвердження загальнонаціональної ідентичності; підвищення спроможності держави щодо захисту інформаційного суверенітету; розвиток системи інформаційної безпеки як складової сектору безпеки та оборони [49].

Ключовим інституційним елементом української системи протидії інформаційним загрозам став «Центр протидії дезінформації» (ЦПД), створений як робочий орган Ради національної безпеки і оборони України. Він функціонує як постійно діюча структура, що забезпечує системний моніторинг інформаційного простору, виявлення, аналіз і спростування фейків та маніпулятивних наративів, переважно спрямованих на дискредитацію ЗСУ та розкол українського суспільства [55].

Основні функції Центру протидії дезінформації охоплюють такі напрями:

– безперервний моніторинг інформаційного простору для виявлення дезінформаційних загроз;

– аналітика та підготовка рекомендацій для РНБО України щодо реагування на виявлені загрози;

– координація діяльності органів державної влади у сфері стратегічних комунікацій;

– розвінчування фейків та поширення достовірної інформації (так звана «інформаційна контрбатарейна боротьба»);

– взаємодія з міжнародними партнерами – аналогічними центрами в країнах-союзницях для обміну даними та координації дій [55].

Фундаментальні правові засади діяльності медіа в Україні визначені Законом України «Про медіа» від 13 грудня 2022 року. Абсолютна більшість його норм набрали чинності з 1 червня 2024 р. [6, с. 3]. Закон встановлює нові правила для суб'єктів у сфері медіа, посилює вимоги до прозорості власності, захищає журналістів від тиску та встановлює механізми саморегулювання для боротьби з дезінформацією [6, с. 5]. Він також імплементує європейські вимоги щодо захисту національного інформаційного простору від ворожого впливу, зокрема в частині заборони трансляції російських пропагандистських каналів.

Інституційний та правовий базис протидії інформаційним загрозам не може існувати без ефективних механізмів моніторингу та реагування. Світові практики та український досвід демонструють, що використання сучасних технологій, зокрема спеціалізованого програмного забезпечення для моніторингу соціальних мереж та систем ШІ, дозволяє значно підвищити ефективність аналізу великих масивів інформації та виявляти загрози задовго до того, як вони досягнуть широкої аудиторії. Водночас сучасні правові та інституційні механізми протидії інформаційним загрозам стикаються з низкою суттєвих викликів:

– по-перше, зберігається ризик використання інструментів боротьби з дезінформацією для політичної цензури та обмеження свободи слова;

– по-друге, глобальний характер інформаційних потоків потребує посилення міжнародної координації, яка сьогодні часто сповільнюється через розбіжності в підходах різних держав;

– по-третє, стрімкий розвиток технологій штучного інтелекту та глибинних фейків (deepfakes) вимагає розробки адекватних засобів проактивного виявлення та блокування таких впливів, а чинне національне законодавство більшості країн світу до цього не готове.

2.3. Особливості інформаційної агресії проти України та стратегії національної протидії

Російсько-українське інформаційне протистояння, що триває вже понад десятиліття є особливим збройним конфліктом нового типу. Його унікальність полягає в тому, що інформаційна складова не просто супроводжує бойові дії, а є самостійним виміром протиборства, здатним визначати перебіг і результат військово-політичного зіткнення ще до застосування традиційних засобів ураження.

Більшість вітчизняних дослідників підкреслюють, що інформаційна агресія російської федерації проти України пройшла кілька якісно різних етапів. Перший етап, що охоплює 2014-2021 рр., характеризувався використанням переважно традиційних засобів масової інформації - державних телеканалів (Russia Today, «россия 24», «Первый канал»), друкованих видань та інформаційних агентств, контрольованих кремлем. У цей період сформувалися основні наративи, які стали фундаментом російської пропаганди: «громадянська війна» на Донбасі, «київська хунта», «руська весна», «переслідування російськомовних» [34, с. 118]. Ці наративи активно поширювалися через традиційні медіа, створюючи в російському суспільстві спотворену картину подій та легітимізуючи передумови для подальшої відкритої агресії.

Другий, принциповий переломний момент, настає з початком повномасштабного вторгнення у 2022 р. Відтоді дослідники фіксують кардинальну трансформацію як інструментарію, так і масштабів російської інформаційної війни. Як слушно зауважує А. Руднєва зі співавторами, вже у 2022 р. інформаційний складник російської агресії набув безпрецедентних масштабів у форматі потужного арсеналу маніпулятивних, пропагандистських методів та прийомів, кібератак, дезінформації [46, с. 186]. Серед основних наративів рф домінували: перекладання провини за розв’язування агресії на США та НАТО,

наратив недієвості санкцій, підрив іміджу України через поширення щоденних фейків, маніпулювання «ядерним питанням», а також розпалювання ворожнечі між владою та населенням через тему «зради» [46, с.189].

Згодом, до 2025-2026 рр., інформаційна війна не послаблюється, а навпаки стає більш технологічно складною. Російські інформаційно-психологічні операції (ІПСО) переходять на якісно новий рівень, де використовуються не окремі фейки, а цілісні системи психологічного впливу, що ґрунтується на експлуатації базових психологічних механізмів – страху, тривоги, втоми й безпорадності [47, с. 31]. Змін зазнає і перелік наративів: домінантними стають «мир будь-якою ціною», необхідність заморожування конфлікту, загроза застосування ядерної зброї, маніпуляції навколо Запорізької АЕС та цілісна системна делегітимація української державної суб'єктності, здатності українців самостійно керувати своєю країною [47, с. 32]. Це є ознакою того, що сучасна російська інформаційна війна стала більш стратегічною, системною і складною, яка має на меті не тимчасову дезорієнтацію, а довготривалу зміну суспільної свідомості українців.

Як слушно зауважують вітчизняні дослідники, дезінформаційні кампанії, маніпулятивні наративи та тактика психологічної війни систематично використовувалися росією для підриву соціальної довіри, розпалювання страху та фрагментації українського суспільства. При цьому методи поширення дезінформації охоплюють величезний спектр: від традиційного телемовлення до глобальних цифрових платформ. Науковці доходять висновку, що мета російських інформаційних атак – викликати зневіру у власних силах та соціальну дестабілізацію населення, що робить протидію дезінформації не просто комунікаційним завданням, а елементом національної безпеки найвищого рівня [25, с. 373].

Окремо варто наголосити на канальній складовій. Якщо на початку агресії домінували телебачення та контрольовані державою медіа в росії та на тимчасово

окупованих територіях, то після 2022 р. головна роль перейшла до платформ соціальних мереж та месенджерів (Telegram, TikTok, Instagram, Twitter), блогів, дезінформаційних мереж та технологій штучного інтелекту [34, с. 120]. З їхньою допомогою російські пропагандисти проводять цілеспрямовані інформаційно-психологічні операції з безпрецедентною точністю сегментування аудиторії. Саме цей перехід робить сучасну інформаційну війну такою небезпечною, адже алгоритми ШІ можуть створювати тисячі унікальних фейкових меседжів, адаптованих до різних соціальних груп, автоматизувати процеси поширення дезінформації та моніторити вразливість аудиторії в реальному часі.

Цільові аудиторії інформаційної агресії також чітко диференційовані: внутрішньо-українська аудиторія (з метою посіяти паніку, розколоти суспільство та знецінити опір), російська внутрішня аудиторія (для консолідації суспільства навколо війни та легітимізації агресії), міжнародна та західна аудиторія (для дискредитації України, виснаження волі до підтримки та просування наративу про воєнне виснаження). Цей багатовимірний підхід вимагає від України структурованої системи стратегічних комунікацій.

Основним документом, який визначає державну політику у сфері інформаційної безпеки, стала Стратегія інформаційної безпеки України, схвалена Указом Президента №685/2021 28 грудня 2021 року на період до 2025 року. Як зазначають аналітики, найбільш критичними загрозами, на які вказує цей документ - збільшення кількості дезінформаційних кампаній, інформаційна політика російської федерації та низький рівень медіаграмотності громадян у поєднанні зі стрімким поширенням цифрових технологій [49].

Всього через два місяці після її ухвалення почалося повномасштабне вторгнення, яке перевірило на міцність правову та інституційну систему. інформаційна безпека стала однією з ключових складових національної безпеки, а інформаційний складник став чи не найактивнішим полем битви поряд з традиційними бойовими діями [37, с. 320].

На практиці протидія російській інформаційній агресії ґрунтується на діяльності цілої низки центральних органів виконавчої влади та спеціалізованих інституцій. Ключову координуючу роль у системі відіграє Рада національної безпеки і оборони України та її робочий орган – «Центр протидії дезінформації (ЦПД)». Україна розпочала повноцінну боротьбу з російськими наративами лише з 2014 р., а до цього тривалий час було відсутнє розуміння необхідності системних контрзаходів [21, с. 258-259]. Спочатку сили були нерівними, адже українці мали дуже низький рівень довіри до власних ТБ-каналів через їхню олігархічну природу, тоді як росіяни споживали пропаганду централізовано. Ключовим завданням ЦПД, стало саме усунення цього дисбалансу через системний моніторинг інформаційного простору, виявлення, аналіз та спростування фейків і маніпулятивних наративів, координацію діяльності органів державної влади у сфері стратегічних комунікацій [55].

Ще однією установою у цьому напрямку є «Центр стратегічних комунікацій та інформаційної безпеки» (StratCom Ukraine), який працює у трьох основних напрямках: стратегічні комунікації, медіа- та кризові комунікації. Підкреслимо, що крім державних інституцій, величезну роль у ранньому виявленні фейків та інформуванні суспільства відіграють й громадські організації та волонтерські спільноти. Проєкти «StopFake», «VoxCheck» та «По той бік новин», які виникли ще на початку російської агресії у 2014 р., стали своєрідною «швидкою допомогою» у верифікації даних. Як засвідчує аналітичний звіт ГО «Український інститут медіа та комунікацій» в умовах повномасштабної війни ефективність протидії російській дезінформації значною мірою залежить від злагодженості роботи державних інституцій та громадянського суспільства [8, с. 7].

Складність сучасної інформаційної війни вимагає комплексного правового та практичного реагування. Важливу роль у системі протидії відіграють кримінально-правові механізми, які активізувалися з початком війни. Кримінальний кодекс України було доповнено статтями про заборону пропаганди

російських наративів (ст. 436-2 – виправдовування збройної агресії рф) та заборону комуністичної символіки (ст. 436-1). Закон України «Про медіа» та рішення РНБО дозволяють блокувати проросійські сайти за спрощеною процедурою. Ці правові інструменти є критично необхідними в умовах воєнного стану, коли дезінформація є зброєю, що вбиває.

Не зважаючи на вагомі зусилля у напрямку протидії інформаційним загрозам, на сьогодні існує і низка критичних проблемних питань: високий рівень технологічної складності сучасних атак, відсутність сталої міжвідомчої координації між державними структурами (особливо на початковому етапі), фрагментарність та неузгодженість законодавчого регулювання у сфері інформаційної безпеки, а також зовнішній контроль над глобальними цифровими платформами (X, TikTok, Google), що суттєво обмежує можливості оперативного реагування на загрози [33, с. 354].

Отже, інформаційна безпека України у 2025-2026 рр. пройшла доволі стрімку інституційну, правову та технологічну еволюцію. Наша держава трансформувала свою систему від практичної відсутності протидії на початку 2014 р. до однієї з найбільш сучасних структур стратегічних комунікацій серед країн-кандидатів у ЄС, що активно вивчається партнерами по НАТО.

Попри значний прогрес, перед системою стоїть низка невирішених викликів: необхідність перегляду Стратегії інформаційної безпеки з огляду на новітні загрози, подолання міжвідомчої неузгодженості, посилення співпраці з Big Tech для видалення ворожого контенту, кримінальне переслідування колаборантів за поширення фейків на окупованих територіях, а також подальший розвиток національної системи медіаграмотності для зміцнення соціальної стійкості до інформаційних маніпуляцій в довгостроковій перспективі.

Український досвід є унікальним полігоном для світової теорії інформаційних війн та гібридних конфліктів. Ефективна протидія агресії

сформувала школу стратегічних комунікацій, яка вже зараз активно впроваджується країнами НАТО для посилення власної резильєнтності.

Висновки до розділу 2

Аналіз сучасних інформаційних війн демонструє, що їх базовою характеристикою виступає циклічна природа інформаційно-психологічних операцій, які розгортаються за послідовними етапами: інформаційний привід, активне поширення в медійному просторі, фаза максимального резонансу та затухання хвилі після досягнення мети.

У Європейському Союзі сформовано найбільш розвинену наднаціональну систему протидії дезінформації, ключовими елементами якої є Акт про цифрові послуги, Кодекс практики протидії дезінформації та Європейський акт про свободу медіа.

Вітчизняна система інформаційної безпеки, закріплена Стратегією інформаційної безпеки та Законом «Про медіа», пройшла шлях від спонтанного волонтерського супротиву до структурованої моделі з ключовими інституціями – Центром протидії дезінформації при РНБО, StratCom Ukraine та Департаментом стратегічних комунікацій ЗСУ.

Системне поєднання аналізу загроз, фазового планування, інституційної спроможності та міжнародної взаємодії є необхідною умовою захисту інформаційного простору та збереження суспільної довіри в умовах збройного конфлікту.

ВИСНОВКИ

Проведене дослідження дозволяє сформулювати низку висновків, що фіксують особливості засобів і механізмів ведення інформаційних війн в умовах сучасного геополітичного протистояння.

По-перше, аналіз теоретико-методологічних засад дослідження зафіксував, що цей феномен є складним, багатовимірним явищем, яке не може бути описане в межах одного наукового підходу. Еволюція дефініції «інформаційна війна» демонструє поступовий перехід від розуміння її як допоміжного засобу підтримки традиційних військових дій до визнання самостійним, а в окремих конфліктах, і визначальним фактором сучасного протистояння. Інформаційну війну найчастіше розглядають як відкритий або прихований цілеспрямований інформаційний вплив, що здійснюється однією із сторін щодо іншої, із використанням системи методів і засобів впливу на масову свідомість, а також на інформаційні ресурси та системи. Саме таке визначення дозволяє охопити весь спектр сучасних форм інформаційного протиборства: від класичної пропаганди до когнітивних і кібернетичних операцій.

Систематизація засобів ведення інформаційних війн дозволила виокремити три групи: традиційні, цифрові та когнітивні. Максимальної ефективності інформаційні кампанії досягають за умови синергетичного поєднання цих трьох груп у межах єдиної стратегічної операції.

Дослідження структурно-функціональних характеристик механізмів реалізації інформаційного впливу продемонструвало, що інформаційна війна розгортається за чіткими циклами, фазами та операційними моделями. Теоретичним базисом для розуміння процесів прийняття рішень в умовах інформаційного протиборства слугує цикл OODA (Observation–Orientation–Decision–Action), адаптований для планування інформаційно-психологічних

операцій: перевага належить тій стороні, яка проходить цей цикл швидше за противника.

На фазовому рівні на прикладі сучасного російсько-українського протистояння виявлено чотири якісно відмінні фази: латентну (підготовчу), фазу відкритої інформаційної агресії та дезорієнтації, інформаційного супроводу бойових дій та гіпотетичну фазу постконфліктного закріплення результатів у масовій свідомості. Та зафіксовано, що на операційному рівні найчастіше домінують три моделі: мережеві атаки через фіктивні акаунти та бот-мережі, залучення добровільних або проплачених агентів впливу (тролів) та техніки блокування небажаного контенту. Усі вони постійно модифікуються з урахуванням нових технологічних можливостей, передусім систем ШІ, здатних генерувати тисячі унікальних фейкових повідомлень, адаптованих до різних соціальних груп, в режимі реального часу.

Аналіз інституційних та правових механізмів протидії інформаційним загрозам у світовій практиці зафіксував значну варіативність підходів залежно від правової культури, геополітичного становища та рівня цифрового розвитку держав. На наднаціональному рівні найбільш розвинену систему сформував Європейський Союз. Трансатлантичний вимір забезпечується через Центр передового досвіду НАТО зі стратегічних комунікацій (StratCom COE) у Ризі, який координує діяльність держав-членів і партнерів у сфері протидії гібридним інформаційним загрозам. На національному рівні найбільш показовими є: німецька модель законодавчого регулювання цифрових платформ, британський підхід до диференційованої відповідальності залежно від масштабу сервісу, французьке законодавство про захист виборчих процесів від дезінформації, а також балтійські практики системного обмеження російського пропагандистського мовлення. Спільною проблемою для всіх правових систем залишається ризик використання інструментів протидії дезінформації для

політичної цензури, а також технологічне відставання нормативної бази від темпів розвитку ШІ та генеративних медіа.

Дослідження специфіки інформаційної агресії проти України з боку росії дозволило встановити, що вона пройшла кілька якісно відмінних етапів, кожен із яких характеризувався розширенням інструментарію та підвищенням технологічної складності операцій. Характеристика стратегій національної протидії засвідчила, що наша держава здійснила стрімку інституційну, правову та технологічну еволюцію у сфері інформаційної безпеки - від практичної відсутності системної протидії на початку 2014 р. до однієї з найбільш сучасних структур стратегічних комунікацій серед країн-кандидатів у ЄС. Ключовими елементами цієї системи є: Центр протидії дезінформації при РНБО, Центр стратегічних комунікацій та інформаційної безпеки (StratCom Ukraine), Департамент стратегічних комунікацій ЗСУ, а також потужний сектор громадянського суспільства, представлений такими організаціями, як «StopFake», «VoxCheck» та «По той бік новин». Правовий базис забезпечується Стратегією інформаційної безпеки України (Указ Президента №685/2021) та Законом «Про медіа» (2022 р.).

Нами підкреслено, що унікальністю українського досвіду є інтеграція стратегічних комунікацій у військове планування на рівні оперативних штабів, що перетворило аналіз циклів і фаз інформаційного впливу з академічного інструменту на бойовий. Цей досвід уже активно вивчається та впроваджується країнами НАТО для посилення власної резильєнтності.

Отже, можемо констатувати, що інформаційні війни в умовах XXI ст. набули якісно нових характеристик, які принципово відрізняють їх від класичних форм пропаганди. Вони ведуться безперервно, не обмежуючись періодом відкритого збройного протистояння, а нерідко передуючи йому. Вони є асиметричними: так порівняно обмежені ресурси за умови точного таргетування здатні завдати значно більшої шкоди, ніж наслідки конвенційного збройного

нападу. Їм властива технологічна інтенсивність, у зв’язку із впровадження ШІ, генеративних медіа та автоматизованих систем поширення контенту кардинально змінює баланс між атакою та захистом. Насамкінець, їх кінцевою метою є не тимчасова дезорієнтація, а довготривала трансформація системи цінностей, моделей сприйняття реальності та механізмів прийняття рішень на рівні масової свідомості.

Перспективи подальших досліджень можуть бути пов’язані з вивченням методів нейтралізації когнітивних атак в умовах масового поширення генеративного ШІ, розробкою ефективних моделей міжнародно-правового регулювання цифрових платформ в умовах збройних конфліктів, а також з порівняльним аналізом ефективності різних систем стратегічних комунікацій серед держав, які зіткнулися з масштабними інформаційними агресіями.