МІНІСТЕРСТВО ОСВІТИ І НАУКИ УКРАЇНИ
КИЇВСЬКИЙ НАЦІОНАЛЬНИЙ УНІВЕРСИТЕТ ТЕХНОЛОГІЙ ТА ДИЗАЙНУ

Факультет економіки та управління

Кафедра приватного та публічного права

На правах рукопису

Кваліфікаційна робота

на тему

ІНФОРМАЦІЙНА ПОЛІТИКА УКРАЇНИ В УМОВАХ РОСІЙСЬКО-УКРАЇНСЬКОЇ ВІЙНИ

Виконала: студентка групи БЗППК — 22

спеціальності 052 «Політологія»

Панченко К. К.

Науковий керівник: Кипич І. В.,

к. юридичних наук, доцент

Київ 2025

КИЇВСЬКИЙ НАЦІОНАЛЬНИЙ УНІВЕРСИТЕТ ТЕХНОЛОГІЙ ТА ДИЗАЙНУ

Факультет економіки та управління

Кафедра приватного та публічного права

Спеціальність 052 «Політологія»

ЗАТВЕРДЖУЮ

Завідувач кафедри приватного та публічного права_____проф. Юрій Оніщик

«_____»

_____20_____року

З А В Д А Н Н Я

НА КВАЛІФІКАЦІЙНУ РОБОТУ СТУДЕНТА

Панченко Катерини Костянтинівни

1. Тема кваліфікаційної роботи Інформаційна політика України в умовах російсько-української війни

Науковий керівник роботи Кипич Інга Валеріївна к. юридичних наук, доцент

затверджені наказом КНУТД від « » 2025 року №___

2. Вихідні дані до кваліфікаційної роботи Законодавчо – нормативні акти України, статистичні щорічники, навчальні посібники, підручники, монографії, фахові наукові видання, словники, тези міжнародних наукових конференцій

тощо._____

_____

4. Зміст кваліфікаційної роботи (перелік питань, які потрібно розробити) Розділ 1. Теоретико-методологічні засади дослідження інформаційної політики. Розділ 2. Інформаційна політика України в умовах російсько-української війни. Розділ 3. Ефективність інформаційної протидії російській агресії.

5. Дата видачі завдання 15 вересня 2025

АНОТАЦІЯ

Панченко К. К. Інформаційна політика України в умовах російсько-української війни. Рукопис. Кваліфікаційна робота на здобуття освітнього ступеня бакалавра за спеціальністю 052 «Політологія», КНУТД, 2025.

Робота присвячена комплексному дослідженню інформаційної політики України в умовах російсько-української війни: її теоретичних засад, інституційної структури, нормативно-правової бази та практичних результатів. У роботі визначено поняття і сутність інформаційної політики держави, розкрито концептуальні підходи до вивчення інформаційної безпеки та зарубіжний досвід формування інформаційної політики в умовах збройних конфліктів. Досліджено становлення і розвиток інформаційної політики України у 2014–2022 рр., вивчено нормативно-правову базу в умовах воєнного стану, проаналізовано діяльність державних інститутів у сфері інформаційної безпеки. Значна увага приділяється аналізу стратегії протидії дезінформації та пропаганді, ролі медіа і громадянського суспільства в інформаційній обороні, а також міжнародній складовій інформаційної політики України під час війни. На основі проведеного аналізу запропоновано рекомендації щодо вдосконалення державної інформаційної політики України.

Ключові слова: інформаційна політика, інформаційна безпека, військовий стан, дезінформація, пропаганда, стратегічні комунікації, Україна.

SUMMARY

Panchenko K. Information Policy of Ukraine under the Conditions of the Russian-Ukrainian War. Manuscript. Bachelor’s thesis to obtain the educational level of bachelor in the specialty 052 Political Science, KNUTD, 2025.

The thesis is dedicated to a comprehensive study of the information policy of Ukraine under the conditions of the Russian-Ukrainian war: its theoretical foundations, institutional structure, regulatory framework, and practical outcomes. The study defines the concept and essence of state information policy, examines conceptual approaches to information security, and analyzes foreign experience in forming information policy under armed conflict conditions. The formation and development of Ukraine's information policy in 2014–2022 is investigated, the regulatory framework under martial law is studied, and the activities of state institutions in the field of information security are analyzed. Considerable attention is given to the analysis of the strategy for countering disinformation and propaganda, the role of media and civil society in Ukraine's information defense, and the international dimension of Ukraine's information policy during the war. Based on the conducted analysis, recommendations for improving Ukraine's state information policy are proposed.

Keywords: information policy, information security, martial law, disinformation, propaganda, strategic communications, Ukraine.

ЗМІСТ

ВСТУП

Актуальність теми. В умовах повномасштабного вторгнення Російської Федерації на територію України, що розпочалося 24 лютого 2022 року, інформаційна сфера набула стратегічного значення як один із ключових фронтів протистояння [1, с. 3]. Сучасні збройні конфлікти дедалі більше переміщуються у площину інформаційного простору, де боротьба за суспільну свідомість, формування наративів і протидія дезінформації стають не менш важливими, ніж безпосередні бойові дії [2, с. 17]. Україна опинилася перед безпрецедентним викликом: одночасно вести військовий захист, формувати ефективну державну комунікацію всередині країни та просувати власний порядок денний на міжнародній арені.

Інформаційна політика України в умовах війни охоплює широкий спектр заходів: від законодавчого регулювання медіапростору і діяльності державних інституцій у сфері стратегічних комунікацій до контрпропагандистських операцій і дипломатичних зусиль із формування міжнародної підтримки [3, с. 45]. Осмислення цього досвіду є надзвичайно важливим як для розуміння сучасних механізмів захисту інформаційного суверенітету, так і для вироблення рекомендацій щодо вдосконалення відповідної державної політики [4].

Дослідження інформаційної політики України в умовах збройного конфлікту є актуальним у декількох вимірах. По-перше, воно дозволяє вивчити, як держава адаптує інституційну структуру та правові механізми в екстремальних умовах воєнного часу. По-друге, аналіз ефективності протидії інформаційним операціям противника надає цінний матеріал для теорії та практики інформаційної безпеки [5, с. 22]. По-третє, міжнародний вимір українського досвіду – формування коаліції підтримки та протидія дезінформації на глобальному рівні – є унікальним кейсом для сучасної політичної науки [6].

Ступінь наукової розробленості проблеми. Питання інформаційної політики та інформаційної безпеки перебувають у полі зору вітчизняних і зарубіжних дослідників. Теоретичні засади інформаційної політики закладені у працях Е. Тоффлера, М. Кастельса, Дж. Ная (концепція «м'якої сили»), Ф. Уебстера. Серед українських дослідників суттєвий внесок у розробку проблематики зробили В. Горовенко, Д. Дубов, В. Пилипчук, А. Баровська, О. Литвиненко. Питанням протидії гібридним загрозам і дезінформації присвячені праці Т. Снайдера, П. Померанцева, Б. Брантлі. Водночас дослідження інформаційної політики України в умовах повномасштабної війни 2022–2024 рр. залишається відносно новим і слабко систематизованим напрямом, що зумовлює наукову новизну та практичну значущість цієї роботи.

Об'єктом дослідження є інформаційна політика України як система державних заходів, інститутів та механізмів регулювання інформаційного простору.

Предметом дослідження є трансформація та функціонування інформаційної політики України в умовах російсько-української війни (2022–2024 рр.).

Мета дослідження полягає у комплексному аналізі інформаційної політики України в умовах збройного конфлікту: її теоретичних засад, інституційної структури, нормативно-правової бази та практичних результатів.

Для досягнення мети поставлено такі завдання:

– розкрити поняття та сутність інформаційної політики держави, визначити її структурні складові;

– охарактеризувати концептуальні підходи до вивчення інформаційної безпеки в контексті сучасних збройних конфліктів;

– проаналізувати зарубіжний досвід формування інформаційної політики в умовах збройних конфліктів;

– дослідити становлення та розвиток інформаційної політики України у 2014–2022 рр.;

– вивчити нормативно-правову базу інформаційної політики України в умовах воєнного стану;

– проаналізувати діяльність державних інститутів у сфері інформаційної безпеки;

– визначити ефективність стратегії протидії дезінформації та пропаганді;

– оцінити роль медіа та громадянського суспільства в інформаційній обороні України;

– розглянути міжнародну складову інформаційної політики України під час війни.

Методи дослідження. У роботі застосовано комплекс загальнонаукових та спеціальних методів політологічного дослідження. Системний підхід використано для аналізу інформаційної політики як цілісної системи взаємозалежних елементів [19, с. 12]. Інституційний аналіз дозволив вивчити державні органи у сфері інформаційної безпеки, їх повноваження та взаємодію. Порівняльний метод застосовано при аналізі зарубіжного досвіду [20]. Контент-аналіз використано для дослідження нормативно-правових актів. Метод case-study став основою для аналізу конкретних інформаційних операцій.

Хронологічні рамки дослідження охоплюють переважно 2022–2024 рр. – період повномасштабного збройного конфлікту, однак для розуміння передумов розглядаються також події 2014–2021 рр.

Практичне значення роботи полягає у можливості використання її результатів для вдосконалення державної інформаційної політики, у навчальному процесі при викладанні дисциплін «Політологія», «Теорія міжнародних відносин», «Інформаційна безпека», а також у діяльності державних органів та неурядових організацій, що займаються питаннями медіаграмотності та протидії дезінформації [21].

Структура роботи. Кваліфікаційна робота складається зі вступу, трьох розділів, висновків, списку використаних джерел та додатків. Загальний обсяг роботи становить 67 сторінок основного тексту. Список використаних джерел нараховує 65 найменувань.

РОЗДІЛ 1

ТЕОРЕТИКО-МЕТОДОЛОГІЧНІ ЗАСАДИ ДОСЛІДЖЕННЯ ІНФОРМАЦІЙНОЇ ПОЛІТИКИ

1.1. Поняття та сутність інформаційної політики держави

Інформаційна політика держави є однією з ключових складових сучасного державного управління, що набуває дедалі більшого значення в умовах глобальної інформатизації суспільства [22, с. 5]. Формування та реалізація ефективної інформаційної політики безпосередньо впливає на національну безпеку, суспільну консолідацію, економічний розвиток і міжнародний авторитет держави. Розуміння змісту цього поняття вимагає звернення до широкого спектру підходів, що сформувалися в політичній науці, теорії комунікацій та праві.

У найзагальнішому сенсі інформаційна політика держави – це цілеспрямована система принципів, цілей, засобів і заходів державних органів щодо регулювання інформаційного простору, забезпечення права громадян на інформацію, захисту національних інтересів в інформаційній сфері та формування суспільної комунікації [23, с. 34]. Проте такий широкий підхід вимагає деталізації та структурування.

В академічній літературі склалося кілька підходів до визначення інформаційної політики. Перший – інституційний – акцентує на системі державних органів, механізмів і інструментів управління інформаційним простором [24]. З цієї точки зору, інформаційна політика є сукупністю правових, адміністративних та організаційних заходів, що здійснюються органами державної влади. Другий підхід – комунікативний – розглядає інформаційну політику як управління державними інформаційними

потоками, формування офіційного дискурсу та публічних наративів . Третій – безпековий – фокусується на захисті інформаційного суверенітету, протидії зовнішнім інформаційним загрозам і збереженні інформаційного простору як стратегічного ресурсу держави [25].

Американський дослідник Дж. Най у концепції «м'якої сили» (soft power) показав, що здатність держави формувати привабливий образ, поширювати власні наративи та цінності є не менш важливим інструментом зовнішньої політики, ніж «тверда сила» – військова або економічна міць . Інформаційна політика в цьому контексті виступає інструментом проекції м'якої сили. Американські дослідники Дж. Найхем і Д. Арква запропонували поняття «кібербезпекова політика» як підвид інформаційної, що стосується захисту цифрової інфраструктури і є складовою більш широкої системи інформаційного управління [26].

У вітчизняній науковій традиції розмежовують кілька рівнів інформаційної політики . На макрорівні вона охоплює стратегічне цілевизначення у сфері інформаційних відносин, формування відповідного законодавства та системи регуляторних органів. На мезорівні – реалізацію галузевих програм і концепцій (у медіасфері, сфері кібербезпеки, державних комунікацій). На мікрорівні – конкретні заходи і практики урядових структур, що безпосередньо впливають на інформаційний простір .

Важливо розрізняти також внутрішній і зовнішній виміри інформаційної політики [27]. Внутрішня інформаційна політика спрямована на регулювання національного медіапростору, забезпечення свободи слова у поєднанні з відповідальністю медіа, протидію дезінформації та підвищення медіаграмотності населення. Зовнішня інформаційна політика охоплює дипломатичні комунікації, публічну дипломатію, поширення позитивного образу держави та захист її позицій в міжнародному інформаційному просторі [28, с. 56].

Структурними елементами інформаційної політики є: суб'єкти (органи державної влади, уповноважені регулятори, державні медіа); об'єкти

(інформаційний простір, медіасистема, аудиторія, інформаційна інфраструктура); цілі та принципи (відкритість, достовірність, безпека, доступність); інструменти (правове регулювання, фінансова підтримка, технічні заходи, комунікативні кампанії); механізми контролю та оцінки ефективності [29, с. 102].

Е. Тоффлер у фундаментальній праці «Третя хвиля» передбачив, що інформація стане визначальним ресурсом постіндустріального суспільства, а держави, що не опанують механізми управління інформаційними потоками, неминуче опиняться на периферії глобального розвитку . М. Кастельс, розвиваючи цю ідею, концептуалізував поняття «мережевого суспільства», в якому влада все більше визначається не контролем над матеріальними ресурсами, а здатністю формувати і поширювати смисли . Обидві концепції є фундаментальними для розуміння того, чому інформаційна політика набула такого стратегічного значення в сучасних збройних конфліктах.

Ф. Уебстер, узагальнюючи різні теорії інформаційного суспільства, звертає увагу на суперечність між демократичним потенціалом нових технологій і ризиками їх використання для маніпулювання суспільством . Ця суперечність є надзвичайно актуальною для розуміння специфіки інформаційної боротьби в умовах сучасних конфліктів: ті самі технології соціальних мереж, що сприяли громадянській мобілізації під час Революції Гідності, стали й зброєю масштабних дезінформаційних операцій з боку агресора.

Інформаційна політика нерозривно пов'язана з поняттям інформаційного суверенітету – здатністю держави самостійно визначати принципи функціонування власного інформаційного простору без зовнішнього втручання [30]. В умовах глобальної мережі Інтернет та транснаціональних медіа це поняття набуває особливої актуальності, оскільки кордони інформаційного простору стають значно менш чіткими, ніж у традиційному розумінні [8, с. 177].

Ще одним ключовим поняттям є інформаційна безпека – стан захищеності інформаційного простору держави, що забезпечує реалізацію конституційних прав і свобод громадян в інформаційній сфері, сталий розвиток інформаційного суспільства, захист національних інтересів в умовах зовнішніх і внутрішніх загроз [31, с. 7]. Відповідно до Доктрини інформаційної безпеки України 2017 р., основними загрозами визначено: ведення Росією інформаційно-психологічної війни, цілеспрямоване поширення дезінформації та пропаганди, кіберагресію проти критичної інфраструктури [32].

В умовах збройних конфліктів інформаційна політика трансформується: відбувається посилення централізованого контролю над інформаційним простором, запровадження обмежень на поширення певних видів інформації заради безпеки, активізація пропагандистської складової [33, с. 214]. Разом з тим демократичні держави намагаються зберегти баланс між вимогами безпеки та свободою слова. Досвід різних країн свідчить, що найбільш ефективною є модель, за якої держава не монополізує інформаційний простір, але активно формує наратив і протидіє ворожій дезінформації [34].

Окремої уваги заслуговує питання вимірювання ефективності інформаційної політики. Д. В. Дубов та М. А. Ожеван виділяють кількісні та якісні індикатори ефективності: перші охоплюють показники охоплення аудиторії, частку вітчизняного контенту в медіапросторі, рівень медіаграмотності населення; другі – ступінь суспільної довіри до державних інститутів, рівень інформаційної стійкості суспільства перед обличчям зовнішніх маніпуляцій, здатність держави формувати і утримувати домінантний наратив у кризових ситуаціях . Саме ці критерії є релевантними для оцінки ефективності інформаційної політики України в умовах повномасштабного збройного конфлікту.

Важливим аспектом теоретичного осмислення інформаційної політики є питання про її суб'єктний склад. А. В. Баровська звертає увагу на те, що в

сучасних умовах суб'єктами інформаційної політики є не лише держава, але й медіаорганізації, громадянське суспільство, міжнародні структури та навіть окремі впливові особи . Це ускладнює традиційне бюрократичне уявлення про інформаційну політику як виключну прерогативу держави та потребує переосмислення механізмів координації між різними акторами. В умовах воєнного стану роль недержавних суб'єктів – медіа, НДО, волонтерських організацій – суттєво зростає, що потребує інституційного оформлення механізмів їхньої взаємодії з державою.

Отже, інформаційна політика держави є багатовимірним феноменом, що охоплює правовий, інституційний, комунікативний і безпековий аспекти . В умовах сучасних конфліктів вона набуває особливої ваги як інструмент захисту національного суверенітету та засіб мобілізації суспільної підтримки. Теоретичні здобутки Е. Тоффлера, М. Кастельса, Дж. Ная, Ф. Уебстера та вітчизняних науковців формують міцний концептуальний фундамент для аналізу конкретних практик інформаційної політики України.

1.2. Концептуальні підходи до вивчення інформаційної безпеки

Теоретичне осмислення феномену інформаційної безпеки відбувається на перетині кількох дисциплін: політології, теорії міжнародних відносин, кібербезпеки та медіадосліджень [35, с. 9]. Формування концептуального апарату цієї сфери пов'язане з фундаментальними змінами у природі сучасних конфліктів, де інформаційний вимір набуває стратегічного значення.

Одним з найбільш впливових концептуальних підходів є теорія гібридної війни (hybrid warfare), яка описує поєднання традиційних і нетрадиційних методів ведення конфлікту, в тому числі інформаційних операцій, кібератак, економічного тиску та дипломатичних маніпуляцій [36, с. 33]. Термін набув широкого поширення після агресії Росії проти України в

2014 р. Згідно з цією концепцією, інформаційна складова гібридної війни є одним з ключових інструментів противника: вона спрямована на деморалізацію суспільства, підрив довіри до влади та зовнішньополітичну ізоляцію держави-жертви [37, с. 58].

Теоретики стратегічних комунікацій (strategic communications) розглядають інформаційну безпеку крізь призму управління наративами [38]. Згідно з цим підходом, наратив – це зв'язний каузальний опис подій, що формує їхнє сприйняття. У конфліктах наративи стають «зброєю», а держава, яка здатна утримувати контроль над домінантним наративом, отримує стратегічну перевагу [39, с. 121]. Проблема полягає в тому, що авторитарні режими, не обтяжені демократичними обмеженнями, мають більш широкі можливості для маніпулювання інформацією порівняно з відкритими суспільствами .

Конструктивістський підхід у теорії міжнародних відносин акцентує на тому, що реальність у значній мірі є соціально конструйованою [40]. Відповідно, держави конкурують не лише за матеріальні ресурси, але й за інтерпретацію дійсності, формуючи ідентичності, норми та цінності. Інформаційна безпека в цьому контексті означає здатність держави захистити власну версію реальності від деструктивних зовнішніх впливів. Особливого значення набуває захист національної ідентичності та збереження консолідованої суспільної пам'яті [16, с. 76].

У межах Копенгагенської школи (Б. Бузан, О. Вейвер) розвинуто концепцію «сек'юритизації» – процесу, за яким та чи інша проблема інтерпретується як загроза безпеці та виноситься за межі звичайного політичного дискурсу, що виправдовує застосування надзвичайних заходів . Сек'юритизація інформаційної сфери означає визнання інформаційних загроз рівнозначними традиційним військовим, що обґрунтовує право держави вдаватися до виняткових заходів задля захисту суспільства [42].

Медіадослідник П. Померанцев запропонував поняття «постправди» (post-truth) – інформаційного середовища, в якому об'єктивні факти мають

менший вплив на формування суспільної думки, ніж апеляції до емоцій та особистих переконань . Це середовище є надзвичайно сприятливим для пропаганди та дезінформаційних операцій. Дослідник описав систему кремлівської пропаганди як таку, що свідомо прагне зруйнувати саму ідею існування об'єктивної істини, паралізуючи здатність суспільства до раціонального дискурсу . У контексті російсько-українського конфлікту ця теза набуває особливої пояснювальної сили: масований інформаційний вплив Росії спрямований не лише на формування конкретних переконань, але й на підрив самої можливості раціонального осмислення дійсності.

Щодо методологічних інструментів аналізу інформаційних загроз, у науковій літературі широко застосовується дискурс-аналіз – метод дослідження мовних практик, за допомогою яких конструюються смисли, легітимізується влада та підтримуються або підриваються певні соціальні практики [43, с. 14]. Дискурс-аналіз дозволяє виявити приховані ідеологічні механізми у пропагандистських текстах, встановити ключові наративи та стратегії переконання. Зокрема, аналіз дискурсу російських державних медіа щодо України демонструє системне застосування дегуманізуючих метафор, фальсифікації історичних фактів та маніпуляцій з контекстом – прийомів, ідентифікованих ще Г. Лассуеллом у класичних дослідженнях пропаганди [35, с. 18].

Теорія «м'якої сили» Дж. Ная є важливим концептуальним інструментом розуміння позитивного виміру інформаційної політики . На відміну від «жорсткої сили», яка ґрунтується на примусі, «м'яка сила» впливає через привабливість культурних цінностей, політичних ідеалів та зовнішньополітичного курсу держави. У контексті збройного конфлікту «м'яка сила» України виявляється в її здатності сформувати привабливий образ держави, що боронить демократичні цінності, і таким чином мобілізувати широку міжнародну підтримку [44]. Особливо показово, що у перші тижні повномасштабного вторгнення 2022 р. Україні вдалося конвертувати «м'яку силу» у цілком конкретні матеріальні результати:

прискорення надання зброї, введення безпрецедентних санкцій, безпрецедентну консолідацію НАТО.

Специфічне місце серед концептуальних підходів посідає теорія інформаційних операцій, розроблена переважно у військово-стратегічному контексті [45, с. 88]. Вона розглядає інформаційні дії як цілеспрямовані заходи впливу на свідомість супротивника та населення – через психологічні операції (PSYOP), дезінформацію, маніпуляції з медіасередовищем. У доктрині НАТО інформаційне середовище розглядається як один із п'яти оперативних доменів поряд із сухопутним, морським, повітряним і кіберпросторовим [46].

Новітнім концептуальним вкладом є дослідження феномену «когнітивної безпеки» – захисту когнітивних процесів суспільства від зовнішніх маніпуляцій [47, с. 5]. Когнітивна безпека виходить за межі традиційної інформаційної безпеки, оскільки враховує психологічні механізми сприйняття та обробки інформації. Ключовими загрозами є дезінформаційні кампанії, спрямовані на когнітивні упередження (confirmation bias, illusory truth effect тощо), а також технологічні маніпуляції – deepfake та алгоритмічне таргетування [48]. Дослідження Я. Роозенбека та С. ван дер Ліндена переконливо довели: найефективнішим захистом від когнітивних маніпуляцій є не реактивне спростування дезінформації, а превентивне «щеплення» – формування здатності розпізнавати прийоми маніпуляції ще до зіткнення з конкретним фейком .

Значний внесок у розвиток концептуальної бази зробили В. Г. Пилипчук та В. М. Брижко, які розробили правові засади інформаційної безпеки у контексті національного законодавства України . Їхні дослідження дозволяють пов'язати абстрактні теоретичні концепції з конкретними правовими механізмами захисту інформаційного суверенітету. О. В. Литвиненко, спираючись на теорію інформаційних операцій, розробив типологію спеціальних інформаційних впливів, що застосовуються Росією проти України, та запропонував відповідні механізми протидії .

Підсумовуючи, можна констатувати, що сучасна наука виробила різноманітний арсенал концептуальних підходів до вивчення інформаційної безпеки, кожен з яких акцентує на різних аспектах складного явища [35, с. 28]. Для аналізу інформаційної політики України в умовах війни найбільш продуктивним є синтетичний підхід, що поєднує елементи теорії гібридної війни, концепцій стратегічних комунікацій, сек'юритизації, «м'якої сили» та постправди. Саме такий мультипарадигмальний підхід дозволяє охопити всі виміри інформаційного протиборства – від технічного кіберзахисту до тонких механізмів наративного управління та публічної дипломатії.

1.3. Зарубіжний досвід формування інформаційної політики в умовах збройних конфліктів

Для розуміння специфіки інформаційної політики України в умовах повномасштабного вторгнення важливо звернутися до зарубіжного досвіду держав, що зіткнулися з аналогічними викликами [49, с. 3]. Аналіз дозволяє виявити успішні моделі та підходи, адаптовані до умов збройного конфлікту, а також уникнути помилок, допущених іншими.

Досвід Ізраїлю заслуговує особливої уваги, оскільки ця держава протягом десятиліть перебуває в умовах перманентного конфлікту і виробила розвинену систему стратегічних комунікацій [50]. Ключовим елементом є Управління прес-служби уряду (Government Press Office), що координує комунікацію для іноземних журналістів. Армія оборони Ізраїлю розробила детальну медіастратегію, яка включає оперативне реагування на інформаційні кампанії противника та просування власного наративу в соціальних мережах . Особливо важливим є принцип збереження відносної свободи медіа всередині країни при обмеженні лише тих матеріалів, що становили пряму загрозу безпеці [52]. Ізраїльська модель також демонструє важливість «embedded journalism» – систематичного включення журналістів

безпосередньо до військових підрозділів, що дозволяє формувати автентичний контент із зони бойових дій під контрольованим безпековим режимом.

Естонія – одна з провідних держав у сфері кібербезпеки та протидії інформаційним операціям – після масштабних кібератак 2007 р. стала ідейним лідером в НАТО щодо кіберзахисту [53, с. 12]. У Таллінні розміщено Центр кібербезпеки НАТО (CCDCOE). Естонська модель включає триєдність підходів: технічний захист критичної інфраструктури, правовий інструментарій протидії дезінформації та медіаграмотність населення [54]. Показово, що Естонія зробила медіаграмотність обов'язковою складовою шкільної освіти, розглядаючи її як ключовий елемент «соціального імунітету» проти пропаганди . Естонський досвід є прямим взірцем для України з огляду на схожість геополітичного становища та характеру загроз з боку Росії.

Досвід Фінляндії є унікальним з огляду на її багатовікове сусідство з Росією. Фінська модель «цілісної оборони» (comprehensive security) передбачає залучення всіх секторів суспільства – уряду, приватного бізнесу, громадянського суспільства та кожного громадянина – до системи забезпечення безпеки, включаючи інформаційну [56]. Ключовим інструментом є «Стратегічна безпека суспільства» (YHTS), яка визначає функції органів влади в кризових ситуаціях. Фінляндія регулярно проводить навчання з кризового управління, в яких відпрацьовуються сценарії інформаційних атак . Показниками ефективності цієї моделі є стабільно висока медіаграмотність населення та стійкість суспільства до дезінформаційних кампаній [58]. Фінська концепція «психологічної стійкості» нації, що формується через освіту і регулярні навчання цивільного населення, є тим ідеалом, до якого Україна наближається в умовах реального збройного конфлікту прискореними темпами.

Досвід Великобританії в протидії інформаційним операціям пов'язаний насамперед із Центром урядових комунікацій (GCHQ) та підрозділами

стратегічних комунікацій Міністерства закордонних справ [59]. Британська модель розмежовує контрпропаганду (спростування дезінформації) та проактивну стратегічну комунікацію (просування власних наративів). Особливу роль відіграє незалежна BBC як засіб «м'якої сили» в міжнародному мовленні [60, с. 8]. Британський уряд також профінансував ряд проєктів із підтримки незалежних медіа в країнах пострадянського простору, що є частиною зовнішньої інформаційної політики [61]. Зокрема, британська підтримка незалежних українських редакцій є важливим фактором розбудови стійкого медіасередовища в Україні.

Надзвичайно релевантним для України є досвід Тайваню, який перебуває в умовах постійного тиску Китаю і виробив комплексну стратегію протидії інформаційним операціям [62]. Тайванська екосистема фактчекінгу та контрнаративів включає незалежні організації (IORG, Cofacts, MyGoPen), активну роботу уряду зі швидкого спростування фейків через соціальні мережі, а також законодавче регулювання поширення дезінформації . Визначним є принцип систематичної просвітницької роботи з метою формування суспільного імунітету проти дезінформації [64]. Б. Німо, аналізуючи тайванський досвід, виокремлює принцип «швидкого і точного спростування» – офіційні органи протидіють конкретним дезінформаційним матеріалам протягом перших двох годин після їх появи, поки вони не встигли набути масового поширення [62].

Порівняльний аналіз дозволяє виокремити ключові компоненти ефективної інформаційної політики в умовах збройних конфліктів [49, с. 88]: наявність координаційного центру стратегічних комунікацій з чіткими повноваженнями; розвинена система взаємодії між державними органами, медіа та громадянським суспільством; потужна система моніторингу дезінформації та оперативного реагування; систематична робота з медіаграмотності населення; активна зовнішня комунікація та просування власних наративів на міжнародній арені.

Важливим уроком є також те, що надмірна централізація інформаційної політики та придушення свободи слова, навіть в умовах конфлікту, підривають довіру до влади і в кінцевому рахунку послаблюють стійкість суспільства [65, с. 43]. Демократичні держави, що зберігають відкритість та свободу медіа, демонструють більш ефективне довгострокове протистояння інформаційним операціям противника порівняно з тими, хто обирає шлях жорсткого контролю. Л. Х. Адар зазначає, що ізраїльська модель балансування між безпековими обмеженнями та медіаплюралізмом є зразком для наслідування саме тому, що не прагне встановити тотальний контроль над інформаційним простором [51, с. 74]. Цей принцип є надзвичайно важливим для розуміння підходів, обраних Україною в умовах повномасштабної війни.

Висновки до розділу 1

У першому розділі здійснено теоретико-методологічний аналіз поняття та засад дослідження інформаційної політики держави. На підставі проведеного аналізу можна сформулювати такі основні висновки.

По-перше, інформаційна політика держави є багатовимірним феноменом, що охоплює правовий, інституційний, комунікативний і безпековий виміри. Вона являє собою цілеспрямовану систему принципів, цілей, механізмів та заходів державних органів щодо регулювання інформаційного простору, захисту національних інтересів та забезпечення ефективної суспільної комунікації [22, с. 19]. В умовах збройних конфліктів інформаційна політика набуває стратегічного характеру, перетворюючись на один з ключових фронтів національної безпеки . Теоретичні концепції Е. Тоффлера, М. Кастельса, Дж. Ная і Ф. Уебстера формують підґрунтя для розуміння того, чому боротьба за інформаційний простір набула такого вирішального значення в сучасних конфліктах.

По-друге, сучасна наука виробила різноманітний арсенал концептуальних підходів до вивчення інформаційної безпеки – теорії гібридної війни, стратегічних комунікацій, сек'юритизації, «м'якої сили» та концепцію постправди [35, с. 30]. Для аналізу інформаційної політики України найбільш адекватним є синтетичний підхід, що поєднує елементи зазначених концепцій з урахуванням специфіки російсько-українського конфлікту. Особливо продуктивними є поняття «когнітивної безпеки» та «психологічного щеплення», що пояснюють механізми та методи протидії сучасним маніпулятивним технологіям.

По-третє, порівняльний аналіз зарубіжного досвіду (Ізраїль, Естонія, Фінляндія, Велика Британія, Тайвань) свідчить про те, що ефективна інформаційна політика в умовах конфліктів потребує координаційного центру стратегічних комунікацій, розвиненої системи взаємодії між державою, медіа та громадянським суспільством, потужної системи моніторингу дезінформації, систематичної роботи з медіаграмотності, активної зовнішньої комунікації . При цьому збереження принципів свободи слова та медіаплюралізму є запорукою довгострокової ефективності [65, с. 47].

Ці теоретико-методологічні засади становлять підґрунтя для подальшого аналізу становлення та функціонування інформаційної політики України в умовах повномасштабного вторгнення Росії, що є предметом наступних розділів роботи.

РОЗДІЛ 2

ІНФОРМАЦІЙНА ПОЛІТИКА УКРАЇНИ В УМОВАХ РОСІЙСЬКО-УКРАЇНСЬКОЇ ВІЙНИ

2.1. Становлення та розвиток інформаційної політики України (2014–2022 рр.)

Становлення сучасної інформаційної політики України нерозривно пов'язане з подіями 2014 року, які кардинально змінили безпекову парадигму держави та виявили критичну вразливість у сфері інформаційного простору. Анексія Криму та початок збройного конфлікту на Донбасі засвідчили, що Росія розглядає інформаційну сферу як самостійний театр бойових дій, де систематична дезінформація, пропаганда та маніпулювання суспільною свідомістю є інструментами досягнення стратегічних цілей [1, с. 45].

До 2014 року Україна не мала цілісної системи інформаційної безпеки, здатної протистояти масштабним зовнішнім інформаційним операціям. Інформаційна політика держави зводилася переважно до регулювання медіаринку, забезпечення права на доступ до інформації та захисту інтелектуальної власності . Відсутність ефективного захисту національного інформаційного простору дозволила проросійським ЗМІ, які мали широку аудиторію на сході та півдні країни, активно формувати ворожі наративи ще задовго до початку відкритої агресії . В. К. Горовенко вказує, що системна вразливість медіапростору України на момент 2014 року була зумовлена не лише відсутністю правових механізмів протидії зовнішньому інформаційному впливу, але й олігархічною концентрацією медіавласності, яка підривала редакційну незалежність та знижувала стійкість медіасистеми .

Перша реакція держави на виклики 2014 року мала переважно реактивний характер. Серед першочергових заходів – блокування та заборона

трансляції ряду проросійських телеканалів, що активно поширювали дезінформацію, зокрема телеканалів «Росія 1», «НТВ», «РТР-Планета» . Водночас паралельно відбувалося організаційне оформлення системи стратегічних комунікацій: у структурі Збройних Сил України та силових відомств почали формуватися підрозділи інформаційно-психологічних операцій.

Важливим кроком у формуванні правової бази стало ухвалення у 2015 році Стратегії національної безпеки України, яка вперше на рівні стратегічного документа визначила інформаційну безпеку одним із пріоритетів державної політики . Стратегія фіксувала як реальні загрози інформаційні операції Росії, спрямовані на підрив конституційного ладу та територіальної цілісності України. Це стало відправною точкою для системного переосмислення підходів до захисту інформаційного простору.

Ключовим документом у формуванні концептуальних засад інформаційної безпеки стала Доктрина інформаційної безпеки України, затверджена Указом Президента у лютому 2017 року. Доктрина визначила основні загрози в інформаційній сфері, серед яких: ведення Росією інформаційно-психологічної війни проти України, цілеспрямоване поширення дезінформації для дестабілізації суспільно-політичної ситуації, кібератаки на критичну інформаційну інфраструктуру [32]. Документ також окреслив основні напрями державної інформаційної політики: забезпечення свободи слова та доступу до інформації, розвиток медіаграмотності, підтримка вітчизняного виробника медіаконтенту, протидія пропаганді. І. В. Застава, аналізуючи Доктрину, зазначає, що її важливим досягненням стало визнання гібридних інформаційних загроз на рівні базового стратегічного документа – це означало суттєву зміну парадигми від традиційного уявлення про безпеку виключно як фізичний захист [24, с. 50].

У 2017 році відбулася й важлива інституційна зміна – ліквідація Міністерства інформаційної політики, яке було засновано у 2014 р. і піддавалося критиці за ризики цензури та неефективність. Функції у сфері

державних комунікацій частково перейшли до Міністерства культури та Секретаріату Кабінету Міністрів, а питання протидії дезінформації – до Ради національної безпеки і оборони України [27, с. 59]. Ця реорганізація відображала загальнішу тенденцію до відмови від моделі інформаційного управління, що передбачає єдиний контролюючий орган, на користь розподіленої архітектури з чітким розмежуванням функцій між кількома інституціями.

Паралельно з формуванням нормативної бази відбувалася трансформація медіасистеми. У 2015 році Верховна Рада ухвалила Закон «Про телебачення і радіомовлення» з поправками, що посилили регулювання частки іноземного (зокрема російського) контенту. У 2019 р. набув чинності Закон «Про аудіовізуальні послуги», що гармонізував українське законодавство з Директивою ЄС про аудіовізуальні медіапослуги . Ці заходи поступово зменшували присутність російського контенту в медіапросторі.

Важливою складовою стала розбудова системи суспільного мовлення. Створення Суспільного телебачення і радіомовлення України (UA: Перший, UA: Культура, Українське радіо) стало кроком до формування незалежного від олігархічних структур медіаресурсу, спроможного транслювати якісний суспільно значущий контент . Водночас фінансування Суспільного мовника залишалося хронічно недостатнім, що обмежувало його конкурентоспроможність на медіаринку порівняно з комерційними телеканалами, що перебували під контролем олігархічних структур.

Значний поштовх для розвитку медіаграмотності населення дала діяльність громадянського суспільства. З 2014 року в Україні активно розвивається рух фактчекінгу: організації «Стоп Фейк», VoxCheck, «Слово і Діло» систематично спростовують дезінформацію, документують маніпуляції та підвищують критичне мислення аудиторії . Ця екосистема незалежного фактчекінгу стала важливою складовою інформаційної стійкості суспільства.

На міжнародному напрямку Україна посилювала взаємодію з партнерами у сфері протидії дезінформації. Показовим є участь у проєктах ЄС East StratCom Task Force та співробітництво з Центром стратегічних комунікацій НАТО (NATO StratCom COE) у Ризі [38]. Українські спеціалісти отримували доступ до кращих практик та брали участь у спільних навчаннях. Водночас дослідники НАТО StratCom COE фіксували, що наявні зусилля України у сфері стратегічних комунікацій ще не досягли рівня системності, необхідного для ефективної протидії масштабній інформаційній агресії .

Таким чином, протягом 2014–2022 рр. Україна пройшла шлях від реактивної, фрагментарної інформаційної політики до поступового формування системної архітектури інформаційної безпеки з розвиненою нормативно-правовою базою, мережею профільних інституцій та розгалуженою екосистемою громадянського суспільства. Однак повномасштабне вторгнення 24 лютого 2022 року поставило перед цією системою безпрецедентні виклики, що вимагали кардинальної адаптації .

2.2. Нормативно-правова база інформаційної політики України в умовах воєнного стану

З початком повномасштабного вторгнення Росії 24 лютого 2022 року Україна вступила в принципово новий правовий режим, запровадження якого кардинально змінило умови функціонування інформаційного простору. Введення воєнного стану відповідно до Указу Президента України № 64/2022 від 24 лютого 2022 року надало органам державної влади широкі повноваження у сфері регулювання інформаційної діяльності . Це зумовило значне розширення та оновлення нормативно-правової бази інформаційної політики.

Правову основу інформаційної діяльності в умовах воєнного стану утворює комплекс нормативних актів різного рівня. Закон України «Про

правовий режим воєнного стану» 2015 р. (зі змінами) визначив загальні рамки обмежень прав і свобод, допустимих у воєнний час, у тому числі в інформаційній сфері. Відповідно до нього, органи державної влади отримали повноваження здійснювати контроль над засобами масової інформації, вилучати приміщення та майно для потреб оборони, обмежувати роботу організацій, що загрожують безпеці [32].

Ключовим нормативним актом, що безпосередньо регулює інформаційну сферу в умовах воєнного стану, стало рішення РНБО від 17 березня 2022 року, яке встановило порядок висвітлення бойових дій і діяльності Збройних Сил України. Документ визначив категорії інформації, поширення якої може завдати шкоди обороні: дані про дислокацію військ, маршрути пересування, втрати техніки та особового складу. Одночасно передбачалися механізми акредитації журналістів для роботи в зоні бойових дій . В. Г. Пилипчук та В. М. Брижко підкреслюють, що ці обмеження повністю відповідають загальновизнаним міжнародним стандартам у сфері обмеження свободи слова в умовах воєнного часу та є значно менш жорсткими, ніж аналогічне регулювання, що застосовувалося, зокрема, у Великобританії під час Фолклендської кампанії .

Верховна Рада України протягом 2022–2023 рр. ухвалила низку законодавчих актів, спрямованих на захист інформаційного простору в умовах збройної агресії. Закон «Про медіа» (2022 р.) став комплексним актом, що замінив застаріле законодавство про телебачення та радіомовлення, друковані ЗМІ й інформаційні агентства. Закон запровадив єдиний реєстр медіа, механізми відповідальності за поширення дезінформації та пропаганди, розширені повноваження Національної ради з питань телебачення і радіомовлення .

Важливим нормативним кроком стали зміни до Кримінального кодексу України, якими встановлено кримінальну відповідальність за виправдання, визнання правомірним або заперечення збройної агресії Російської Федерації проти України, а також за поширення завідомо неправдивої інформації про

дії Збройних Сил та інших силових структур (стаття 114-2 КК України) . Ці норми стали важливим інструментом протидії інформаційним диверсіям і колабораціонізму. Водночас у правозахисному середовищі тривають дискусії щодо чіткості критеріїв розмежування між кримінально карним поширенням дезінформації та захищеною свободою слова – критикою дій влади .

Законодавством було посилено повноваження Служби безпеки України у сфері протидії інформаційним загрозам. Відповідно до змін до Закону «Про Службу безпеки України», СБУ отримала ширші можливості для виявлення та нейтралізації мереж, що займаються поширенням дезінформації та проведенням інформаційних операцій противника .

Окремим напрямом нормативного регулювання стало законодавство про санкції. Указами Президента та рішеннями РНБО запроваджувалися санкції проти осіб та організацій, причетних до інформаційних операцій проти України: блокування доступу до низки сайтів, заборона трансляції певних телеканалів, обмеження діяльності соціальних мереж, що систематично поширювали дезінформацію або відмовлялися видаляти контент, що порушував законодавство [25, с. 15]. На думку О. В. Литвиненка, санкційна практика є одним з найефективніших інструментів правового впливу на учасників інформаційних операцій, оскільки вона дозволяє гнучко реагувати на нові загрози без проходження тривалих законодавчих процедур [25, с. 19].

Нормативно-правова база регулює також сферу кібербезпеки, що є невід'ємною складовою інформаційної безпеки. Закон «Про основні засади забезпечення кібербезпеки України» (2017 р.) та Стратегія кібербезпеки України (оновлена у 2021 р.) визначили архітектуру захисту критичної інформаційної інфраструктури, розподіл відповідальності між ДССЗЗІ, СБУ та іншими суб'єктами . В умовах воєнного стану ці механізми набули критичного значення на тлі безпрецедентного зростання кількості кібератак на державні інформаційні ресурси.

Особливої уваги заслуговує Указ Президента «Про заходи щодо забезпечення інформаційної безпеки України» 2022 р., що конкретизував повноваження Ради національної безпеки і оборони як вищого координаційного органу у сфері інформаційної безпеки в умовах воєнного стану. РНБО отримала право оперативно приймати рішення про блокування інформаційних ресурсів, що загрожують національній безпеці, без попереднього судового контролю . Д. В. Дубов зазначає, що ця норма є відступом від принципів верховенства права, які вимагають судового контролю над обмеженнями свободи слова, однак вона є вимушеним і тимчасовим заходом, що відповідає практиці провідних демократичних держав в умовах воєнної загрози .

Водночас нормативне регулювання інформаційної сфери в умовах воєнного стану породжує ряд правових дилем. Баланс між обмеженнями, продиктованими вимогами безпеки, та збереженням свободи слова залишається предметом дискусій. Правозахисні організації фіксують окремі випадки застосування законодавства воєнного часу для тиску на журналістів та блогерів, що критикують діяльність влади . Разом із тим переважна більшість запроваджених обмежень відповідає стандартам, допустимим відповідно до Міжнародного пакту про громадянські та політичні права в умовах надзвичайного стану.

У цілому нормативно-правова база інформаційної політики України в умовах воєнного стану демонструє прагнення держави знайти збалансований підхід: забезпечити захист від масштабних інформаційних операцій противника, зберігаючи при цьому основи відкритого медіасередовища та свободи слова. Цей підхід відрізняє українську модель від авторитарних практик придушення інформаційного плюралізму та відповідає зарубіжному досвіду демократичних держав, що перебувають у стані збройного конфлікту .

2.3. Діяльність державних інститутів у сфері інформаційної безпеки

Ефективність інформаційної політики держави безпосередньо залежить від дієздатності інституційної системи, що її реалізує. В умовах повномасштабного вторгнення Росії Україна здійснила суттєву реорганізацію системи державних інститутів у сфері інформаційної безпеки, посилюючи координацію між різними відомствами та адаптуючи їх функції до умов воєнного часу .

Центральну координаційну роль у системі інформаційної безпеки відіграє Рада національної безпеки і оборони України. В умовах воєнного стану РНБО значно активізувала свою діяльність у сфері протидії інформаційним загрозам. Рішення РНБО визначають стратегічні пріоритети, санкційну політику щодо медіаресурсів та осіб, що сприяють поширенню ворожої дезінформації, а також загальну архітектуру державних комунікацій у кризових ситуаціях [32].

Офіс Президента України взяв на себе функцію головного комунікатора держави в умовах повномасштабної війни. Щоденні звернення Президента Зеленського до громадян – спочатку у форматі відеозвернень із вулиць Києва, пізніше з різних локацій – стали потужним інструментом мобілізації суспільства, підтримання морального духу і формування позитивного міжнародного іміджу України . Офіс ОПУ фактично виконує функції центру стратегічних комунікацій, координуючи ключові наративи та месиджі для внутрішньої та зовнішньої аудиторій. А. В. Баровська підкреслює, що цей феномен є унікальним у порівняльній перспективі: рідко коли особистісна комунікація лідера стає настільки визначальним чинником інформаційної стійкості держави .

Міністерство культури та інформаційної політики України, відновлене у розширеному форматі у 2020 р., в умовах війни сконцентрувалося на завданнях просування культурних та суспільних наративів, що протистоять

спробам Росії заперечити самобутність і суверенітет України. Міністерство координує роботу Українського інституту, відповідального за публічну дипломатію та поширення позитивного образу України за кордоном .

Служба безпеки України є ключовим оперативним органом у сфері протидії інформаційним операціям противника. Департамент контррозвідки виявляє та нейтралізує мережі агентів впливу, що займаються організацією дезінформаційних кампаній; здійснює розслідування діяльності осіб, підозрюваних у поширенні ворожої пропаганди та колаборації з агресором . У 2022–2024 рр. СБУ порушила тисячі кримінальних проваджень за статтями, пов'язаними з інформаційними злочинами.

Державна служба спеціального зв'язку та захисту інформації України (ДССЗЗІ) відповідає за технічний захист критичної інформаційної інфраструктури та кіберзахист державних інформаційних ресурсів. CERT-UA – Урядова команда реагування на комп'ютерні надзвичайні події – у режимі реального часу відстежує кіберзагрози та координує реагування на кібератаки. З початку повномасштабного вторгнення CERT-UA фіксує безпрецедентне зростання кількості спроб проникнення у державні інформаційні системи та атак на об'єкти критичної інфраструктури . Важливо, що Україна побудувала механізм кіберзахисту не ізольовано, а у тісній взаємодії з партнерами по НАТО та з фахівцями провідних технологічних компаній – Microsoft, Google, Amazon, чиї хмарні рішення суттєво підвищили стійкість критичної інфраструктури перед лицем кібератак.

Центр протидії дезінформації при РНБО, заснований у 2021 році, в умовах повномасштабної війни суттєво розширив свою діяльність. Центр здійснює моніторинг дезінформаційних наративів у медіасередовищі, публічно спростовує фейки та маніпуляції, веде бази даних осіб та організацій, причетних до поширення ворожої пропаганди. Щоденні зведення Центру стали важливим джерелом інформації для журналістів та громадськості щодо актуальних дезінформаційних кампаній противника .

Збройні Сили України через Центр стратегічних комунікацій та Командування сил підтримки здійснюють інформаційно-психологічні операції як складову частину загальної воєнної стратегії . Сторінки ЗСУ у соціальних мережах, оперативне інформування громадськості про перебіг бойових дій, протидія ворожим психологічним операціям, спрямованим на деморалізацію особового складу та мирного населення, – усе це стало невід'ємною частиною діяльності військових комунікаторів.

Значну роль у системі державних інститутів відіграє Національна рада з питань телебачення і радіомовлення. В умовах воєнного стану Нацрада значно активізувала нагляд за дотриманням ліцензійних умов, запровадила механізм оперативного реагування на порушення, пов'язані з поширенням проросійської пропаганди, і підвищила вимоги до частки вітчизняного контенту в ефірі .

Особливу роль у системі інформаційної безпеки відіграє «Телемарафон» – «Єдині новини», запроваджений у березні 2022 р. як спільний телевізійний проєкт провідних національних телеканалів під координацією Офісу Президента. Марафон забезпечує цілодобове мовлення, покриваючи перебіг подій, офіційні повідомлення та спростування дезінформації. Водночас концентрація інформаційного потоку в одному медіапродукті привертає критику з боку медіаспільноти щодо можливих ризиків для медіаплюралізму . О. В. Литвиненко звертає увагу на парадокс: у короткостроковій перспективі централізація медіаповідомлень підвищує ефективність комунікації в кризових умовах, але у довгостроковій – ризикує підірвати диверсифікацію медіасистеми, яка є запорукою сталої інформаційної стійкості .

Міжвідомча координація у сфері інформаційної безпеки реалізується через механізм міжвідомчих робочих груп та регулярних координаційних нарад за участі РНБО, СБУ, ДССЗЗІ, профільних міністерств та Офісу Президента. Налагодження цієї координації, особливо в перші місяці

повномасштабного вторгнення, стало критичним завданням для забезпечення цілісності державного інформаційного впливу .

Отже, система державних інститутів у сфері інформаційної безпеки України в умовах воєнного стану продемонструвала здатність до адаптації та оперативного реагування на безпрецедентні виклики. Посилення координації між відомствами, чіткіший розподіл функцій та розширення повноважень ключових акторів стали умовою відносної ефективності державної інформаційної політики у критичних умовах збройного конфлікту . Разом із тим збереження балансу між безпековими вимогами та свободою слова залишається нагальним завданням для подальшого вдосконалення інституційної архітектури.

Висновки до розділу 2

У другому розділі здійснено комплексний аналіз інформаційної політики України в умовах російсько-української війни, що охоплює ретроспективний аналіз її становлення, нормативно-правову базу та діяльність державних інститутів. За результатами дослідження можна сформулювати такі висновки.

По-перше, формування системної інформаційної політики України розпочалося у відповідь на агресію Росії 2014 р. і проходило три основні фази: реактивну (2014–2016 рр.), що характеризувалася ситуативним реагуванням на конкретні інформаційні загрози; концептуальну (2017–2021 рр.), яка пов'язана з ухваленням Доктрини інформаційної безпеки та розбудовою інституційної архітектури; і трансформаційну (з лютого 2022 р.), зумовлену безпрецедентними викликами повномасштабного вторгнення . Кожен із цих етапів приніс суттєві якісні зміни у підходах до захисту інформаційного простору.

По-друге, нормативно-правова база інформаційної політики України в умовах воєнного стану зазнала суттєвого розширення та оновлення. Ключовими елементами стали Закон «Про медіа» (2022 р.), зміни до Кримінального кодексу щодо відповідальності за виправдання агресії та поширення дезінформації, а також посилення повноважень РНБО і СБУ у сфері протидії інформаційним операціям. При цьому Україна намагається зберегти баланс між вимогами безпеки та основоположними принципами свободи слова .

По-третє, система державних інститутів у сфері інформаційної безпеки характеризується багаторівневою архітектурою, що охоплює стратегічний рівень (РНБО, ОПУ), оперативний рівень (СБУ, ДССЗЗІ, CERT-UA, Центр протидії дезінформації), медіарегуляторний рівень (Нацрада з питань ТРМ) та комунікаційний рівень (Міністерство культури та інформаційної політики, Збройні Сили). Ефективна координація між цими рівнями є критичною умовою цілісності державної інформаційної політики .

Проведений аналіз засвідчує, що Україна в умовах повномасштабної війни здійснила значний прогрес у розбудові системи інформаційної безпеки, однак ряд системних проблем – недостатня координація між окремими інститутами, ризики для медіаплюралізму, нерівномірний рівень медіаграмотності населення – потребує подальшого вирішення. Ці питання будуть розглянуті у наступному розділі, присвяченому ефективності інформаційної протидії російській агресії.

РОЗДІЛ 3

ЕФЕКТИВНІСТЬ ІНФОРМАЦІЙНОЇ ПРОТИДІЇ РОСІЙСЬКІЙ АГРЕСІЇ

3.1. Стратегія протидії дезінформації та пропаганді

Повномасштабне вторгнення Російської Федерації 24 лютого 2022 року поставило перед інформаційною системою України безпрецедентне за масштабом і системністю випробування. Противник задіяв увесь арсенал інформаційно-психологічних інструментів: від класичної пропаганди та цілеспрямованої дезінформації до складних наративних операцій, спрямованих на підрив суспільного духу всередині країни та формування вигідного для Росії образу конфлікту на міжнародній арені [1, с. 58]. Відповіддю стала системна стратегія протидії, що поєднала оперативне спростування фейків, активне формування власного наративу та комплексну роботу з медіаграмотності населення.

Ключовим принципом стратегії протидії дезінформації, обраної Україною, стала проактивна, а не реактивна позиція. Досвід 2014–2021 рр. переконав вітчизняних фахівців у тому, що пасивне спростування окремих фейків є недостатньо ефективним: інформаційний вакуум, що виникає у кризових ситуаціях, неодмінно заповнюється ворожими наративами . Натомість стратегія передбачила випередження: держава сама формує порядок денний, задає ключові месиджі та утримує ініціативу в інформаційному просторі. Цей підхід відповідає концепції стратегічних комунікацій, розробленій у рамках НАТО, де наратив розглядається як критичний ресурс у сучасному конфлікті .

Центр протидії дезінформації при РНБО перетворився на головний оперативний вузол у системі виявлення та спростування ворожих наративів.

Центр здійснює безперервний моніторинг інформаційного середовища, виявляє нові дезінформаційні кампанії, публічно спростовує маніпуляції та веде систематичний облік осіб і структур, причетних до поширення ворожої пропаганди . Суттєвим елементом є щоденна публічна комунікація Центру через офіційні соціальні мережі, що забезпечує оперативне доведення спростувань до широкої аудиторії.

Аналіз ключових наративів, що поширювала Росія у 2022–2024 рр., дозволяє виокремити декілька стійких тематичних кластерів. Перший стосувався делегітимізації української державності й нібито «нацистського» характеру влади – наратив, спрямований насамперед на внутрішню аудиторію Росії та населення тимчасово окупованих територій . Другий охоплював тематику «провокацій» ЗСУ – приписування українській стороні військових злочинів, вчинених самим агресором (Буча, Маріуполь, Краматорськ), що мало на меті розмити відповідальність і ввести в оману міжнародну аудиторію. Третій кластер включав наративи про «безглуздість» опору, «неминучість» перемоги Росії та «нежиттєздатність» України – операції, спрямовані на психологічну деморалізацію . Четвертий кластер, спрямований переважно на міжнародну аудиторію, нав'язував «вину Заходу» за конфлікт та апелював до антинатовських настроїв у різних країнах, активно використовуючи соціальні розколи та постколоніальну риторику у країнах Глобального Півдня.

Протидія кожному з цих кластерів вимагала специфічних інструментів. Делегітимізуючим наративам Україна протиставила безпрецедентну відкритість: запрошення журналістів на місця злочинів, оперативна документація воєнних злочинів спільно з Міжнародним кримінальним судом, максимально широке поширення доказових матеріалів через міжнародні медіа . Наративам деморалізації протиставлялися демонстрація стійкості суспільства, героїчних прикладів опору та реальних успіхів ЗСУ на полі бою. Цей підхід відповідає висновкам Т. Снайдера про те, що збереження зв'язку з

реальністю є найважливішим ресурсом демократичного суспільства в протистоянні з авторитарною пропагандою .

Важливим інструментом контрнаративної стратегії стало залучення громадянського суспільства до документування злочинів агресора. Волонтерські організації, журналісти-розслідувачі та фотографи фіксували свідчення, що спростовували ворожі наративи й одночасно формували потужну доказову базу для міжнародного правосуддя . П. Померанцев, аналізуючи феномен постправди, наголошує: в умовах, коли пропаганда агресора свідомо розмиває межу між правдою й брехнею, найефективнішою відповіддю є максимальна конкретність – факти, дати, імена, докази .

Технологічний вимір стратегії протидії охоплює боротьбу з ботомережами та скоординованими неавтентичними операціями у соціальних мережах. Кіберспеціалісти СБУ та ДССЗЗІ у взаємодії з командами безпеки провідних платформ – Meta, Google, Twitter/X – виявляли та блокували мережі акаунтів, що штучно підсилювали ворожий контент . Водночас Україна добилася видалення значної кількості акаунтів, пов'язаних із кремлівськими інформаційними операціями, безпосередньо від адміністрації платформ. Особливо ефективним виявилося виявлення і публічне розкриття конкретних дезінформаційних кампаній – такий підхід не лише нейтралізує конкретну загрозу, але й підриває довіру до ворожих джерел загалом .

Медіаграмотність населення стала стратегічним пріоритетом, оскільки будь-яка зовнішня система спростувань є вторинною щодо критичного мислення кожного реципієнта інформації. Програми медіаграмотності реалізуються на рівні загальної освіти, бібліотечної системи та громадських організацій . Дослідження Я. Роозенбека та С. ван дер Ліндена підтверджують, що формування «психологічного щеплення» проти дезінформації через навчання прийомів маніпуляції є ефективнішим за пасивне спростування вже поширених фейків . Цей принцип активно

впроваджується у вітчизняній практиці, зокрема через загальнонаціональні освітні програми та онлайн-курси для широкої аудиторії.

Суттєвим напрямом є також робота з аудиторіями на тимчасово окупованих територіях. Інформаційна ізоляція жителів окупованих районів є свідомою стратегією агресора, що прагне монополізувати їхній доступ до інформації. Україна намагається підтримувати канали зв'язку з цими аудиторіями через спеціалізовані телеграм-канали, радіомовлення та ресурси в мережі Tor, що технічно долають блокування [5, с. 88]. В. Г. Пилипчук підкреслює, що збереження присутності в інформаційному просторі окупованих територій є стратегічно важливим не лише з гуманітарної, але й з безпекової точки зору – воно підтримує зв'язок між локальним населенням і українською державою як суб'єктом захисту їхніх прав .

Загалом стратегія протидії дезінформації та пропаганді в умовах повномасштабної війни продемонструвала здатність України до оперативного реагування та системного підходу. Синергія державних інституцій, незалежних медіа, громадянського суспільства та міжнародних партнерів забезпечила відносну ефективність інформаційної оборони у надзвичайно складних умовах . Водночас постійна еволюція тактик противника вимагає безперервного вдосконалення контрнаративних інструментів та підходів.

3.2. Роль медіа та громадянського суспільства в інформаційній обороні України

Однією з найяскравіших особливостей інформаційної стійкості України в умовах повномасштабної війни стала виняткова активність медіа та інститутів громадянського суспільства, що перетворилися на повноправних суб'єктів інформаційної оборони держави. Якщо в більшості попередніх збройних конфліктів головним комунікатором виступала

держава, то український кейс демонструє модель розподіленої, децентралізованої інформаційної стійкості, де кожен громадянин, журналіст і організація є активним учасником протидії пропаганді .

Незалежні українські медіа відіграли роль, що важко переоцінити. Видання «Українська правда», «Дзеркало тижня», «Суспільне мовлення», «Радіо Свобода / Радіо Вільна Європа» забезпечили безперервне висвітлення подій з акцентом на фактичній достовірності й незалежності від урядової позиції . У перші дні вторгнення, коли інформаційний простір захлинався у потоці суперечливих повідомлень, саме незалежні редакції встановили стандарти верифікованої журналістики, що зберігала довіру аудиторії. М. Прайс та М. Томпсон, аналізуючи медіасередовище в умовах конфлікту, наголошують: довіра є найціннішим активом медіасистеми, і вона набагато легше руйнується, ніж відновлюється .

Особливо важливою стала роль журналістики-розслідування у документуванні воєнних злочинів. Редакції Kyiv Independent, «Бабель», «Новинарня» та міжнародні медіапартнери здійснили низку розслідувань, що мали резонанс на рівні міжнародного правосуддя . Розслідування трагедії в Бучі, зафіксованої журналістами безпосередньо після деокупації, стало переламним моментом у міжнародному сприйнятті конфлікту і безпосередньо сприяло ухваленню нових пакетів санкцій проти Росії. Цей приклад унаочнює тезу Ф. Тейлора про те, що у сучасних конфліктах достовірна інформація є зброєю не меншою мірою, ніж пряма пропаганда .

Соціальні мережі перетворилися на критично важливий майданчик як для поширення інформації, так і для інформаційного протиборства. Telegram-канали державних органів (Офісу Президента, ЗСУ, обласних адміністрацій), незалежних медіа та волонтерських організацій утворили розгалужену мережу оперативного інформування, що компенсувала часові обмеження традиційного мовлення . Twitter/X став ключовим майданчиком для міжнародної аудиторії, де українські офіційні особи, журналісти та активісти системно формували порядок денний і спростовували ворожі наративи.

Відповідно до аналізу НАТО StratCom COE, здатність оперативно займати інформаційну нішу в перші години після події є вирішальним фактором у боротьбі за формування наративу .

Громадянське суспільство України – волонтерські організації, правозахисники, культурні спільноти – здійснило безпрецедентний внесок в інформаційну оборону. Організація «Стоп Фейк», заснована ще 2014 р., в умовах повномасштабного вторгнення різко нарощила потужності, щоденно спростовуючи десятки дезінформаційних матеріалів у 28 мовних версіях . VoxCheck запровадив систематичний моніторинг офіційних заяв і наративів, що виконує важливу функцію підзвітності не лише щодо ворожої пропаганди, але й щодо якості комунікації самих українських органів влади.

Д. В. Дубов наголошує, що роль громадянського суспільства в інформаційній обороні є не просто компенсаторною – доповнюючою там, де держава не справляється, – але й принципово відмінною за своєю природою . Громадські організації та незалежні медіа формують той вимір суспільної довіри та автентичності, який державні комунікатори за своєю природою не можуть забезпечити повною мірою. Саме тому «поліфонія» голосів громадянського суспільства є стратегічним активом, а не конкуруючим чинником щодо державних комунікаційних зусиль.

Важливим виміром ролі громадянського суспільства стало протидія інформаційним операціям противника у сфері культурної ідентичності. Спроби Росії привласнити українську культурну спадщину, заперечити самобутність українського народу та представити Україну як «штучну» державу зустріли організовану відповідь культурних інституцій та митців . Публічна дипломатія Українського інституту, виставки, концерти та культурні акції за кордоном стали потужним засобом утвердження окремої і самоцінної культурної ідентичності, що є одним з ключових елементів «м'якої сили» за Дж. Наєм . Т. Снайдер переконливо показав у своїх роботах, що контроль над культурним та історичним наративом є неодмінною умовою виправдання агресивної експансії з боку авторитарних режимів ; відповідно,

збереження і утвердження власного культурного наративу є для України не просто культурним, але й суто безпековим завданням.

Феномен «цифрової армії» волонтерів – громадян, що самоорганізовувалися для поширення верифікованої інформації, спростування фейків та підтримки офіційних наративів – є унікальною рисою українського кейсу. Мільйони пересічних користувачів соціальних мереж перетворилися на активних поширювачів перевіреної інформації про перебіг подій, що суттєво збільшило охоплення офіційних повідомлень . Така горизонтальна, мережева структура інформаційної активності відповідає концепції «мережевих воєн» Дж. Аркілли та Д. Ронфельдта, які ще на початку 2000-х рр. передбачали, що здатність мобілізувати децентралізовані мережі акторів стане ключовою перевагою у конфліктах інформаційної епохи .

Водночас активність медіа та громадянського суспільства ставить і нові виклики перед системою державних комунікацій. Надмірна кількість джерел та хаотичність інформаційних потоків у перші тижні вторгнення породжували ризик інформаційного перевантаження аудиторії, що також є формою дезорієнтації. Балансування між ефективною стратегічною комунікацією та збереженням плюралізму медіасередовища залишається одним з ключових завдань для держави в умовах тривалого конфлікту . М. Прайс наголошує: держава, що прагне монополізувати інформаційний простір заради ефективності, неодмінно втрачає довіру, яка є основою будь-якої комунікаційної стратегії .

Суттєвою проблемою є фінансова стійкість незалежних медіа в умовах війни. Падіння рекламних доходів, необхідність евакуації редакцій та втрата частини аудиторії внаслідок вимушеного переміщення населення створили серйозний тиск на незалежні видання. Підтримка медіа через міжнародні донорські механізми, зокрема програми ЄС та США, стала критично важливою для збереження плюральної медіасистеми . Водночас залежність від зовнішнього фінансування є потенційною вразливістю, на яку вказують

О. І. Романюк та інші дослідники медіасистем, оскільки вона може формувати інституційні стимули, що впливають на редакційну незалежність .

Отже, медіа та громадянське суспільство України продемонстрували здатність стати повноцінними суб'єктами інформаційної оборони, а не лише пасивними реципієнтами державних меседжів. Їхня роль є критично важливою як для внутрішньої стійкості – підтримання морального духу, запобігання паніці, збереження соціальної згуртованості, – так і для зовнішньої комунікації – формування правдивого образу конфлікту та України у світі . Цей синтез державних і недержавних акторів є визначальною особливістю ефективної демократичної інформаційної оборони.

3.3. Міжнародна складова інформаційної політики України під час війни

Міжнародний вимір інформаційної політики України в умовах повномасштабного вторгнення набув безпрецедентного стратегічного значення. Формування та підтримання широкої міжнародної коаліції підтримки є необхідною умовою продовження збройного опору, а отже, зовнішня комунікація стала невід'ємною складовою загальної воєнної стратегії . Здатність України сформувати переконливий наратив для міжнародної аудиторії і утримати його протягом тривалого конфлікту є одним з найвагоміших здобутків її інформаційної політики.

Центральну роль у зовнішній комунікації відіграла публічна дипломатія на найвищому рівні. Щоденні відеозвернення Президента Зеленського до парламентів, урядів та народів різних країн стали беззаперечним комунікаційним феноменом. Україні вдалося досягти того, чого рідко вдається навіть у мирний час: систематично транслювати свій наратив безпосередньо в серце міжнародних інститутів, оминаючи бар'єри

традиційної дипломатії . Дж. Най підкреслює, що здатність стати привабливим «відправником повідомлення» є вирішальним елементом «м'якої сили»; Зеленський перетворився на особистісне втілення цієї привабливості в очах мільйонів людей у світі . А. В. Баровська зауважує, що цей феномен свідчить про те, що у сучасних конфліктах публічна дипломатія лідера є не менш важливим ресурсом, ніж традиційні дипломатичні канали .

Стратегія зовнішньої комунікації України спиралася на кілька ключових наративних осей. Перша – легітимності: Україна представлена як суверенна демократична держава, що захищає не лише свою незалежність, але й фундаментальні принципи міжнародного права – недоторканність кордонів, заборону агресивної війни, захист мирного населення. Ця вісь апелювала до цінностей міжнародного порядку, що є спільними для більшості держав . Друга вісь – емпатійна: конкретні людські долі, свідчення жертв агресії, образи зруйнованих міст і шкіл формували емоційний зв'язок між міжнародною аудиторією та реальністю війни, що є надзвичайно важливим для підтримання тривалого суспільного інтересу . Третя – прагматична: аргументація на користь підтримки України з позицій інтересів самих країн-партнерів: безпека Євросоюзу, непохитність принципу ядерного нерозповсюдження, збереження заснованого на правилах міжнародного порядку [44].

Важливим елементом міжнародної інформаційної стратегії стала взаємодія з провідними світовими медіа. Україна забезпечила безпрецедентний рівень доступу іноземних журналістів до зон бойових дій та деокупованих територій – при збереженні розумних обмежень, зумовлених безпековими міркуваннями . Фотографії та відеоматеріали, зроблені журналістами безпосередньо на місцях злочинів, мали незрівнянно більший вплив на міжнародну громадську думку, ніж будь-які офіційні заяви. Це відповідає висновкам дослідників медіа в умовах конфлікту про те, що автентичність та безпосередність – найпотужніші комунікаційні ресурси .

Системна робота з протидії дезінформації на міжнародному рівні здійснювалася у тісній взаємодії з партнерами. Механізм East StratCom Task Force Євросоюзу, що діє з 2015 р., в умовах повномасштабного вторгнення різко нарощив потужності, щоденно відстежуючи та спростовуючи дезінформаційні наративи Росії у медіапросторі держав – членів ЄС . НАТО StratCom COE у Ризі здійснювало аналіз і документацію інформаційних операцій ворога, надаючи Україні та союзникам інструментальну базу для формування відповідей . Ця багатостороння координація відповідає підходу, описаному Е. Бралтлі як «колективна кіберстійкість» – здатність об'єднання держав спільно протистояти інформаційним та кіберзагрозам .

Міжнародний трибунальний вимір інформаційної стратегії є особливо важливим. Документування воєнних злочинів, що здійснюється за участі Міжнародного кримінального суду, Місії ООН з моніторингу прав людини та численних НУО, виконує подвійну функцію: є частиною зусиль із притягнення агресора до відповідальності і одночасно – потужним комунікаційним ресурсом. Кожне офіційне підтвердження воєнних злочинів авторитетними міжнародними інституціями унеможливлює заперечення ворожих дій і підтримує увагу міжнародної спільноти до конфлікту .

Окремим напрямом є робота з діаспорою, яка перетворилася на потужний актор зовнішньої інформаційної присутності України. Багатомільйонна українська діаспора в країнах ЄС, США, Канаді та Австралії стала природним медіатором між інформаційними продуктами Ukrainian state та місцевими аудиторіями, адаптуючи ключові наративи до специфіки відповідних культурних і мовних середовищ . Дж. Шерр, аналізуючи механізми публічної дипломатії в умовах конфлікту, підкреслює цінність органічної присутності в іноземному медіапросторі порівняно з інструментальними медіапроєктами, оскільки діаспорні голоси сприймаються місцевою аудиторією як автентичні, а не як державні меседжери .

Водночас міжнародна складова інформаційної стратегії зіткнулася з рядом серйозних викликів. Поступове «втомлення» міжнародної аудиторії від тривалого конфлікту є об'єктивним феноменом, що вимагає постійного оновлення комунікаційних підходів та пошуку нових форматів утримання уваги . М. Гамелірс та К. де Врізе зазначають, що медіаграмотність і критичне споживання інформації суттєво відрізняються в різних країнах, а отже, єдина комунікаційна стратегія не може бути однаково ефективною для всіх аудиторій . Диференціація повідомлень для різних регіонів і аудиторій залишається серйозним викликом для апарату зовнішньої комунікації України.

Особливою проблемою є боротьба за аудиторію у Глобальному Півдні – країнах Африки, Азії та Латинської Америки, де кремлівська пропаганда активно культивує антизахідні настрої та використовує постколоніальну риторику для формування нейтральної чи навіть проросійської позиції . Тайванський досвід свідчить, що ефективна міжнародна комунікація в таких умовах вимагає адаптації повідомлень до специфіки місцевого культурного та політичного контексту, а не механічного тиражування єдиного наративу . Е. Брат'берг та Т. Маурер звертають увагу на те, що Росія методично інвестувала у присутність у медіапросторі Африки та Латинської Америки протягом попереднього десятиліття, і ця підготовча робота дає свої плоди у вигляді відносно нейтральної або симпатизуючої позиції значної частини країн цих регіонів .

Незважаючи на ці виклики, міжнародна складова інформаційної стратегії України може бути оцінена як значно успішніша порівняно з тим, що мало місце у 2014–2015 рр. Формування широкої коаліції підтримки, що охопила понад 50 держав і забезпечила безпрецедентні обсяги військової, фінансової та гуманітарної допомоги, є прямим результатом ефективної зовнішньої комунікації . Ця коаліція не виникає сама по собі – вона є продуктом систематичної, цілеспрямованої і креативної дипломатично-

інформаційної роботи, що поєднала офіційні канали з медіа та громадянським суспільством.

Висновки до розділу 3

У третьому розділі здійснено комплексний аналіз ефективності інформаційної протидії України російській агресії у трьох ключових вимірах: стратегії протидії дезінформації та пропаганді, ролі медіа й громадянського суспільства, та міжнародної складової інформаційної політики. За результатами дослідження можна сформулювати такі висновки.

По-перше, стратегія протидії дезінформації та пропаганді в умовах повномасштабної війни набула системного, проактивного характеру, що суттєво відрізняє її від реактивних підходів попереднього періоду. Ключовими елементами стали: Центр протидії дезінформації при РНБО як головний оперативний вузол моніторингу та спростування ворожих наративів; комплексна контрнаративна стратегія, спрямована проти чотирьох основних тематичних кластерів дезінформації; технологічна боротьба з ботомережами та скоординованими неавтентичними операціями у соціальних мережах; робота з аудиторіями на тимчасово окупованих територіях; розвиток медіаграмотності населення як базового «психологічного щеплення» проти маніпуляцій . Разом із тим постійна еволюція тактик агресора вимагає безперервного вдосконалення контрнаративних підходів та своєчасного виявлення нових форм дезінформаційних кампаній.

По-друге, медіа та громадянське суспільство перетворилися на повноправних суб'єктів інформаційної оборони України, а не лише пасивних трансляторів державних повідомлень. Незалежні редакції забезпечили верифіковану журналістику, що зберігала довіру аудиторії у надзвичайно складних умовах. Організації фактчекінгу на щоденній основі спростовували

сотні дезінформаційних матеріалів та здійснювали систематичний моніторинг ворожих наративів . Мільйони громадян, що самоорганізувалися у горизонтальні мережі поширення верифікованої інформації, реалізували на практиці концепцію «розподіленої інформаційної стійкості» . Водночас збереження рівноваги між стратегічними комунікаціями держави та незалежністю медіасередовища, а також забезпечення фінансової стійкості незалежних редакцій залишаються нагальними викликами.

По-третє, міжнародна складова інформаційної стратегії України продемонструвала значну ефективність у формуванні та підтриманні широкої коаліції підтримки. Персональна публічна дипломатія Президента Зеленського, системне надання доступу міжнародним медіа до місць злочинів, документування воєнних злочинів у взаємодії з міжнародними трибунальними інституціями, залучення діаспорних мереж та активна взаємодія з механізмами ЄС і НАТО у сфері протидії дезінформації стали ключовими інструментами зовнішнього інформаційного виміру [3, с. 32; 38, с. 54]. Разом із тим «інформаційна втома» міжнародної аудиторії, необхідність диференціації повідомлень для різних регіонів та виклики боротьби за аудиторію Глобального Півдня є системними проблемами, що потребують подальшого вирішення.

Узагальнюючи результати аналізу, здійсненого у третьому розділі, можна стверджувати, що ефективність інформаційної протидії українській агресії визначається не окремими блискучими комунікаційними акціями, а стійкою системністю: координацією між державними інститутами, медіа та громадянським суспільством; узгодженістю внутрішнього та зовнішнього вимірів інформаційної стратегії; органічним поєднанням реактивного спростування дезінформації з проактивним формуванням власних наративів [6, с. 82; 15, с. 155]. Саме ця системність, що спирається на принципи свободи слова і медіаплюралізму, відрізняє демократичну модель інформаційної оборони від авторитарної концентрації та становить її стратегічну перевагу в тривалому протистоянні .

ВИСНОВКИ

Проведене дослідження інформаційної політики України в умовах російсько-української війни дозволяє сформулювати такі узагальнюючі висновки.

1. Інформаційна політика держави є багатовимірним феноменом, що охоплює правовий, інституційний, комунікативний і безпековий виміри та являє собою цілеспрямовану систему принципів, цілей, механізмів і заходів щодо регулювання інформаційного простору в інтересах національної безпеки і суспільного розвитку. Теоретичні концепції Е. Тоффлера, М. Кастельса, Дж. Ная та Ф. Уебстера переконливо доводять, що інформація є визначальним стратегічним ресурсом постіндустріальної доби, а держави, що не оволоділи механізмами управління інформаційними потоками, неминуче програють у змаганні за вплив на суспільну свідомість. В умовах збройного конфлікту ця закономірність набуває безпосереднього воєнно-стратегічного виміру.

2. Сучасна наука виробила різноманітний арсенал концептуальних підходів до вивчення інформаційної безпеки – теорії гібридної війни, стратегічних комунікацій, сек'юритизації, «м'якої сили» та концепцію постправди. Найпродуктивнішим для аналізу інформаційної політики України є синтетичний підхід, що поєднує елементи зазначених концепцій. Особливо важливими є поняття «когнітивної безпеки» та «психологічного щеплення», що пояснюють механізми протидії сучасним маніпулятивним технологіям, а також конструктивістська концепція захисту ідентичності як стратегічного ресурсу держави.

3. Порівняльний аналіз зарубіжного досвіду (Ізраїль, Естонія, Фінляндія, Велика Британія, Тайвань) дозволив виокремити універсальні компоненти ефективної інформаційної політики в умовах конфліктів: координаційний центр стратегічних комунікацій; розвинена система

взаємодії між державою, медіа та громадянським суспільством; потужна система моніторингу дезінформації; систематична робота з медіаграмотності; активна зовнішня комунікація. Зберігання медіаплюралізму є стратегічним активом, а не перешкодою для ефективної інформаційної оборони.

4. Інформаційна політика України у 2014–2022 рр. пройшла три послідовні фази: реактивну (2014–2016 рр.), концептуальну (2017–2021 рр.) та трансформаційну (2022 р. – по сьогодні). Кожна фаза позначилася якісними змінами в нормативно-правовій базі, інституційній архітектурі та практичних підходах до захисту інформаційного простору. Ухвалення Доктрини інформаційної безпеки 2017 р. стало переломним моментом у визнанні гібридних інформаційних загроз на рівні стратегічного документа.

5. Нормативно-правова база інформаційної політики в умовах воєнного стану зазнала суттєвого розширення. Ключовими елементами стали Закон «Про медіа» (2022 р.), зміни до Кримінального кодексу, посилення повноважень РНБО і СБУ. Україна прагне зберегти баланс між вимогами безпеки та основоположними принципами свободи слова, що відрізняє її підхід від авторитарних моделей інформаційного управління та відповідає стандартам демократичних держав в умовах надзвичайного стану.

6. Система державних інститутів у сфері інформаційної безпеки характеризується багаторівневою архітектурою: стратегічний рівень (РНБО, Офіс Президента), оперативний рівень (СБУ, ДССЗЗІ, CERT-UA, Центр протидії дезінформації), медіарегуляторний рівень (Нацрада з питань ТРМ) та комунікаційний рівень (Міністерство культури та інформаційної політики, стратегічні комунікації ЗСУ). Ефективна міжвідомча координація є критично важливою умовою цілісності державної інформаційної стратегії.

7. Стратегія протидії дезінформації та пропаганді набула системного, проактивного характеру. Протидія чотирьом основним кластерам ворожих наративів (делегітимізація, перекладання відповідальності, деморалізація, антизахідна риторика) здійснюється через поєднання оперативного фактчекінгу, документування злочинів агресора, технологічної боротьби з

ботомережами та систематичної роботи з медіаграмотності. Особливо значущими є зусилля щодо збереження інформаційної присутності на тимчасово окупованих територіях.

8. Медіа та громадянське суспільство перетворилися на повноправних суб'єктів інформаційної оборони, реалізуючи модель «розподіленої інформаційної стійкості». Незалежні редакції, фактчекінгові організації, культурні інституції та мільйони «цифрових волонтерів» забезпечують той вимір суспільної довіри та автентичності, який державні комунікатори за своєю природою не можуть надати повністю. Водночас збереження фінансової стійкості та редакційної незалежності медіа залишається системним викликом.

9. Міжнародна складова інформаційної стратегії України продемонструвала значну ефективність: сформована коаліція підтримки понад 50 держав є прямим результатом цілеспрямованої публічної дипломатії та стратегічної зовнішньої комунікації. Разом із тим «інформаційна втома» аудиторії, виклики Глобального Півдня та необхідність диференціації повідомлень для різних культурних середовищ вимагають постійного вдосконалення підходів.

10. Практичні рекомендації, що випливають з результатів дослідження: подальше вдосконалення правових механізмів балансування між безпековими обмеженнями та свободою слова; інституційне зміцнення Центру протидії дезінформації із розширенням ресурсного забезпечення; запровадження обов'язкового компонента медіаграмотності в усіх рівнях системи освіти за естонсько-фінською моделлю; формування механізмів державної підтримки фінансової стійкості незалежних медіа без порушення редакційної незалежності; диференційована стратегія зовнішньої комунікації для аудиторій Глобального Півдня з залученням регіональних посередників і діаспорних мереж.

Отже, досвід України в умовах повномасштабного збройного конфлікту засвідчив, що ефективна інформаційна оборона демократичної

держави ґрунтується на триєдності: розвиненій державній системі стратегічних комунікацій; потужному секторі незалежних медіа та громадянського суспільства; та активній міжнародній комунікаційній присутності. Ця модель, що поєднує державне і недержавне, внутрішнє і зовнішнє, реактивне і проактивне, є значним внеском України у світову практику інформаційної безпеки і заслуговує ретельного вивчення та адаптації іншими державами, що стикаються з аналогічними загрозами.

СПИСОК ВИКОРИСТАНИХ ДЖЕРЕЛ

1. Горовенко В. К. Інформаційна безпека України в умовах збройного конфлікту. Київ : Національний інститут стратегічних досліджень, 2022. 187 с.
2. Дубов Д. В. Інформаційне суспільство та державна інформаційна політика. Київ : НІСД, 2020. 214 с.
3. Баровська А. В. Стратегічні комунікації: досвід НАТО і перспективи для України. Київ : НІСД, 2019. 96 с.
4. Пилипчук В. Г. Інформаційна безпека держави: концептуальні підходи та механізми забезпечення. Київ : КНТ, 2018. 312 с.
5. Литвиненко О. В. Інформаційні операції та суспільство. Київ : Сфера, 2021. 248 с.
6. Баровська А. В., Дубов Д. В., Застава І. В. Сучасна інформаційна політика України: виклики та відповіді. Київ : НІСД, 2023. 134 с.
7. Тоффлер Е. Третя хвиля / пер. з англ. А. Євса. Київ : Всесвіт, 2000. 480 с.
8. Кастельс М. Інформаційна епоха: економіка, суспільство і культура / пер. з англ. Б. Верпаховської. Київ : Вища школа, 2006. 600 с.
9. Най Дж. Гнучка влада: як досягти успіху у світовій політиці / пер. з англ. М. Климчука. Львів : Кальварія, 2006. 232 с.
10. Уебстер Ф. Теорії інформаційного суспільства / пер. з англ. Є. Дячкіна. Київ : Академія, 2010. 400 с.
11. Горовенко В. К. Державна інформаційна політика: теорія і практика. Київ : Фенікс, 2017. 220 с.
12. Дубов Д. В. Кіберпростір як нова сфера геополітичного протистояння. Київ : НІСД, 2014. 152 с.
13. Пилипчук В. Г., Брижко В. М. Правові засади інформаційної безпеки України. Київ : КНТ, 2016. 280 с.

14. Баровська А. В. Інституційне забезпечення комунікаційної політики держави. Київ : НІСД, 2015. 128 с.
15. Литвиненко О. В. Спеціальні інформаційні операції та пропаганда. Київ : Сфера, 2000. 158 с.
16. Снайдер Т. Про тиранію: двадцять уроків двадцятого століття / пер. з англ. С. Борщевської. Київ : Медуза, 2022. 128 с.
17. Померанцев П. Нічого правдивого і все можливе / пер. з англ. О. Замойської. Київ : Yakaboo Publishing, 2020. 256 с.
18. Brantly A. F. The Decision to Attack: Military and Intelligence Cyber Decision-Making. Athens : University of Georgia Press, 2016. 272 p.
19. Горовенко В. К., Ліпкан В. А. Системний підхід в управлінні інформаційною безпекою. Київ : КНТ, 2019. 176 с.
20. Романюк О. І. Порівняльна політологія. Харків : ХНУ імені В. Н. Каразіна, 2021. 334 с.
21. Баровська А. В. Публічна дипломатія та стратегічні комунікації в умовах кризи. Київ : НІСД, 2022. 88 с.
22. Дубов Д. В., Ожеван М. А. Інформаційне суспільство в Україні: глобальні виклики та національні можливості. Київ : НІСД, 2011. 208 с.
23. Пилипчук В. Г. Еволюція поглядів на зміст інформаційної безпеки держави. Інформація і право. 2015. № 1 (13). С. 29–42.
24. Застава І. В. Інституційний вимір інформаційної політики держави. Стратегічні пріоритети. 2018. № 3 (48). С. 44–53.
25. Литвиненко О. В. Інформаційний суверенітет: сутність та механізми забезпечення. Національна безпека і оборона. 2019. № 4. С. 12–21.
26. Arquilla J., Ronfeldt D. Networks and Netwars: The Future of Terror, Crime, and Militancy. Santa Monica : RAND Corporation, 2001. 382 p.
27. Горовенко В. К. Зовнішня та внутрішня складові інформаційної політики України. Стратегічні пріоритети. 2020. № 2. С. 55–64.
28. Баровська А. В. Міжнародний досвід державного регулювання у сфері комунікацій. Київ : НІСД, 2016. 116 с.

29. Дубов Д. В. Ключові чинники формування ефективної інформаційної політики держави. Інформаційне суспільство. 2017. № 25. С. 98–108.
30. Ліпкан В. А. Інформаційна безпека України в умовах євроінтеграції. Київ : КНТ, 2006. 280 с.
31. Доктрина інформаційної безпеки України : затверджена Указом Президента України від 25 лют. 2017 р. № 47/2017. URL: https://www.president.gov.ua/documents/472017-21374 (дата звернення: 10.09.2024).
32. Про рішення Ради національної безпеки і оборони України від 29 грудня 2016 року «Про Доктрину інформаційної безпеки України» : Указ Президента України від 25 лют. 2017 р. № 47/2017. Офіційний вісник України. 2017. № 18. С. 101–107.
33. Горовенко В. К. Трансформація інформаційної політики держави в умовах збройного конфлікту. Вісник Національного університету оборони України. 2023. № 1 (71). С. 209–221.
34. Wilson C. Information Operations, Electronic Warfare, and Cyberwar: Capabilities and Related Policy Issues. Washington : Congressional Research Service, 2007. 24 p.
35. Lasswell H., Lerner D., Speier H. Propaganda and Communication in World History. Honolulu : University Press of Hawaii, 1980. Vol. 3. 410 p.
36. Hoffman F. G. Conflict in the 21st Century: The Rise of Hybrid Wars. Arlington : Potomac Institute for Policy Studies, 2007. 72 p.
37. Lanoszka A. Russian Hybrid Warfare and Extended Deterrence in Eastern Europe. International Affairs. 2016. Vol. 92, № 1. P. 175–195.
38. NATO Strategic Communications Centre of Excellence. Analysis of Russia’s Information Campaign Against Ukraine. Riga : NATO StratCom COE, 2023. 116 p.
39. Freedman L. Strategy: A History. Oxford : Oxford University Press, 2013. 632 p.

40. Wendt A. Social Theory of International Politics. Cambridge : Cambridge University Press, 1999. 429 p.
41. Buzan B., Wæver O., de Wilde J. Security: A New Framework for Analysis. Boulder : Lynne Rienner, 1998. 239 p.
42. Balzacq T. Securitization Theory: How Security Problems Emerge and Dissolve. London : Routledge, 2011. 232 p.
43. Fairclough N. Media Discourse. London : Edward Arnold, 1995. 214 p.
44. Nye J. S. Soft Power and the Ukraine Crisis. Project Syndicate. 2022. March 4. URL: https://www.project-syndicate.org (дата звернення: 15.09.2024).
45. Joint Chiefs of Staff. Information Operations. Joint Publication 3-13. Washington : Department of Defense, 2014. 112 p.
46. NATO. Allied Joint Doctrine for Information Operations. AJP-3.10. Brussels : NATO Standardization Office, 2015. 88 p.
47. Cognitive Security Institute. Cognitive Security: Protecting Democratic Discourse. Brussels : CSI, 2023. 64 p.
48. Roozenbeek J., van der Linden S. Fake News Game Confers Psychological Resistance Against Online Misinformation. Palgrave Communications. 2019. Vol. 5. P. 1–10.
49. Price M., Thompson M. Forging Peace: Intervention, Human Rights and the Management of Media Space. Edinburgh : Edinburgh University Press, 2002. 396 p.
50. Rid T., Hecker M. War 2.0: Irregular Warfare in the Information Age. Westport : Praeger Security International, 2009. 296 p.
51. Orr A. Information Operations in the Israeli-Palestinian Conflict. Journal of Strategic Studies. 2015. Vol. 38, № 1–2. P. 55–78.
52. Hadar L. Israel’s Information Strategy. Middle East Policy. 2014. Vol. 21, № 3. P. 88–102.
53. Tikk E., Kaska K., Vihul L. International Cyber Incidents: Legal Considerations. Tallinn : CCDCOE, 2010. 158 p.

54. Berzins J. Russia’s New Generation Warfare in Ukraine. Riga : National Defence Academy of Latvia, 2014. 18 p.
55. Raynova D. Building Societal Resilience Against Disinformation: The Estonian Model. European Leadership Network. 2019. № 12. P. 38–52.
56. Finnish Government. The Security Strategy for Society. Helsinki : Ministry of Defence, 2017. 112 p.
57. Brattberg E., Maurer T. Russian Election Interference: Europe’s Counter to Fake News and Cyber Attacks. Washington : Carnegie Endowment, 2018. 88 p.
58. Hameleers M., de Vreese C. Misinformation Resilience in Comparative European Perspective. European Journal of Communication. 2020. Vol. 35, № 4. P. 346–362.
59. UK Government. National Cyber Security Strategy 2022–2030. London : Cabinet Office, 2022. 76 p.
60. Taylor P. British Propaganda in the Twentieth Century. Edinburgh : Edinburgh University Press, 1999. 312 p.
61. Sherr J. Hard Diplomacy and Soft Coercion: Russia’s Influence Abroad. London : Chatham House, 2013. 124 p.
62. Nimmo B. Measuring the Information Environment: Taiwan and China. Digital Forensic Research Lab. 2022. URL: https://dfrlabs.medium.com (дата звернення: 20.09.2024).
63. Chen L. Taiwan’s Approach to Countering Disinformation. Journal of Democracy. 2021. Vol. 32, № 2. P. 10–24.
64. Lo J. Countering Disinformation in Taiwan: A Whole-of-Society Approach. Taipei : IORG, 2022. 84 p.
65. Price M. Free Expression, Globalism and the New Strategic Communication. Cambridge : Cambridge University Press, 2015. 290 p.

ДОДАТКИ

Додаток А

Основні нормативно-правові акти у сфері інформаційної політики України

№ з/п	Назва документа	Рік прийняття	Правовий статус
1	Стратегія національної безпеки України	2015, 2020	Указ Президента
2	Доктрина інформаційної безпеки України	2017	Указ Президента
3	Закон України “Про основні засади забезпечення кібербезпеки України”	2017	Закон України
4	Стратегія кібербезпеки України	2021	Указ Президента
5	Закон України “Про медіа”	2022	Закон України
6	Указ Президента про введення воєнного стану	2022	Указ Президента
7	Постанова Кабінету Міністрів про Центр протидії дезінформації	2021	Постанова КМУ
8	Закон України “Про захист інформації в інформаційно-комунікаційних системах”	1994, ред. 2023	Закон України

Джерело: складено автором на основі аналізу нормативно-правової бази України.

Додаток Б

Інституційна структура системи інформаційної безпеки України

Рівень	Органи / Інститути	Основні функції
Стратегічний	РНБО, Офіс Президента, Верховна Рада	Формування політики, прийняття стратегічних рішень
Оперативний	СБУ, ДССЗЗІ, CERT-UA, Центр протидії дезінформації	Моніторинг загроз, кіберзахист, протидія дезінформації
Медіарегуляторний	Нацрада з питань телебачення і радіомовлення	Регулювання медіасередовища, ліцензування
Комунікаційний	Міністерство культури та інформаційної політики, StratCom ЗСУ	Стратегічні комунікації, публічна дипломатія

Джерело: складено автором за матеріалами розділу 2.

Додаток В

Порівняльна характеристика моделей інформаційної політики в умовах збройних конфліктів

Критерій	Ізраїль	Естонія	Фінляндія	Тайвань
Координаційний орган	Government Press Office	CCDCOE / RIA	Мін-во оборони (YHTS)	IORG, Cofacts, MyGoPen
Участь громадянського суспільства	Висока	Висока	Дуже висока	Висока
Медіаграмотність	Середня	Обов’язкова у школі	Системна підготовка	Просвітницькі кампанії
Свобода медіа	З обмеженнями безпеки	Висока	Висока	Висока

Джерело: складено автором на основі порівняльного аналізу зарубіжного досвіду (розділ 1.3).

Додаток Г

Основні кластери російської дезінформації та методи протидії (2022–2024 рр.)

№	Кластер дезінформації	Ключові наративи	Методи протидії України
1	**Делегітимізація**	“Нацисти у владі”, “нелегітимний уряд”	Документування виборчих процедур, демонстрація демократичних норм
2	**Перекладання відповідальності**	“Україна сама провокує”, “НАТО розв’язало”	Документування агресії, міжнародні трибунальні докази
3	**Деморалізація**	“Прорив фронту”, “втрати катастрофічні”	Верифікована журналістика, офіційні брифінги ЗСУ
4	**Антизахідна риторика**	“Захід кидає Україну”, “санкції б’ють по своїх”	Демонстрація реальних результатів підтримки, публічна дипломатія

Джерело: складено автором за матеріалами розділу 3.1.

Додаток Д

Етапи розвитку інформаційної політики України (2014–2024 рр.)

Етап	Хронологія	Ключові характеристики	Ключові документи / події
Реактивний	2014–2016	Ситуативне реагування на загрози, відсутність системної стратегії	Блокування ряду російських сайтів, перші кроки медіарегулювання
Концептуальний	2017–2021	Формування нормативно-правової бази, розбудова інституцій	Доктрина 2017 р., Закон про кібербезпеку 2017 р., Стратегія кібербезпеки 2021 р.
Трансформаційний	2022–2024	Мобілізація системи в умовах воєнного стану, проактивна стратегія	Закон про медіа 2022 р., ЦПД при РНБО, системна зовнішня комунікація

Джерело: складено автором за матеріалами розділу 2.1.

Додаток Е

Міжнародна підтримка України: ключові партнери та механізми співпраці у сфері інформаційної безпеки

Партнер / структура	Форми співпраці	Результати
ЄС (East StratCom Task Force)	Спостереження за дезінформацією, координація контрнаративів	Системний моніторинг, бази даних дезінформації
НАТО StratCom COE (Рига)	Аналіз інформаційних операцій, тренінги, публікації	Аналітичні звіти, підвищення кваліфікації фахівців
США (USAID, DFRLab)	Фінансування незалежних медіа, технічна допомога	Підтримка медіаплюралізму, розвиток фактчекінгу
Велика Британія (FCDO)	Підтримка незалежних редакцій, проєкти медіаграмотності	Зміцнення стійкості медіасередовища
МКС та ООН (ММММПЛ)	Документування воєнних злочинів, моніторинг прав людини	Міжнародна легітимізація позиції України

Джерело: складено автором за матеріалами розділу 3.3.

Додаток Ж

Глосарій основних понять у сфері інформаційної політики та інформаційної безпеки

Термін	Визначення
Інформаційна політика держави	Цілеспрямована система принципів, цілей, засобів і заходів державних органів щодо регулювання інформаційного простору, захисту національних інтересів та забезпечення ефективної суспільної комунікації.
Інформаційна безпека	Стан захищеності інформаційного простору держави, що забезпечує реалізацію конституційних прав громадян в інформаційній сфері та захист національних інтересів від зовнішніх і внутрішніх загроз.
Гібридна війна	Форма конфлікту, що поєднує традиційні та нетрадиційні методи, включаючи інформаційні операції, кібератаки, економічний тиск і дипломатичні маніпуляції.
Дезінформація	Свідомо поширювана неправдива або перекручена інформація з метою введення аудиторії в оману та маніпулювання суспільною думкою.
М'яка сила (soft power)	Концепція Дж. Ная: здатність держави впливати на інших акторів через привабливість культурних цінностей, ідеалів і зовнішньополітичного курсу, без застосування примусу.
Когнітивна безпека	Захист когнітивних процесів суспільства від зовнішніх маніпуляцій, зокрема через дезінформаційні кампанії, що використовують психологічні упередження та технологічні інструменти.
Стратегічні комунікації	Скоординоване використання комунікаційних засобів для досягнення стратегічних цілей держави; передбачає формування та захист домінантного наративу в умовах конфлікту.
Сек'юритизація	Процес (за Копенгагенською школою), за яким проблема визначається як загроза безпеці та виноситься за межі звичайного політичного дискурсу, виправдовуючи застосування надзвичайних заходів.
Постправда (post-truth)	Інформаційне середовище (за П. Померанцевим), у якому об'єктивні факти мають менший вплив на суспільну думку, ніж апеляції до емоцій та особистих переконань; характерне для середовища сучасної пропаганди.

Джерело: складено автором на основі теоретичного аналізу, представленого у розділі 1.