

МІНІСТЕРСТВО ОСВІТИ І НАУКИ УКРАЇНИ
Харківський національний університет імені В.Н. Каразіна

Навчально-науковий інститут «Інститут державного управління»
Кафедра права, національної безпеки та європейської інтеграції

Кваліфікаційна робота магістра
на тему
ФОРМУВАННЯ ЕФЕКТИВНИХ КОМУНІКАЦІЙНИХ СТРАТЕГІЙ В
УМОВАХ ГІБРИДНИХ ЗАГРОЗ

Виконав студент 2 курсу,
групи ППГЗ-3-24
Спеціальності 281 «Публічне
управління та адміністрування»
Освітньо-професійної програми
«Публічна політика та управління в
умовах гібридних загроз»
_____ Вадим МОСКАЛЕЦЬ

Науковий керівник роботи:
кандидат наук з державного управління
_____ Борис ДЗЮНДЗЮК

ЗМІСТ

ПЕРЕЛІК СКОРОЧЕНЬ, УМОВНИХ ПОЗНАК, ОДИНИЦЬ І ТЕРМІНІВм	3
ВСТУП.....	4
РОЗДІЛ 1 ТЕОРЕТИЧНІ ТА МЕТОДОЛОГІЧНІ ОСНОВИ СТРАТЕГІЧНИХ КОМУНІКАЦІЙ В УМОВАХ ГІБРИДНИХ ЗАГРОЗ.....	7
1.1 Концептуальні засади стратегічних комунікацій та гібридних загроз..	7
1.2 Міжнародний досвід формування комунікаційних стратегій	16
РОЗДІЛ 2 АНАЛІЗ ГІБРИДНИХ ЗАГРОЗ ТА КОМУНІКАЦІЙНОЇ ПОЛІТИКИ УКРАЇНИ	26
2.1 Характеристика гібридних загроз для національної безпеки України	26
2.2 Система стратегічних комунікацій України: стан та проблеми	36
РОЗДІЛ 3 ФОРМУВАННЯ ТА РЕАЛІЗАЦІЯ ЕФЕКТИВНИХ КОМУНІКАЦІЙНИХ СТРАТЕГІЙ	45
3.1 Розробка комплексної комунікаційної стратегії протидії гібридним загрозам.....	45
3.2 Оцінка ефективності та рекомендації щодо вдосконалення комунікаційних стратегій.....	54
ВИСНОВКИ	62
СПИСОК ВИКОРИСТАНИХ ДЖЕРЕЛ	65

ПЕРЕЛІК СКОРОЧЕНЬ, УМОВНИХ ПОЗНАК, ОДИНИЦЬ І ТЕРМІНІВ

ЄС	Європейський Союз
ЗМІ	засоби масової інформації
НАТО	Організація Північноатлантичного договору
НІСД	Національний інститут стратегічних досліджень
ОБСЄ	Організація з безпеки і співробітництва в Європі
РНБО	Рада національної безпеки і оборони України
ШІ	штучний інтелект

ВСТУП

Актуальність теми. Сучасні загрози національній безпеці держав набули якісно нового характеру, що визначається їх комплексністю, гібридністю, асиметричністю та високим ступенем непередбачуваності. В умовах стрімкого розвитку інформаційних технологій, глобалізації медіа-простору та посилення ролі соціальних мереж, питання формування ефективних комунікаційних стратегій стає критично важливим для протидії гібридним загрозам, забезпечення національної безпеки та підтримки суспільної стійкості.

Проблематика стратегічних комунікацій у контексті протидії гібридним загрозам особливо актуалізувалась після незаконної анексії Криму Російською Федерацією та початку збройного конфлікту на сході України у 2014 році. Повномасштабне вторгнення Росії в Україну в лютому 2022 року продемонструвало, що інформаційний та комунікаційний компоненти є не просто супутніми елементами військової агресії, а складають її ключову й невід’ємну частину. В таких умовах стратегічні комунікації перетворюються з теоретичного концепту на практичний інструмент протидії агресії, формування суспільної згуртованості та міжнародної підтримки.

Україна зіткнулася з безпрецедентними за масштабом та інтенсивністю гібридними атаками, спрямованими на підрив державності, розкол суспільства, поширення деструктивних наративів та маніпуляцій, формування негативного образу країни в світі. Ці виклики вимагають створення комплексної, гнучкої та адаптивної системи стратегічних комунікацій, яка б забезпечувала ефективну протидію інформаційним загрозам та координувала зусилля всіх державних інституцій, громадянського суспільства та міжнародних партнерів.

Дослідження проблематики формування комунікаційних стратегій в умовах гібридних загроз набуває особливої актуальності з огляду на необхідність систематизації накопиченого Україною унікального досвіду, його теоретичного осмислення та розробки практичних рекомендацій щодо подальшого розвитку

національної системи стратегічних комунікацій. Важливим аспектом дослідження є також вивчення передових світових практик та підходів до організації стратегічних комунікацій, аналіз можливостей їх адаптації до специфічних умов України як держави, що перебуває в епіцентрі гібридної агресії.

Актуальність дослідження підсилюється стрімкою еволюцією інформаційних технологій, зокрема, появою генеративного штучного інтелекту, розширенням можливостей створення синтетичного медіа-контенту, розвитком технологій дипфейків та інших засобів маніпулювання інформаційним простором. Ці технологічні тренди створюють нові виклики для систем стратегічних комунікацій та вимагають розробки інноваційних підходів до формування комунікаційних стратегій, що враховували б як традиційні, так і новітні методи інформаційного впливу та протидії дезінформації.

Мета і завдання дослідження. Метою магістерської роботи є теоретичне обґрунтування та розробка практичних рекомендацій щодо формування ефективних комунікаційних стратегій в умовах гібридних загроз національній безпеці України.

Для досягнення поставленої мети визначено такі завдання:

- дослідити теоретичні та методологічні основи стратегічних комунікацій у контексті протидії гібридним загрозам;
- проаналізувати міжнародний досвід формування та реалізації комунікаційних стратегій в умовах гібридних конфліктів;
- охарактеризувати сучасні гібридні загрози для національної безпеки України з акцентом на їх інформаційну складову;
- оцінити стан та проблеми функціонування системи стратегічних комунікацій України;
- розробити комплексну модель формування комунікаційної стратегії протидії гібридним загрозам з урахуванням специфіки цільових аудиторій;
- запропонувати методику оцінки ефективності комунікаційних стратегій та практичні рекомендації щодо їх удосконалення в умовах України.

Об'єкт дослідження – процес формування та реалізації комунікаційних стратегій у системі забезпечення національної безпеки.

Предмет дослідження – теоретичні, методологічні та практичні аспекти розробки ефективних комунікаційних стратегій в умовах гібридних загроз національній безпеці України.

Методи дослідження. Теоретико-методологічну основу дослідження складає комплекс загальнонаукових та спеціальних методів. Системний підхід дав змогу розглянути стратегічні комунікації як цілісну систему в контексті забезпечення національної безпеки. За допомогою структурно-функціонального методу визначено роль і місце різних суб'єктів у системі стратегічних комунікацій України. Порівняльний метод застосовано при аналізі міжнародного досвіду формування комунікаційних стратегій. Методи контент-аналізу та дискурс-аналізу використано для дослідження наративів та меседжів, що поширюються в інформаційному просторі. Ситуаційний аналіз та метод кейс-стаді дозволили виявити характерні особливості гібридних загроз для України. Для розробки практичних рекомендацій застосовано методи моделювання та прогнозування.

Практичне значення отриманих результатів полягає в можливості їх використання державними органами для формування цілісної системи стратегічних комунікацій, розробки комунікаційних стратегій протидії гібридним загрозам, підвищення ефективності інформаційної політики держави. Рекомендації дослідження можуть бути використані в роботі Міністерства культури та інформаційної політики, Центру стратегічних комунікацій та інформаційної безпеки, підрозділів стратегічних комунікацій силових відомств, прес-служб органів державної влади, громадських організацій, що працюють у сфері протидії дезінформації. Матеріали дослідження також можуть стати корисними для навчальних закладів при підготовці фахівців у сфері публічного управління, національної безпеки, інформаційної політики та стратегічних комунікацій.

РОЗДІЛ 1

ТЕОРЕТИЧНІ ТА МЕТОДОЛОГІЧНІ ОСНОВИ СТРАТЕГІЧНИХ КОМУНІКАЦІЙ В УМОВАХ ГІБРИДНИХ ЗАГРОЗ

1.1 Концептуальні засади стратегічних комунікацій та гібридних загроз

Стратегічні комунікації як системна, цілеспрямована діяльність із формування та просування ключових наративів держави, координації комунікаційних зусиль та досягнення інформаційного впливу на цільові аудиторії, набувають особливого значення в умовах сучасних гібридних загроз. Для глибшого розуміння феномену стратегічних комунікацій та їхнього місця в системі національної безпеки необхідно детально розглянути сутність, структуру та еволюцію цього поняття.

Концепт стратегічних комунікацій пройшов значний шлях трансформації та розвитку. Первісно термін «стратегічні комунікації» з'явився у військовій сфері США на початку 2000-х років як відповідь на нові виклики глобалізованого інформаційного середовища та асиметричних конфліктів. Згодом він еволюціонував від суто військового інструменту до комплексного підходу, що охоплює всі аспекти взаємодії держави із внутрішніми та зовнішніми аудиторіями [12].

У сучасному розумінні стратегічні комунікації визначаються як скоординоване і належне використання комунікативних можливостей держави – публічної дипломатії, зв'язків із громадськістю, військових зв'язків, інформаційних та психологічних операцій, заходів, спрямованих на просування цілей держави [9]. Також їх можна розглядати як системну комунікативну діяльність, спрямовану на формування сприятливого внутрішнього та зовнішнього інформаційного середовища, що передбачає координацію

інформаційних потоків та узгодження повідомлень між різними суб'єктами відповідно до стратегічних цілей та національних інтересів [19].

У документах НАТО стратегічні комунікації трактуються як «скоординоване і належне використання комунікативних заходів та спроможностей Альянсу на підтримку політики, операцій та діяльності Альянсу для досягнення цілей НАТО» [48]. Це визначення підкреслює інструментальний характер стратегічних комунікацій, їхню підпорядкованість загальним стратегічним цілям організації та необхідність координації різних комунікативних активностей.

Основними характеристиками та принципами стратегічних комунікацій є:

- Стратегічний характер – підпорядкованість комунікацій загальним стратегічним цілям держави чи організації. Стратегічні комунікації не є самоціллю, вони інтегровані в загальну стратегію та служать інструментом досягнення довгострокових цілей.

- Системність та координованість – узгодження комунікативних зусиль різних суб'єктів (органів влади, інституцій, організацій) для досягнення спільної мети. Відсутність координації призводить до розбалансування комунікацій, суперечливості повідомлень та, як наслідок, до зниження довіри з боку цільових аудиторій [22].

- Наративний підхід – формування та просування ключових наративів, які відображають цінності, цілі та позицію держави. Наратив у стратегічних комунікаціях є не просто оповіддю, а цілісною світоглядною конструкцією, яка структурує реальність, надаючи їй певного сенсу.

- Мультиканальність та мультиінструментальність – використання різних каналів та інструментів комунікації (традиційних медіа, соціальних мереж, особистої комунікації тощо) для донесення повідомлень до цільових аудиторій.

- Цільовий підхід – орієнтація комунікацій на конкретні аудиторії з урахуванням їхніх особливостей, потреб та характеристик сприйняття інформації.

– Єдність слів та дій – узгодженість між тим, що комунікується, і реальними діями та політиками держави або організації. Розрив між словами та діями є найбільш деструктивним чинником, який підриває ефективність стратегічних комунікацій.

Структура системи стратегічних комунікацій є багатокomпонентною та включає різні функціональні елементи. До базових компонентів стратегічних комунікацій належать [30]:

– Публічна дипломатія – комплекс заходів, спрямованих на формування позитивного іміджу держави в міжнародному середовищі, взаємодію з іноземними аудиторіями та просування національних інтересів через інформаційно-комунікативні інструменти.

– Зв'язки з громадськістю (PR) – системна діяльність із побудови взаємовигідних відносин між організацією та громадськістю, формування позитивного іміджу та довіри до інституцій.

– Інформаційно-психологічні операції – цілеспрямовані заходи з впливу на свідомість та поведінку цільових аудиторій для досягнення певних стратегічних цілей.

– Військові комунікації – система заходів з інформування громадськості про діяльність військових структур, формування позитивного ставлення до них та підтримки військових операцій.

– Кризові комунікації – комплекс комунікативних заходів, спрямованих на мінімізацію негативного впливу кризових ситуацій на репутацію та функціонування держави чи організації.

– Громадські заходи та залучення – активності, спрямовані на безпосередню взаємодію з цільовими аудиторіями, формування спільнот та підтримку громадських ініціатив.

Роль стратегічних комунікацій у системі національної безпеки постійно зростає, особливо в умовах гібридних загроз, де інформаційний компонент стає одним із ключових елементів протистояння. Інформаційний простір перетворився на повноцінний театр військових дій, де перемоги та поразки

можуть мати не менш важливе значення, ніж на фізичному полі бою.

Ефективна система стратегічних комунікацій є не просто інструментом інформаційної політики, а складовою національної стійкості та безпеки [5]. Ключові функції стратегічних комунікацій у системі національної безпеки включають:

- Забезпечення суспільної підтримки державної політики у сфері безпеки та оборони.
- Протидія деструктивним інформаційним впливам та операціям ворожих сил.
- Формування та підтримка позитивного іміджу держави на міжнародній арені.
- Зміцнення національної єдності та соціальної згуртованості.
- Забезпечення інформаційної стійкості суспільства в умовах криз та конфліктів.
- Координація інформаційної діяльності різних державних органів та інституцій.

Значущість стратегічних комунікацій у системі національної безпеки підтверджується їх включенням до ключових стратегічних документів багатьох держав. Наприклад, у Стратегії національної безпеки України 2020 року стратегічні комунікації визначено як один із пріоритетних напрямів забезпечення національної безпеки [27]. Подібний підхід спостерігається і в стратегічних документах країн-членів НАТО, де комунікаційний компонент розглядається як невід’ємна складова системи безпеки та оборони.

Для розуміння контексту, в якому функціонують стратегічні комунікації в сучасному світі, необхідно проаналізувати сутність, типологію та характеристики гібридних загроз, які стали визначальним викликом для національної безпеки багатьох держав.

Поняття «гібридна загроза» та «гібридна війна» відносно нові в науковому дискурсі, хоча самі явища, які вони описують, мають глибокі історичні корені. Активне використання цих термінів почалося після російської агресії проти

України у 2014 році, хоча окремі елементи концепції гібридної війни розроблялися і раніше, зокрема в працях закордонних дослідників [51, 53].

За визначенням Гаазького центру стратегічних досліджень (HCSS), гібридні загрози – це «скоординоване використання різноманітних конвенційних та неконвенційних засобів та методів, які спрямовані на досягнення конкретних цілей, при одночасному уникненні формального порогу війни» [55]. Також гібридні загрози можна трактувати як комплекс різнорідних впливів на противника дипломатичними, військовими, економічними, політичними, інформаційними та іншими засобами для досягнення стратегічних цілей [20].

Основними характеристиками гібридних загроз є:

- Комплексність та синергетичність – використання комбінації різних інструментів впливу, які підсилюють один одного та створюють синергетичний ефект.
- Асиметричність – застосування нетрадиційних методів для компенсації нерівності в силах або ресурсах.
- Маскування та неочевидність – прагнення приховати реальні цілі та суб'єктів впливу, створення фасаду «природності» процесів, які насправді є спланованими операціями.
- Розмивання меж – стирання чітких кордонів між війною та миром, внутрішньою та зовнішньою політикою, державними та недержавними акторами.
- Гнучкість та адаптивність – швидке пристосування тактик та інструментів до мінливого середовища та реакцій противника.
- Таргетованість – орієнтація на конкретні вразливості противника, його «слабкі місця».
- Тривалість та поступовість – реалізація впливів протягом тривалого часу з поступовою ескалацією напруги.

Гібридні загрози можна класифікувати за сферами їх прояву [38]:

- Військові загрози – використання регулярних та нерегулярних збройних формувань, спеціальних операцій, підривної діяльності, тероризму.

- Політичні загрози – підрив легітимності державних інституцій, політична дестабілізація, формування проксі-сил та п'ятої колони.
- Економічні загрози – економічний тиск, санкції, блокади, енергетичний шантаж, корупційні схеми.
- Інформаційні загрози – пропаганда, дезінформація, маніпулювання громадською думкою, кібератаки.
- Соціальні загрози – загострення соціальних протиріч, розпалювання ворожнечі між різними групами населення.
- Культурно-ідентичні загрози – підрив національної ідентичності, нав'язування чужих ціннісних наративів, розмивання культурного коду.

Особливу роль у системі гібридних загроз відіграє інформаційна складова, яка часто виступає не лише як окремий напрям впливу, але і як об'єднуючий елемент для інших компонентів гібридної агресії. Інформаційний компонент є наскрізним для всіх елементів гібридної війни, він забезпечує їх легітимізацію, формує сприятливий контекст для реалізації інших впливів [23].

Інформаційна складова гібридної війни включає широкий спектр інструментів та методів впливу на свідомість, громадську думку та інформаційний простір у цілому. Серед ключових елементів інформаційного впливу в контексті гібридних загроз особливе місце займають пропаганда, дезінформація та різноманітні форми інформаційно-психологічних маніпуляцій.

Пропаганда представляє собою систематичну діяльність, спрямовану на поширення певних ідей, поглядів, цінностей з метою формування бажаних установок, переконань та моделей поведінки у цільових аудиторій [24]. Сучасна пропаганда характеризується використанням витончених психологічних технік, мультимедійних форматів та таргетованого підходу до різних аудиторій.

Основні типи пропаганди, які використовуються в контексті гібридних загроз [3]:

- Біла пропаганда – відкрите поширення ідей та повідомлень з чітко ідентифікованого джерела.
- Сіра пропаганда – поширення інформації з невизначеним або

прихованим джерелом, де складно встановити достовірність повідомлень.

- Чорна пропаганда – навмисне поширення неправдивої інформації від імені третьої сторони, часто противника.
- Стратегічна пропаганда – комплексні довгострокові кампанії, спрямовані на формування певного світогляду або системи цінностей.
- Тактична пропаганда – короткострокові інформаційні кампанії для досягнення конкретних оперативних цілей.

Дезінформація є одним із ключових інструментів гібридної війни і представляє собою навмисне поширення неправдивої або спотвореної інформації з метою введення в оману цільових аудиторій [16]. На відміну від пропаганди, яка може використовувати й правдиву інформацію, дезінформація базується на свідомому поширенні неправди.

У сучасному інформаційному середовищі дезінформація набуває різних форм та проявів. Це можуть бути фейкові новини, маніпулятивно відредаговані фото- та відеоматеріали, підроблені документи, фальшиві акаунти та боти в соціальних мережах, фабрикація «експертних» оцінок тощо. Основною метою дезінформації є підриг довіри, створення атмосфери непевності та сумніву, формування хибних уявлень та переконань, які в подальшому впливатимуть на поведінку та рішення цільових аудиторій.

Інформаційно-психологічні маніпуляції охоплюють широкий спектр технік та прийомів, спрямованих на управління сприйняттям, емоціями, переконаннями та поведінкою цільових аудиторій. На відміну від прямої пропаганди чи дезінформації, маніпуляції часто мають більш витончений характер, використовують складні психологічні механізми та спираються на особливості когнітивних процесів людини.

Серед найпоширеніших маніпулятивних технік, які застосовуються в гібридній війні, можна виділити [7]:

- Формування порядку денного – контроль над тим, які теми та питання потрапляють у фокус суспільної уваги, а які залишаються на периферії або взагалі випадають з інформаційного поля.

- Фреймінг – створення певних рамок інтерпретації подій, фактів, явищ, які визначають, як цільова аудиторія сприйматиме та оцінюватиме інформацію.
- Прайминг – підготовка аудиторії до сприйняття певної інформації через попереднє активування відповідних асоціацій, стереотипів, емоцій.
- Емоційне зараження – поширення певних емоційних станів (страху, гніву, ворожості, ентузіазму тощо) через інформаційні канали.
- Використання когнітивних упереджень – експлуатація природних особливостей мислення людини для досягнення маніпулятивних цілей.

Технології інформаційного впливу постійно еволюціонують, пристосовуючись до нових умов та викликів. Особливої актуальності набувають проблеми, пов'язані з розвитком цифрових платформ та соціальних мереж, які стали ключовими каналами поширення інформації та формування громадської думки. Соціальні мережі створюють сприятливе середовище для таргетованих інформаційних операцій, оскільки дозволяють точно виділяти цільові аудиторії, аналізувати їхні преференції та адаптувати контент відповідно до їхніх особливостей [33].

Важливим аспектом сучасної інформаційної війни є також використання технологій штучного інтелекту, зокрема, для створення «дипфейків» – синтетичного аудіо- та відеоконтенту, який важко відрізнити від автентичного. Ці технології дозволяють створювати фальшиві, але переконливі відеозаписи, де публічні особи нібито говорять або роблять те, чого насправді не було, що створює нові серйозні виклики для інформаційної безпеки та системи стратегічних комунікацій [31].

У відповідь на зростаючі загрози в інформаційній сфері розробляються різноманітні теоретичні моделі та практичні підходи до протидії деструктивним інформаційним впливам. Ці моделі враховують багатовимірний характер інформаційних загроз та передбачають комплексне застосування різних інструментів та методів протидії.

Одним із ключових підходів до протидії інформаційним впливам є модель

стратегічної стійкості, яка фокусується на формуванні здатності держави та суспільства протистояти інформаційним атакам, адаптуватися до них та швидко відновлюватися після них. Ця модель передбачає розвиток інституційних, технологічних, когнітивних та соціальних механізмів стійкості, які дозволяють мінімізувати негативний вплив дезінформації та пропаганди на суспільство [18].

Інша поширена модель – проактивний підхід (*proactive approach*), який базується на принципі, що краща оборона – це напад. Відповідно до цього підходу, найефективнішою стратегією протидії інформаційним впливам є не реактивне спростування дезінформації, а формування власного сильного наративу, контроль над порядком денним та інформаційним простором, а також превентивне викриття потенційних інформаційних атак [13].

Модель медіаграмотності зосереджується на розвитку критичного мислення та навичок аналізу інформації серед населення. Ця модель передбачає систематичну освітню та просвітницьку діяльність, спрямовану на підвищення здатності громадян розпізнавати дезінформацію, пропаганду та маніпуляції, верифікувати інформацію та критично оцінювати джерела [15].

Технологічна модель акцентує увагу на використанні сучасних цифрових технологій для виявлення, моніторингу та протидії інформаційним загрозам. Ця модель включає розробку та впровадження систем автоматизованого виявлення дезінформації, аналізу контенту, відстеження ботів та фейкових акаунтів, а також інших технологічних рішень для захисту інформаційного простору [35].

Інтегрована модель стратегічних комунікацій (*integrated strategic communications model*) пропонує комплексний підхід, який об'єднує всі комунікативні ресурси та канали держави для формування єдиної, узгодженої системи протидії інформаційним загрозам. Ця модель передбачає координацію зусиль різних державних та недержавних акторів, узгодження наративів та повідомлень, синхронізацію комунікативних дій з реальними політичними, економічними та військовими заходами [26].

Кожна з цих моделей має свої переваги та обмеження, і на практиці найчастіше використовується їх комбінація, адаптована до конкретних умов та

викликів, з якими стикається держава. Важливим аспектом ефективної протидії інформаційним впливам є також міжнародна співпраця, обмін досвідом та координація зусиль різних країн та організацій, особливо в умовах транснаціонального характеру сучасних інформаційних загроз.

Теоретичні моделі та концепції стратегічних комунікацій та протидії гібридним загрозам активно розвиваються та вдосконалюються, відображаючи динамічний характер сучасного інформаційного середовища та постійну еволюцію технологій та методів інформаційного впливу. Розуміння цих концептуальних засад є необхідною передумовою для розробки ефективних практичних підходів до формування комунікаційних стратегій в умовах гібридних загроз.

1.2 Міжнародний досвід формування комунікаційних стратегій

Розробка та впровадження ефективних комунікаційних стратегій у контексті протидії гібридним загрозам є актуальним завданням для багатьох країн та міжнародних організацій. Вивчення передового міжнародного досвіду в цій сфері дозволяє виявити найкращі практики, інноваційні підходи та перевірені часом рішення, які можуть бути адаптовані до українських реалій.

Особливої уваги заслуговує досвід НАТО, який упродовж останніх років активно розвиває власну систему стратегічних комунікацій у відповідь на зростаючі гібридні загрози. Організація Північноатлантичного договору розглядає стратегічні комунікації як ключовий елемент своєї діяльності, що інтегрується в усі аспекти політики та операцій Альянсу.

Доктринальною основою стратегічних комунікацій НАТО є низка документів, серед яких ключове місце займає «Військова концепція стратегічних комунікацій НАТО» (NATO Military Concept for Strategic Communications), затверджена у 2010 році. Цей документ визначає стратегічні комунікації як

«скоординоване та належне використання комунікативних заходів та спроможностей НАТО – публічної дипломатії, зв'язків із громадськістю, військових зв'язків із громадськістю, інформаційних та психологічних операцій – на підтримку політики, операцій та діяльності Альянсу для просування цілей НАТО» [52].

Іншим важливим документом є «Політика НАТО щодо стратегічних комунікацій» (NATO Strategic Communications Policy), яка встановлює загальні принципи та підходи до організації стратегічних комунікацій на рівні Альянсу. Згідно з цим документом, ефективні стратегічні комунікації повинні базуватися на таких принципах, як правдивість та точність інформації, узгодженість наративів із діями, відповідність цільовим аудиторіям, своєчасність комунікацій та їхня інтеграція в усі аспекти діяльності [48].

В інституційному плані система стратегічних комунікацій НАТО включає низку структур та механізмів, які забезпечують координацію комунікативних зусиль різних підрозділів Альянсу. На найвищому рівні функціонує Комітет зі стратегічних комунікацій (Strategic Communications Committee), який відповідає за формування загальної політики та стратегії комунікацій. На оперативному рівні діє Центр координації стратегічних комунікацій (Strategic Communications Coordination Centre), який забезпечує узгодження комунікативних активностей різних підрозділів НАТО [44].

Важливу роль у розвитку спроможностей Альянсу у сфері стратегічних комунікацій відіграє Центр передового досвіду НАТО зі стратегічних комунікацій (NATO Strategic Communications Centre of Excellence, NATO StratCom COE), створений у 2014 році в Ризі. Центр займається дослідженням сучасних тенденцій та викликів у сфері стратегічних комунікацій, розробкою доктрин та концепцій, навчанням та підготовкою фахівців, а також наданням експертної підтримки державам-членам Альянсу [50].

Практичний досвід НАТО у сфері стратегічних комунікацій формується через реалізацію різноманітних комунікативних заходів та кампаній, спрямованих на підтримку операцій Альянсу, протидію дезінформації,

формування позитивного іміджу організації та зміцнення суспільної підтримки. Особливої інтенсивності ці зусилля набули після 2014 року, коли НАТО зіткнулася з новими викликами, пов'язаними з російською агресією проти України та активізацією гібридних загроз.

Одним із прикладів успішної комунікаційної кампанії НАТО стала інформаційна підтримка операції «Resolute Support» в Афганістані, яка включала комплекс заходів із роз'яснення цілей та завдань місії, взаємодії з місцевим населенням, протидії пропаганді екстремістських груп. Кампанія базувалася на ретельному аналізі цільових аудиторій, формуванні ключових наративів та повідомлень, використанні різних комунікаційних каналів – від традиційних медіа до соціальних мереж та особистих контактів [46].

Іншим важливим напрямом діяльності НАТО у сфері стратегічних комунікацій є протидія дезінформації та фейкам. Для цього в структурі Альянсу створено спеціальні підрозділи, які займаються моніторингом інформаційного простору, виявленням неправдивих повідомлень та розробкою стратегій реагування. НАТО активно впроваджує принцип «pre-bunking» – превентивного спростування потенційних фейків та маніпуляцій, що дозволяє формувати стійкість аудиторії до дезінформації.

До найбільш ефективних практик НАТО у сфері стратегічних комунікацій належить також постійне вдосконалення методів роботи з соціальними мережами та цифровими платформами. Альянс активно використовує різні соціальні медіа для поширення офіційної інформації, взаємодії з аудиторіями, моніторингу суспільних настроїв та протидії дезінформації [42]. Особлива увага приділяється формуванню привабливого та інтерактивного контенту, який може конкурувати з матеріалами протилежної сторони за увагу аудиторії.

Важливим компонентом системи стратегічних комунікацій НАТО є також тісна співпраця з національними структурами держав-членів. Альянс надає методологічну, експертну та ресурсну підтримку країнам у розбудові їхніх власних спроможностей у сфері стратегічних комунікацій, сприяє обміну досвідом та кращими практиками між різними національними системами,

забезпечує координацію комунікативних зусиль на міжнародному рівні [47].

Поряд із загальними підходами НАТО, значний інтерес представляють також національні моделі та практики стратегічних комунікацій, розроблені та впроваджені окремими країнами відповідно до їхніх специфічних потреб та викликів.

Сполучені Штати Америки мають одну з найбільш розвинених систем стратегічних комунікацій у світі. У структурі органів державної влади США існує розгалужена мережа інституцій та підрозділів, відповідальних за різні аспекти комунікаційної діяльності. Ключову роль відіграє Державний департамент, де функціонує Центр глобальної взаємодії (Global Engagement Center, GEC), створений у 2016 році для координації зусиль уряду США з протидії іноземній дезінформації та пропаганді [56].

У військовій сфері стратегічні комунікації США базуються на концепції інформаційних операцій (Information Operations), яка передбачає інтеграцію різних інформаційних можливостей та активностей для впливу на процес прийняття рішень противника. Важливим елементом американського підходу є також тісна співпраця між урядовими структурами та приватним сектором, зокрема технологічними компаніями, у розробці та впровадженні інноваційних рішень для протидії інформаційним загрозам [43].

Особливістю американської моделі стратегічних комунікацій є також значна увага до розвитку публічної дипломатії та «м'якої сили» як інструментів формування сприятливого міжнародного середовища. США активно використовують культурні, освітні, наукові та інформаційні програми для просування своїх цінностей та інтересів у світі, формування позитивного іміджу країни та протидії негативним наративам [41].

Велика Британія також має значний досвід у сфері стратегічних комунікацій, який формувався протягом тривалого часу і ввібрав у себе кращі практики британської дипломатії, розвідки та військової справи. У структурі уряду Великої Британії функціонує Урядова комунікаційна служба (Government Communication Service, GCS), яка відповідає за координацію комунікативної

діяльності різних міністерств та відомств, розробку єдиних стандартів та підходів до комунікацій [39].

Значну роль у системі стратегічних комунікацій Великої Британії відіграє також Міністерство оборони, де створено спеціалізовані підрозділи для планування та реалізації комунікативних заходів у військовій сфері. Зокрема, 77-а бригада британської армії спеціалізується на веденні інформаційних операцій, протидії дезінформації та використанні соціальних мереж у військових цілях [45].

Важливим елементом британського підходу до стратегічних комунікацій є також тісна співпраця з громадським сектором та експертним середовищем. Уряд активно залучає незалежних дослідників, аналітичні центри та неурядові організації до розробки та реалізації комунікативних стратегій, проведення досліджень та моніторингу інформаційного простору [40].

Польща, як країна, що безпосередньо межує з Україною та Росією, приділяє особливу увагу розвитку системи стратегічних комунікацій для протидії гібридним загрозам. У структурі польського уряду функціонує Рада з національної безпеки (Rada Bezpieczeństwa Narodowego), яка координує діяльність різних державних органів у сфері безпеки, включаючи інформаційну безпеку та стратегічні комунікації [36].

Польща активно розвиває спроможності з моніторингу інформаційного простору та раннього виявлення дезінформації. Для цього створено спеціалізовані підрозділи в структурі розвідувальних та контррозвідувальних органів, а також налагоджено співпрацю з громадськими організаціями та незалежними ініціативами з факт-чекінгу [6].

Особливістю польського підходу до стратегічних комунікацій є також активна робота з діаспорою та сусідніми країнами для формування єдиного фронту протидії інформаційним загрозам. Польща ініціювала створення регіональних платформ співпраці у сфері інформаційної безпеки, зокрема в рамках Вишеградської групи та формату Бухарест 9 [32].

Країни Балтії та Скандинавії, які також перебувають під значним

інформаційним тиском з боку Росії, розробили унікальні та ефективні моделі протидії гібридним загрозам, які становлять значний інтерес для України.

Естонія, яка у 2007 році стала однією з перших країн, що зазнала масштабної кібератаки, приділяє особливу увагу розвитку цифрової стійкості та кіберзахисту. У країні створено Центр кіберзахисту НАТО (NATO Cooperative Cyber Defence Centre of Excellence), який проводить дослідження, тренінги та навчання у сфері кібербезпеки та інформаційної протидії [54].

Естонський підхід до стратегічних комунікацій базується на концепції цифрової стійкості, яка передбачає формування здатності суспільства протистояти інформаційним та кібератакам через розвиток критичного мислення, медіаграмотності та технологічної обізнаності. Естонія є однією з перших країн, яка впровадила системні програми з медіаграмотності в освітній процес, починаючи з початкової школи [28].

Латвія, яка виступила ініціатором створення Центру передового досвіду НАТО зі стратегічних комунікацій, розвиває комплексний підхід до інформаційної безпеки, який поєднує державні та громадські ініціативи. У структурі латвійського уряду функціонує Департамент стратегічних комунікацій, який координує комунікативну діяльність різних міністерств та відомств, розробляє єдині стандарти та підходи до комунікацій [49].

Латвійський досвід цінний також розвитком механізмів співпраці з медіа та громадянським суспільством у протидії дезінформації. У країні діють програми підтримки незалежних медіа, розвитку якісної журналістики, навчання та підготовки фахівців у сфері стратегічних комунікацій [10].

Литва активно розвиває стратегічні комунікації у військовій сфері, зокрема через впровадження концепції тотальної оборони, яка передбачає залучення всього суспільства до протидії гібридним загрозам. У структурі Міністерства оборони Литви створено спеціалізований підрозділ зі стратегічних комунікацій, який розробляє та впроваджує комунікативні стратегії для підтримки обороноздатності країни [2].

Фінляндія, яка також має тривалу історію протистояння інформаційному

впливу зі Сходу, розробила модель стійкості суспільства, яка базується на високому рівні довіри між владою та громадянами, розвиненій системі громадської освіти та критичному мисленні. Фінляндія регулярно проводить національні навчання та тренування з протидії гібридним загрозам, до яких залучаються як державні органи, так і приватний сектор та громадськість [14].

У Фінляндії також функціонує Європейський центр протидії гібридним загрозам (European Centre of Excellence for Countering Hybrid Threats), створений у 2017 році для координації зусиль європейських країн у протидії гібридним загрозам, проведення досліджень та розробки спільних підходів до стратегічних комунікацій [37].

Швеція також має розвинену систему стратегічних комунікацій, яка базується на принципах прозорості, довіри та відкритого діалогу. У структурі шведського уряду функціонує Агентство психологічного захисту (Psychological Defence Agency), створене у 2022 році для координації зусиль з протидії іноземному інформаційному впливу та дезінформації [57].

Шведський підхід до стратегічних комунікацій включає також активну роботу з громадянським суспільством та медіа для формування стійкості до інформаційних загроз. У країні діють програми підтримки якісної журналістики, розвитку медіаграмотності, навчання та підготовки фахівців у сфері комунікацій [4].

Значний внесок у розвиток міжнародних підходів до стратегічних комунікацій роблять спеціалізовані центри передового досвіду, які працюють над дослідженням сучасних тенденцій, розробкою нових концепцій та методик, навчанням фахівців та обміном кращими практиками.

Центр передового досвіду НАТО зі стратегічних комунікацій (NATO StratCom COE) у Ризі є провідною міжнародною інституцією у цій сфері. Центр проводить дослідження різних аспектів стратегічних комунікацій, розробляє доктринальні документи та методики, організовує тренінги та навчання для фахівців з країн-членів НАТО та партнерів Альянсу, проводить конференції та семінари для обміну досвідом [50].

Важливим напрямом діяльності NATO StratCom COE є також моніторинг та аналіз інформаційного простору, виявлення тенденцій та паттернів у використанні дезінформації та пропаганди, розробка рекомендацій щодо протидії інформаційним загрозам. Центр регулярно публікує аналітичні звіти та дослідження, які становлять значний інтерес для фахівців з різних країн, включаючи Україну [11].

Європейський центр протидії гібридним загрозам (European Centre of Excellence for Countering Hybrid Threats) у Гельсінкі спеціалізується на розробці комплексних підходів до протидії гібридним загрозам, включаючи їхню інформаційну складову. Центр працює над розвитком концепцій та методик протидії гібридним впливам, проводить дослідження та тренінги, сприяє обміну інформацією та координації зусиль між європейськими країнами [37].

Центр передового досвіду НАТО з кіберзахисту (NATO Cooperative Cyber Defence Centre of Excellence) у Таллінні фокусується на питаннях кібербезпеки та інформаційної протидії в цифровому просторі. Центр розробляє концепції та підходи до захисту інформаційної інфраструктури, протидії кібератакам та інформаційним операціям у цифровому середовищі, проводить тренінги та навчання для фахівців з різних країн [54].

Загалом міжнародний досвід демонструє різноманітність підходів та моделей стратегічних комунікацій, які формуються з урахуванням специфічних умов та викликів, з якими стикаються різні країни та організації. Водночас можна виділити низку спільних тенденцій та принципів, які характеризують сучасний стан розвитку стратегічних комунікацій у світі:

- Інтеграція стратегічних комунікацій у загальну систему національної безпеки та оборони, їхнє включення до стратегічних документів та планів.
- Розвиток інституційної спроможності через створення спеціалізованих органів та підрозділів, відповідальних за координацію комунікативної діяльності на різних рівнях.
- Акцент на формуванні суспільної стійкості до інформаційних впливів через розвиток критичного мислення, медіаграмотності та

інформаційної культури.

- Проактивний підхід до протидії дезінформації, який передбачає не лише реагування на фейки, а й формування власних сильних наративів та контроль над порядком денним.

- Тісна співпраця між державним та недержавним секторами, залучення громадянського суспільства, медіа, експертного середовища до розробки та реалізації комунікативних стратегій.

- Використання інноваційних технологій та рішень для моніторингу інформаційного простору, виявлення дезінформації, аналізу аудиторій та оцінки ефективності комунікацій.

- Міжнародна співпраця та координація зусиль у протидії транснаціональним інформаційним загрозам, обмін досвідом та кращими практиками між різними країнами та організаціями.

Для України, яка перебуває в епіцентрі гібридної агресії і стикається з безпрецедентними інформаційними викликами, адаптація кращих світових практик у сфері стратегічних комунікацій є одним із ключових завдань. Вивчення та творче переосмислення міжнародного досвіду дозволяє не лише уникнути повторення помилок, а й розробити власну ефективну модель стратегічних комунікацій, яка враховуватиме специфіку українських умов та викликів.

Серед підходів та практик, які можуть бути адаптовані до українського контексту, варто виділити:

1. Формування єдиної інституційної архітектури стратегічних комунікацій з чітким розподілом повноважень та механізмами координації між різними суб'єктами, за прикладом систем, впроваджених у США, Великій Британії та країнах Балтії.

2. Розвиток спроможностей з моніторингу інформаційного простору та раннього виявлення дезінформації, використовуючи досвід Латвії, Литви та Естонії.

3. Впровадження системних програм з медіаграмотності та

інформаційної культури за фінським та естонським зразком.

4. Розбудова механізмів взаємодії з громадянським суспільством, медіа та експертним середовищем у протидії інформаційним загрозам, використовуючи досвід Швеції та Фінляндії.

5. Розвиток проактивних підходів до формування та просування стратегічних наративів, за прикладом НАТО та США.

6. Використання інноваційних технологій та рішень для аналізу інформаційного простору та оцінки ефективності комунікацій, спираючись на практики, розроблені провідними центрами передового досвіду.

7. Поглиблення міжнародної співпраці у сфері стратегічних комунікацій, зокрема, через участь у діяльності міжнародних центрів передового досвіду, обмін фахівцями, проведення спільних навчань та тренувань.

Водночас, важливо усвідомлювати, що пряме копіювання зарубіжних моделей та підходів без урахування українських реалій може бути неефективним. Україна має специфічні виклики та умови, які вимагають розробки унікальних рішень та підходів. Зокрема, варто враховувати такі фактори, як високий рівень інформаційного протистояння, мовні та культурні особливості, наявність окупованих територій, значний вплив історичних наративів на сучасні комунікації тощо.

Отже, міжнародний досвід формування комунікаційних стратегій у контексті протидії гібридним загрозам представляє значний інтерес для України і може бути використаний для розвитку вітчизняної системи стратегічних комунікацій. Творча адаптація кращих світових практик з урахуванням специфіки українських умов та викликів дозволить розробити ефективні підходи та механізми протидії інформаційним загрозам, зміцнення національної стійкості та забезпечення інформаційної безпеки держави.

РОЗДІЛ 2

АНАЛІЗ ГІБРИДНИХ ЗАГРОЗ ТА КОМУНІКАЦІЙНОЇ ПОЛІТИКИ УКРАЇНИ

2.1 Характеристика гібридних загроз для національної безпеки України

Україна з 2014 року перебуває в епіцентрі безпрецедентної за масштабами та інтенсивністю гібридної агресії з боку Російської Федерації. Російсько-українське протистояння стало своєрідним полігоном для випробування та вдосконалення широкого спектру гібридних інструментів впливу, від традиційних військових операцій до витончених інформаційно-психологічних маніпуляцій. Аналіз характеру та специфіки гібридних загроз, з якими стикається Україна, є необхідною передумовою для розробки ефективних стратегій протидії та формування комплексної системи національної стійкості.

Російська гібридна агресія проти України є класичним прикладом сучасного гібридного конфлікту, який поєднує військові та невійськові інструменти впливу, розмиває межі між війною та миром, використовує асиметричні тактики та спрямований на досягнення стратегічних цілей агресора без відкритого оголошення війни. Починаючи з анексії Криму та розпалювання сепаратизму на Сході України у 2014 році і до повномасштабного вторгнення у лютому 2022 року, Росія послідовно реалізовувала комплексну стратегію гібридної війни, спрямовану на підірив суверенітету, територіальної цілісності та незалежності України [5].

Військова складова російської гібридної агресії включає використання як регулярних збройних сил, так і нерегулярних формувань, приватних військових компаній, найманців та місцевих колаборантів. Характерними рисами військових операцій РФ проти України в свій час були:

- Маскування власної участі через використання «зелених чоловічків» без розпізнавальних знаків (Крим, 2014) або підтримку псевдо-республік на Донбасі (2014-2022).

- Поєднання конвенційних та неконвенційних методів ведення бойових дій.

- Використання проксі-сил та маріонеткових режимів для створення буферних зон та ведення «війни чужими руками».

- Застосування терористичних тактик, включаючи захоплення заручників, обстріли цивільної інфраструктури, мінування територій.

- Використання енергетичної інфраструктури як зброї (атаки на АЕС, ГЕС, ГРЕС).

Політична складова гібридної агресії спрямована на підрив легітимності української влади, дестабілізацію політичної системи, посилення внутрішніх протиріч та розколів у суспільстві. Серед ключових інструментів політичного впливу РФ на Україну можна виділити:

- Підтримка проросійських політичних сил, створення «п'ятої колони» в органах влади та управління.

- Штучне загострення мовних, релігійних, регіональних відмінностей для поляризації суспільства.

- Делегітимізація демократичних інститутів та процедур, зокрема виборів.

- Формування сепаратистських настроїв та створення псевдо-державних утворень на окупованих територіях.

- Використання корупції як інструменту впливу на прийняття політичних рішень [20].

Економічна складова гібридної агресії включає широкий спектр інструментів тиску, спрямованих на підрив економічної стабільності України, створення залежності від російського ринку та ресурсів, обмеження можливостей для інтеграції в європейський економічний простір. Серед ключових економічних важелів гібридного впливу РФ за час незалежності

України варто відзначити:

- Енергетичний шантаж через маніпулювання цінами на газ, нафту та інші енергоносії.
- Торговельні обмеження та блокади, включаючи заборону імпорту українських товарів.
- Атаки на критичну інфраструктуру, включаючи енергетичну, транспортну, фінансову системи.
- Економічну дестабілізацію через створення штучних кризових ситуацій.
- Блокування морських портів та обмеження свободи судноплавства в Чорному та Азовському морях.

Соціокультурна складова гібридної агресії орієнтована на підрив національної ідентичності українців, нав'язування проросійських наративів та цінностей, створення штучних ліній розколу в суспільстві. Ця складова реалізується через:

- Просування концепції «русского мира» як альтернативи українській національній ідентичності.
- Маніпулювання історичною пам'яттю, зокрема, щодо Другої світової війни, Голодомору, радянського періоду.
- Використання релігійного чинника, зокрема, через діяльність УПЦ МП.
- Нав'язування російської мови та культури як «природних» для українців.
- Формування відчуття меншовартості української культури, мови, ідентичності [38].

Особливу роль у гібридній агресії РФ проти України відіграє інформаційна складова, яка не лише є окремим напрямом впливу, але й забезпечує координацію та ефективність інших компонентів гібридної війни. Інформаційні операції Росії проти України характеризуються безпрецедентними масштабами, інтенсивністю та різноманітністю використовуваних інструментів і тактик [8].

Аналіз інформаційних операцій РФ проти України дозволяє виділити кілька ключових наративів, які систематично просуваються через різні канали комунікації:

1. Наратив «штучності» української державності та нації. Ключова ідея цього наративу полягає в тому, що Україна – це «штучне утворення», «недодержава», яка не має власної історичної, культурної та політичної суб'єктності. Відповідно, українці не є окремою нацією, а представляють собою частину «триєдиного російського народу». Цей наратив активно просувався на найвищому державному рівні РФ, зокрема, у відомій статті В. Путіна «Про історичну єдність росіян та українців» та його промові від 21 лютого 2022 року перед повномасштабним вторгненням [25].

2. Наратив «нацистської України». Цей наратив спрямований на демонізацію української влади та патріотичних сил через їх позиціонування як «нацистів», «фашистів», «бандерівців». Використовується маніпулятивне поєднання символів та подій Другої світової війни із сучасним українським національним рухом, акцентуація на діяльності праворадикальних груп (реальних чи вигаданих) для формування образу України як держави, де «панує нацизм» і яка «загрожує російськомовному населенню». Цей наратив активно використовувався для виправдання анексії Криму, війни на Донбасі та повномасштабного вторгнення 2022 року під гаслом «денацифікації» України [7].

3. Наратив «зовнішнього управління» Україною. Згідно з цим наративом, Україна не є по-справжньому незалежною державою, а перебуває під зовнішнім управлінням США, НАТО, ЄС або «світової закуліси». Українська влада зображується як «маріонетки Заходу», які діють в інтересах іноземних держав, а не власного народу. Цей наратив спрямований на підрив легітимності української влади, створення образу України як несамоостійного геополітичного актора та формування антизахідних настроїв в українському суспільстві [33].

4. Наратив «громадянської війни» в Україні. Цей наратив спрямований на заперечення російської агресії та представлення конфлікту на Сході України

як внутрішнього протистояння між різними групами українського суспільства. Згідно з цим наративом, на Донбасі відбувається не російсько-українська війна, а «громадянський конфлікт» або «внутрішньоукраїнське протистояння», в якому Росія виступає лише як миротворець або посередник. Цей наратив активно просувався російською пропагандою з 2014 року і був спрямований на зняття з РФ відповідальності за агресію.

5. Наратив «загрози з боку НАТО». Цей наратив представляє розширення НАТО на схід та євроатлантичні прагнення України як екзистенційну загрозу для безпеки Росії. Відповідно до цього наративу, Україна є лише «плацдармом» для розміщення військових баз НАТО, які нібито будуть спрямовані проти Росії. Цей наратив використовувався для виправдання агресії проти України як «превентивного заходу» для захисту російських національних інтересів та безпеки [25].

6. Наратив «братніх народів». Цей наратив, на відміну від більш агресивних, апелює до спільної історії, культури, релігії росіян та українців, позиціонуючи їх як «братні народи», які мають бути разом. При цьому поняття «разом» трактується виключно як підпорядкування України російським інтересам та включення її в орбіту російського впливу. Цей наратив часто використовується в комбінації з наративом про «штучність» української державності, формуючи посил про «природність» об'єднання українців та росіян в єдиному державному утворенні під егідою Росії [23].

Для поширення цих та інших наративів Росія використовує різноманітні канали комунікації, спрямовані на різні цільові аудиторії як в Україні, так і за її межами:

1. Традиційні медіа. До повномасштабного вторгнення в Україні діяла розгалужена мережа проросійських телеканалів, газет, радіостанцій, які були інтегровані в загальну систему російської пропаганди. Після введення санкцій та обмежень діяльність багатьох з цих медіа була припинена, але частина з них продовжує функціонувати в інтернет-просторі або на окупованих територіях. Крім того, російські державні телеканали (Russia Today, Russia 1, Channel One)

активно транслюють пропагандистські наративи на міжнародну аудиторію.

2. Соціальні мережі та цифрові платформи. Росія активно використовує соціальні мережі для поширення дезінформації та пропаганди, створюючи мережі ботів, тролів, фейкових акаунтів, які масово тиражують потрібні наративи. Також використовуються методи таргетованої реклами для донесення повідомлень до конкретних аудиторій. Особлива увага приділяється платформам, які мають глобальне охоплення – Facebook, Instagram, X, YouTube, Telegram.

3. Проксі-канали. Для маскуванню походження інформації та підвищення її довіри Росія часто використовує «проксі» – псевдонезалежні медіа, експертні центри, громадські організації, які насправді є інструментами російського впливу. Ці канали можуть видавати себе за об'єктивні джерела інформації, але насправді транслюють кремлівські наративи.

4. Дипломатичні та офіційні канали. Російські дипломати, офіційні представники, державні діячі активно просувають пропагандистські наративи через офіційні заяви, виступи, міжнародні форуми, використовуючи статус державних інституцій для надання легітимності своїм повідомленням.

5. Релігійні організації. Російська православна церква та пов'язані з нею релігійні структури в Україні використовуються як канал поширення проросійських наративів, особливо серед віруючих. Через проповіді, церковні медіа, публічні заяви ієрархів просувається ідея «духовної єдності» росіян та українців, критика європейських цінностей, підтримка концепції «русского мира».

Аналіз цільових аудиторій російських інформаційних операцій дозволяє виділити кілька ключових груп, на які спрямований вплив:

1. Внутрішня аудиторія в Україні. Російська пропаганда активно працює з різними сегментами українського суспільства, особливо з тими, які мають потенційну вразливість до проросійських наративів – мешканцями південних та східних регіонів, російськомовним населенням, старшою віковою групою, що має ностальгію за радянським минулим. Метою впливу на цю

аудиторію є створення розколів у суспільстві, підрив довіри до української влади, формування проросійських або принаймні антизахідних настроїв.

2. Населення окупованих територій. Ця аудиторія перебуває під тотальним інформаційним контролем РФ, і робота з нею спрямована на легітимізацію окупаційних адміністрацій, формування негативного ставлення до України, створення штучної «ідентичності» ОРДЛО або «Новоросії», виправдання російської агресії як «захисту від українських нацистів».

3. Російська внутрішня аудиторія. Інформаційні операції, спрямовані на власне населення РФ, мають на меті формування підтримки агресивної політики Кремля щодо України, виправдання військових дій та економічних витрат на війну, створення образу України як «ворожої держави», якою керують «нацисти» та «західні куратори».

4. Міжнародна аудиторія. Російська пропаганда активно працює з громадською думкою в країнах Заходу, намагаючись створити сприятливе для себе міжнародне середовище. Основні наративи для цієї аудиторії включають представлення України як «failed state», звинувачення України в порушеннях прав людини, корупції, відсутності реформ, просування ідеї про необхідність «врахування інтересів Росії» у вирішенні конфлікту.

5. Країни глобального півдня. Окремим напрямом російських інформаційних операцій є робота з країнами Африки, Азії, Латинської Америки, де РФ намагається позиціонувати себе як захисника від «західного колоніалізму» та «однополярного світу». В цьому контексті війна проти України подається як частина глобального протистояння з колективним Заходом.

Механізми впливу на суспільну свідомість та громадську думку, які використовує Росія в гібридній війні проти України, є різноманітними та комплексними. Вони включають:

1. Масована дезінформація. Поширення неправдивої або маніпулятивної інформації через різні канали з метою формування хибних уявлень про ситуацію в Україні, дії української влади, характер російсько-українського конфлікту. Дезінформація може набувати різних форм – від прямих

фейків до складних маніпуляцій з реальними фактами.

2. Операції впливу. Комплексні інформаційні кампанії, спрямовані на формування певних настроїв, переконань, моделей поведінки у цільових аудиторіях. Такі операції часто включають координоване використання різних каналів комунікації, поєднання онлайн та офлайн активностей, залучення впливових осіб (лідерів думок, експертів, політиків).

3. Інформаційні бульбашки. Створення замкнених інформаційних середовищ, де користувачі отримують лише певний тип контенту, що відповідає заданій наративній матриці. Це призводить до формування спотвореної картини реальності та посилення поляризації в суспільстві.

4. Психологічні операції. Цілеспрямовані заходи з впливу на психологічний стан цільових аудиторій – створення атмосфери страху, невпевненості, апатії, агресії тощо. Ці операції можуть включати залякування, дискредитацію опонентів, поширення чуток, провокації, психологічний тиск.

5. Маніпулювання історичною пам'яттю. Використання історичних подій, символів, травматичного досвіду для формування потрібних емоційних реакцій та ідеологічних установок. Зокрема, активно експлуатується тема Другої світової війни, радянського минулого, історичних відносин між Україною та Росією.

Особливу загрозу для національної безпеки України становлять кібератаки та операції в цифровому просторі, які є невід'ємною складовою російської гібридної агресії. Росія використовує широкий спектр кіберінструментів для досягнення своїх стратегічних цілей:

1. Атаки на критичну інфраструктуру. Зокрема, у грудні 2015 року російські хакери здійснили кібератаку на українські енергетичні компанії, що призвело до масштабного відключення електроенергії в кількох регіонах. Подібні атаки повторювалися і в наступні роки, зокрема, напередодні та під час повномасштабного вторгнення у 2022 році [19].

2. Хакерські атаки на державні установи та інформаційні системи. Метою таких атак є викрадення конфіденційної інформації, порушення

функціонування державних органів, дестабілізація ситуації. Наприклад, у січні 2022 року відбулася масштабна кібератака на українські урядові сайти, які були дефейснуті з розміщенням провокаційних повідомлень [34].

3. Операції в соціальних мережах. Російські спецслужби та пов'язані з ними групи активно використовують соціальні мережі для поширення дезінформації, маніпулювання громадською думкою, координації проросійських активістів. Для цього створюються мережі ботів, фейкових акаунтів, «фабрики тролів», які масово поширюють потрібні наративи.

4. Використання даркнету та месенджерів. Закриті канали комунікації, такі як Telegram-канали, чати в Discord, форуми в даркнеті, використовуються для координації дій проросійських груп, поширення забороненого контенту, організації провокацій та протестних акцій.

5. Атаки на медіа та інформаційні ресурси. DDOS-атаки, зламування сайтів, фішингові атаки на журналістів та редакції спрямовані на обмеження доступу українських громадян до достовірної інформації, особливо в періоди загострення ситуації або важливих політичних подій.

Вплив російської дезінформації на різні сегменти українського населення є неоднорідним і залежить від багатьох факторів – регіону проживання, віку, освіти, мовних преференцій, медіаспоживання тощо. Дослідження, проведені українськими та міжнародними організаціями, дозволяють виділити деякі закономірності у сприйнятті дезінформації різними групами населення:

1. Регіональний аспект. Традиційно більшу вразливість до проросійських наративів демонстрували мешканці південних та східних регіонів України, що пов'язано з історичними, культурними, мовними факторами, а також з інтенсивнішим впливом російських медіа в цих регіонах. Однак після 2014 року, і особливо після повномасштабного вторгнення 2022 року, спостерігається значне зменшення впливу російської пропаганди на ці регіони та консолідація українського суспільства [13].

2. Віковий аспект. Старші вікові групи (65+) часто демонструють більшу вразливість до проросійських наративів, що пов'язано з ностальгією за

радянським минулим, сформованими в радянський період світоглядними установками, меншою медіаграмотністю та обмеженим доступом до альтернативних джерел інформації. Молодша аудиторія (18-35) загалом менш сприйнятлива до російської пропаганди, має кращі навички критичного мислення та більш проєвропейські орієнтації [24].

3. Мовний аспект. Російськомовні громадяни в цілому виявляють більшу вразливість до проросійських наративів, особливо якщо вони є споживачами російського медіаконтенту. Це пов'язано не стільки з мовою як такою, скільки з культурним та інформаційним контекстом, в якому перебувають російськомовні українці. Однак після 2014 року, і особливо після 2022 року, спостерігається значне зниження кореляції між мовою спілкування та політичними преференціями [18].

4. Освітній аспект. Люди з вищою освітою загалом менш сприйнятливі до пропаганди та дезінформації, оскільки мають кращі навички критичного мислення, аналізу інформації, перевірки фактів. Однак освіта не є гарантією імунітету до дезінформації, особливо якщо вона супроводжується сильними ідеологічними переконаннями.

5. Медійний аспект. Споживачі різних типів медіа демонструють різну вразливість до дезінформації. Ті, хто отримує інформацію переважно з традиційних медіа (телебачення, радіо, газети), особливо з проросійських каналів, більш схильні вірити пропаганді. Користувачі інтернету та соціальних мереж мають доступ до більш різноманітних джерел інформації, але стикаються з іншими викликами – інформаційними бульбашками, алгоритмічною фільтрацією контенту, таргетованою дезінформацією.

Українська держава та суспільство демонструють високий рівень стійкості та адаптивності до гібридних загроз, особливо після початку повномасштабного вторгнення у 2022 році. Це проявляється в консолідації суспільства навколо спільних цінностей та цілей, зміцненні національної ідентичності, розвитку громадянського суспільства та волонтерського руху, підвищенні рівня медіаграмотності та критичного мислення громадян.

Однак, незважаючи на значний прогрес, залишаються вразливості та проблеми, які потребують системного вирішення. Зокрема, це недостатня координація дій різних державних органів у протидії гібридним загрозам, обмежені ресурси для розвитку спроможностей у сфері інформаційної безпеки, технологічне відставання в деяких аспектах кібербезпеки, вразливість критичної інфраструктури до атак, наявність «інформаційних бульбашок» та поляризація в суспільстві.

2.2 Система стратегічних комунікацій України: стан та проблеми

Система стратегічних комунікацій України почала формуватися як відповідь на гібридну агресію Російської Федерації, що розпочалася у 2014 році. До того часу в Україні не існувало цілісної системи координації комунікативної діяльності держави, і різні інституції діяли автономно, без єдиного стратегічного підходу та узгоджених наративів. Російська інформаційна агресія виявила критичні вразливості в інформаційному просторі України та спонукала до серйозного переосмислення підходів до організації комунікацій у сфері національної безпеки.

Аналіз інституційної архітектури стратегічних комунікацій України дозволяє виділити кілька ключових елементів, які формують загальну структуру цієї системи:

- Рада національної безпеки і оборони України (РНБО) відіграє важливу роль у координації діяльності органів виконавчої влади у сфері національної безпеки, включаючи інформаційну складову. В структурі РНБО функціонує Центр протидії дезінформації, створений у 2021 році відповідно до Указу Президента України. Центр відповідає за моніторинг інформаційного простору, виявлення дезінформації, координацію зусиль різних державних органів у протидії інформаційним загрозам. Також при РНБО діє Національний

координаційний центр кібербезпеки, який займається координацією діяльності у сфері кіберзахисту.

– Міністерство культури та інформаційної політики України (МКІП) є головним органом у системі центральних органів виконавчої влади, що формує та реалізує державну політику в інформаційній сфері. До сфери управління МКІП належить Центр стратегічних комунікацій та інформаційної безпеки, створений у 2021 році як державна установа. Центр відповідає за розробку та імплементацію стратегічних наративів, координацію комунікативної діяльності різних державних органів, протидію дезінформації, роботу з медіа та громадськістю.

– Міністерство закордонних справ України (МЗС) відповідає за стратегічні комунікації у сфері зовнішньої політики, формування та просування позитивного іміджу України на міжнародній арені, протидію російській дезінформації в іноземних медіа. В структурі МЗС діє Департамент комунікацій та публічної дипломатії, який координує комунікативну діяльність дипломатичних установ України за кордоном, взаємодію з іноземними медіа, реалізацію проєктів публічної дипломатії.

– Міністерство оборони України та Збройні Сили України розвивають власну систему стратегічних комунікацій, спрямовану на підтримку військових операцій, формування позитивного іміджу армії, протидію дезінформації у військовій сфері. В структурі Міноборони діє Директорат інформаційної політики у сфері оборони та стратегічних комунікацій, а в Генеральному штабі ЗСУ – Управління стратегічних комунікацій. Ці підрозділи відповідають за планування та реалізацію комунікативних заходів у сфері оборони, взаємодію з медіа та громадськістю, протидію дезінформації щодо діяльності ЗСУ.

– Служба безпеки України (СБУ) займається протидією інформаційним операціям спецслужб іноземних держав, виявленню та припиненню діяльності інформаційних ресурсів, які загрожують національній безпеці, розслідуванням кіберінцидентів та інформаційних атак. В структурі СБУ функціонує Департамент контррозвідувального захисту інтересів держави

у сфері інформаційної безпеки та Ситуаційний центр забезпечення кібербезпеки.

– Міністерство цифрової трансформації України відповідає за цифровізацію державного управління, розвиток електронних послуг, забезпечення технологічної складової інформаційної безпеки. В контексті стратегічних комунікацій Мінцифри займається розробкою та впровадженням технологічних рішень для протидії дезінформації, захисту цифрової інфраструктури, моніторингу інформаційного простору.

– Державна служба спеціального зв'язку та захисту інформації України (Держспецзв'язку) відповідає за захист державних інформаційних ресурсів, критичної інформаційної інфраструктури від кібератак, забезпечення функціонування захищених каналів комунікації для органів державної влади.

Важливу роль у системі стратегічних комунікацій України відіграють також недержавні актори – громадські організації, аналітичні центри, медіа, які співпрацюють з державними інституціями у протидії дезінформації, моніторингу інформаційного простору, розвитку медіаграмотності населення. Серед ключових недержавних організацій, активних у сфері стратегічних комунікацій, варто відзначити «Детектор медіа», «StopFake», Український кризовий медіа-центр, Центр протидії дезінформації VoxCheck, Інститут масової інформації та інші.

Нормативно-правове забезпечення стратегічних комунікацій в Україні формувалося поступово, відображаючи еволюцію підходів до розуміння сутності та ролі стратегічних комунікацій у системі національної безпеки. Ключовими документами, що регулюють цю сферу, є:

– Доктрина інформаційної безпеки України, затверджена Указом Президента України від 25 лютого 2017 року. Цей документ визначає національні інтереси України в інформаційній сфері, загрози інформаційній безпеці, пріоритети державної політики в інформаційній сфері, механізми реалізації цієї політики. Доктрина вперше на офіційному рівні ввела поняття стратегічних комунікацій та визначила їх як «скоординоване і належне використання комунікативних можливостей держави – публічної дипломатії,

зв'язків із громадськістю, військових зв'язків, інформаційних та психологічних операцій, заходів, спрямованих на просування цілей держави» [9].

– Стратегія національної безпеки України «Безпека людини – безпека країни», затверджена Указом Президента України від 14 вересня 2020 року. Цей документ визначає стратегічні комунікації як один із пріоритетних напрямів забезпечення національної безпеки, підкреслює необхідність розвитку спроможностей у сфері стратегічних комунікацій для протидії гібридним загрозам. Стратегія передбачає «забезпечення стратегічного контрнарративу, спрямованого на захист українського інформаційного простору від російської інформаційної експансії, який сприятиме формуванню стійкості суспільства до гібридних впливів» [27].

– Стратегія комунікації у сфері європейської інтеграції на 2018–2021 роки, схвалена розпорядженням Кабінету Міністрів України від 25 жовтня 2017 року. Цей документ визначав цілі, завдання, цільові аудиторії, ключові повідомлення та механізми комунікації щодо європейської інтеграції України. Хоча термін дії цієї Стратегії вже завершився, вона заклала важливі засади для розвитку системного підходу до стратегічних комунікацій в Україні [28].

– Концепція стратегічних комунікацій Міністерства оборони України та Збройних Сил України, затверджена наказом Міністерства оборони України від 22 листопада 2017 року. Цей документ визначає цілі, завдання, принципи та механізми стратегічних комунікацій у сфері оборони, регламентує взаємодію різних структурних підрозділів Міноборони та ЗСУ у комунікативній діяльності [6].

– Положення про Центр стратегічних комунікацій та інформаційної безпеки, затверджене наказом Міністерства культури та інформаційної політики України від 7 травня 2021 року. Цей документ визначає статус, функції та повноваження Центру, його роль у координації діяльності різних державних органів у сфері стратегічних комунікацій [25].

Незважаючи на значний прогрес у формуванні нормативно-правової бази стратегічних комунікацій, в Україні досі відсутній комплексний закон, який би

системно регулював цю сферу. Існуючі документи мають переважно концептуальний характер, визначаючи загальні принципи та підходи, але не створюють чіткого механізму координації та взаємодії різних суб'єктів стратегічних комунікацій, не встановлюють конкретні процедури та стандарти. Це створює певні правові прогалини та неузгодженості, які ускладнюють ефективне функціонування системи стратегічних комунікацій [13].

Координація комунікаційних зусиль між різними відомствами є одним із найбільш проблемних аспектів системи стратегічних комунікацій України. Незважаючи на створення координаційних механізмів, таких як Центр стратегічних комунікацій та інформаційної безпеки, Центр протидії дезінформації, міжвідомчі робочі групи, на практиці спостерігається недостатня узгодженість дій різних державних органів, дублювання функцій, розбіжності в підходах та повідомленнях.

Основними проблемами координації комунікаційних зусиль є:

- Відсутність єдиного центру прийняття рішень у сфері стратегічних комунікацій, який би мав достатні повноваження та ресурси для координації діяльності всіх суб'єктів. Існуючі координаційні механізми часто не мають реальних важелів впливу на інші державні органи, особливо на силові структури.
- Відомча замкненість та конкуренція між різними органами державної влади, які прагнуть зберегти автономність у своїй комунікативній діяльності, не бажають ділитися інформацією, конкурують за ресурси та увагу аудиторії.
- Різні підходи та стандарти до організації комунікативної діяльності в різних відомствах, відсутність єдиних методик, процедур, критеріїв оцінки ефективності. Це призводить до несумісності форматів, різного розуміння пріоритетів, неузгодженості дій.
- Відсутність ефективних механізмів обміну інформацією між різними суб'єктами стратегічних комунікацій. Інформація часто не передається своєчасно або передається неповно, що ускладнює формування адекватної картини ситуації та розробку узгоджених комунікативних заходів.

– Недостатня залученість недержавних акторів до системи стратегічних комунікацій. Попри значний потенціал громадських організацій, аналітичних центрів, незалежних медіа, їх взаємодія з державними органами часто має епізодичний, несистемний характер.

Після повномасштабного вторгнення Росії координація комунікаційних зусиль суттєво покращилася, особливо в контексті висвітлення ситуації на фронті, гуманітарних питань, міжнародної допомоги. Однак системні проблеми залишаються і потребують комплексного вирішення.

Аналіз державних наративів та їх ефективності є важливим аспектом оцінки системи стратегічних комунікацій України. Наративи, які формуються та просуваються державними інституціями, відображають загальне бачення ситуації, цінності, пріоритети, напрями розвитку країни і мають суттєвий вплив на формування громадської думки та прийняття рішень різними аудиторіями.

За результатами аналізу комунікативної діяльності українських державних органів можна виділити кілька ключових наративів, які активно просуваються через різні канали комунікації:

– Наратив «Україна як демократична європейська держава», який підкреслює цивілізаційний вибір України, її прагнення до інтеграції в ЄС та НАТО, відданість демократичним цінностям та принципам верховенства права. Цей наратив протиставляється російській пропаганді про «штучність» української державності та «нацистську» Україну.

– Наратив «Україна як жертва російської агресії», який акцентує увагу на незаконній анексії Криму, окупації частини Донбасу, повномасштабному вторгненні 2022 року, численних воєнних злочинах та порушеннях міжнародного права з боку РФ. Цей наратив спрямований на мобілізацію міжнародної підтримки, забезпечення єдності союзників, легітимізацію вимог щодо санкцій проти Росії та надання Україні військової допомоги.

– Наратив «українці як нація, що бореться за свободу», який підкреслює мужність, стійкість, волелюбність українського народу, його готовність боротися за свою незалежність та гідність. Цей наратив спирається на

історичні приклади української боротьби за свободу і є важливим елементом формування національної ідентичності та єдності.

- Наратив «Україна як щит Європи», який позиціонує Україну як захисника європейських цінностей та безпеки, форпост протистояння російській агресії, яка загрожує всьому демократичному світу. Цей наратив спрямований на зміцнення солідарності із західними партнерами, обґрунтування необхідності підтримки України як спільної справи всіх демократичних держав.

- Наратив «реформи в умовах війни», який підкреслює рішучість України продовжувати трансформаційні процеси навіть в умовах збройного конфлікту, її прагнення до модернізації державних інституцій, боротьби з корупцією, розвитку економіки. Цей наратив спрямований на зміцнення довіри міжнародних партнерів та інвесторів, обґрунтування необхідності фінансової та технічної допомоги.

Ефективність цих наративів варіюється залежно від цільової аудиторії, контексту, каналів комунікації, загальної ситуації. Загалом, державні наративи демонструють високу ефективність у консолідації українського суспільства, формуванні національної ідентичності та єдності, мобілізації міжнародної підтримки. Особливо це проявилось після повномасштабного вторгнення Росії у 2022 році, коли спостерігався безпрецедентний рівень національної згуртованості та міжнародної солідарності з Україною.

Водночас, аналіз ефективності державних наративів виявляє і певні проблеми та обмеження:

- Недостатня адаптованість наративів до різних цільових аудиторій. Часто використовується уніфікований підхід, який не враховує специфіку різних груп населення України (за віком, регіоном, мовою, політичними преференціями) та міжнародних аудиторій.

- Реактивність замість проактивності. Державні наративи часто формуються як реакція на російську пропаганду, а не як самостійна, проактивна комунікативна стратегія. Це призводить до того, що порядок денний фактично визначається російською стороною, а Україна змушена постійно

виправдовуватися та спростовувати фейки.

– Недостатня підкріпленість наративів конкретними діями та результатами. Наратив «реформи в умовах війни», наприклад, часто стикається з критикою через повільність реформ, корупційні скандали, неефективність деяких державних інституцій. Розрив між словами та діями підриває довіру до державних повідомлень.

– Фрагментованість та неузгодженість наративів між різними державними органами. Різні інституції можуть акцентувати різні аспекти, використовувати різну термінологію, по-різному розставляти пріоритети, що створює враження відсутності єдиної позиції держави.

– Недостатнє використання сучасних форматів та підходів до комунікації. Державні наративи часто подаються у традиційних форматах (офіційні заяви, прес-релізи, брифінги), які не завжди ефективні для роботи з молодістю аудиторією, соціальними мережами, нетрадиційними медіа.

Повномасштабне вторгнення Росії у лютому 2022 року поставило українську систему стратегічних комунікацій перед безпрецедентними викликами, але водночас стало потужним стимулом для її розвитку та вдосконалення. В умовах екзистенційної загрози для держави відбулася консолідація зусиль різних інституцій, активізувалася міжнародна співпраця, підвищилася ефективність координації. Українські державні органи продемонстрували здатність оперативно реагувати на інформаційні виклики, формувати та просувати ефективні наративи, протидіяти російській дезінформації в умовах активних бойових дій.

Зокрема, значно покращилася комунікативна діяльність Офісу Президента України, Міністерства оборони та Генерального штабу ЗСУ, які забезпечують регулярне та достовірне інформування суспільства про ситуацію на фронті, дії української армії, російські воєнні злочини. Підвищилася ефективність міжнародних комунікацій, особливо з країнами ЄС та НАТО, що сприяло формуванню потужної міжнародної коаліції на підтримку України. Активізувалася співпраця з громадським сектором, особливо у сфері протидії

дезінформації, розвитку медіаграмотності, підтримки незалежних медіа [19].

Водночас, система стратегічних комунікацій України все ще перебуває на стадії формування та розвитку, і потребує подальшого вдосконалення для ефективної протидії гібридним загрозам. Особливої уваги потребує розвиток інституційної спроможності, формування чіткої вертикалі координації, забезпечення належного ресурсного забезпечення, підготовка кваліфікованих кадрів, впровадження сучасних технологій та методик, розвиток міжнародного співробітництва.

Системний аналіз стану та проблем стратегічних комунікацій України дозволяє визначити пріоритетні напрями їх розвитку та вдосконалення, які будуть детальніше розглянуті у наступному розділі. Ключовим завданням є формування цілісної, адаптивної та ефективної системи стратегічних комунікацій, яка б відповідала масштабу та характеру гібридних загроз, з якими стикається Україна, та забезпечувала надійний захист інформаційного простору держави.

РОЗДІЛ 3

ФОРМУВАННЯ ТА РЕАЛІЗАЦІЯ ЕФЕКТИВНИХ КОМУНІКАЦІЙНИХ СТРАТЕГІЙ

3.1 Розробка комплексної комунікаційної стратегії протидії гібридним загрозам

Формування ефективної комунікаційної стратегії протидії гібридним загрозам є складним та багатоаспектним процесом, який вимагає системного підходу, врахування специфіки різних цільових аудиторій, використання різноманітних каналів комунікації та інструментів впливу. В умовах активної гібридної агресії Росії проти України розробка такої стратегії стає ключовим завданням для забезпечення національної безпеки та стійкості.

Комплексна комунікаційна стратегія протидії гібридним загрозам має базуватися на чіткому розумінні цільових аудиторій, їхніх особливостей, потреб, вразливостей та преференцій. Сегментація аудиторії дозволяє адаптувати меседжі та канали комунікації відповідно до специфіки кожної групи, підвищуючи ефективність комунікаційних заходів.

У контексті протидії гібридним загрозам можна виділити кілька ключових цільових аудиторій:

Внутрішні аудиторії.

— Загальне населення України – найширша цільова група, яка включає громадян різного віку, статі, соціального статусу, регіону проживання. Комунікація з цією аудиторією спрямована на формування національної єдності, підвищення резильєнтності до дезінформації, зміцнення довіри до держави та її інституцій.

— Молодь (16-30 років) – особливо важлива аудиторія, яка активно користується соціальними мережами, формує тренди, впливає на суспільні

процеси. Комунікація з молоддю має враховувати їхні ціннісні орієнтації, способи споживання інформації, мовні та культурні преференції. Ключовим завданням є формування критичного мислення, медіаграмотності, патріотичних установок.

– Старша вікова група (60+) – аудиторія, яка часто демонструє вищу вразливість до дезінформації, більше довіряє традиційним медіа, особливо телебаченню, має сформовані світоглядні установки. Комунікація з цією групою потребує особливого підходу, з акцентом на емоційні, ціннісні аспекти, використання зрозумілої мови, уникнення складних технічних термінів [16].

– Мешканці прикордонних регіонів та територій, наближених до зони бойових дій – аудиторія, яка безпосередньо стикається з наслідками російської агресії, має особливі безпекові потреби, перебуває під інтенсивним інформаційним тиском з боку противника. Комунікація з цією групою має зосереджуватися на практичних аспектах безпеки, підтримці моралі, протидії панічним настроям.

– Внутрішньо переміщені особи (ВПО) – громадяни, які були змушені залишити свої домівки через бойові дії або окупацію. Ця аудиторія має специфічні потреби в інформації щодо соціальної підтримки, житла, працевлаштування, доступу до освіти та медицини, можливостей повернення. Комунікація з ВПО має враховувати їхній травматичний досвід, психологічний стан, соціально-економічні проблеми.

– Військовослужбовці та їхні родини – аудиторія, яка безпосередньо залучена до захисту держави і потребує особливої уваги. Комунікація з цією групою має спрямовуватися на підтримку бойового духу, протидію деморалізуючим наративам, надання практичної інформації щодо соціального захисту, медичної допомоги, психологічної підтримки.

– Лідери думок та експертне середовище – особи, які мають значний вплив на формування громадської думки, можуть виступати як мультиплікатори ключових меседжів держави. До цієї групи належать журналісти, блогери, громадські активісти, науковці, культурні діячі. Комунікація з ними має

будуватися на принципах партнерства, прозорості, обміну експертизою.

Зовнішні аудиторії.

– Міжнародні партнери та союзники України – уряди, парламенти, міжнародні організації, які надають Україні політичну, фінансову, військову, гуманітарну підтримку. Комунікація з цією аудиторією спрямована на зміцнення солідарності, обґрунтування необхідності подальшої підтримки, протидію «втомі від України».

– Громадськість країн Заходу – населення держав ЄС, НАТО, інших демократичних країн, від позиції якого значною мірою залежить політика їхніх урядів щодо України. Комунікація з цією аудиторією має фокусуватися на формуванні розуміння спільності цінностей, загроз, інтересів, важливості підтримки України для європейської та глобальної безпеки.

– Населення глобального півдня – громадяни країн Африки, Азії, Латинської Америки, які часто стають об'єктами російської пропаганди, спрямованої на формування антизахідних настроїв та виправдання агресії проти України. Комунікація з цією аудиторією має враховувати їхні специфічні інтереси, історичний контекст, регіональні особливості, роль України у забезпеченні глобальної продовольчої безпеки.

– Населення Росії та Білорусі – громадяни держав-агресорів, які перебувають під тотальним інформаційним контролем своїх урядів, але можуть бути досяжні через альтернативні канали комунікації. Ця аудиторія важлива для підриву внутрішньої підтримки агресивної політики Кремля, розвінчання пропагандистських міфів, формування об'єктивного розуміння ситуації.

– Українська діаспора – мільйони етнічних українців та громадян України, які проживають за кордоном і можуть виступати як амбасадори України у своїх країнах, лобіювати українські інтереси, мобілізувати підтримку. Комунікація з діаспорою має будуватися на принципах включеності, визнання їхнього внеску, надання інструментів для ефективного представлення українських позицій.

Вразливі групи.

– Мешканці тимчасово окупованих територій – громадяни України, які перебувають під окупацією і мають обмежений доступ до об'єктивної інформації. Комунікація з цією аудиторією ускладнена технічними обмеженнями та ризиками для безпеки, але є критично важливою для підтримки зв'язку з цими територіями, збереження української ідентичності, протидії російській індоктринації.

– Національні меншини – громадяни, які належать до етнічних, мовних, релігійних меншин і можуть стати об'єктом спеціальних інформаційних операцій, спрямованих на розпалювання міжнаціональної ворожнечі. Комунікація з цими групами має враховувати їхню специфічну ідентичність, культурні особливості, історичну пам'ять, забезпечувати інклюзивність та повагу до їхніх прав.

– Соціально вразливі верстви населення – особи з низькими доходами, обмеженим доступом до інформації, нижчим рівнем освіти, які можуть бути більш сприйнятливими до популістських та маніпулятивних наративів. Комунікація з цією аудиторією має фокусуватися на практичних питаннях соціального захисту, пояснювати зв'язок між підтримкою держави та забезпеченням їхнього добробуту.

Ефективна комунікаційна стратегія має спиратися на чітко сформульовані наративи та меседжі, які відображають стратегічні цілі держави, її цінності, позицію щодо ключових подій та процесів. Формування наративів передбачає визначення основних сюжетних ліній, які створюють загальний контекст для сприйняття інформації, надають їй смислової єдності та емоційного забарвлення.

Для реалізації наративів та меседжів необхідно використовувати різноманітні канали комунікації, які забезпечують охоплення різних цільових аудиторій. В умовах сучасного інформаційного суспільства комунікаційна стратегія має передбачати комплексне використання як традиційних, так і цифрових каналів:

– Традиційні медіа (телебачення, радіо, преса) залишаються важливим каналом комунікації, особливо для старшої вікової групи, мешканців сільської

місцевості, соціально вразливих верств населення. В умовах війни особливого значення набувають загальнонаціональні телемарафони, які забезпечують постійне інформування населення про ситуацію в країні. Водночас, важливо зберігати плюралізм думок та уникати надмірної уніфікації контенту, яка може знижувати довіру аудиторії.

— Соціальні мережі (Facebook, Instagram, Twitter, TikTok, Telegram) стали ключовим каналом комунікації, особливо для молодшої та середньої вікових груп. Кожна платформа має свою специфіку, аудиторію, формати контенту, що необхідно враховувати при розробці комунікаційної стратегії. Наприклад, TikTok ефективний для короткого, емоційного, візуального контенту, спрямованого на молодь, а Twitter – для лаконічних повідомлень, які можуть швидко поширюватися серед міжнародної аудиторії.

— Месенджери (Telegram, WhatsApp, Signal, Viber) набули особливого значення в умовах війни як канали оперативного інформування, координації дій, підтримки комунікації в умовах технічних обмежень. Особливістю месенджерів є можливість створення закритих груп та каналів для специфічних аудиторій, прямої та персоналізованої комунікації.

— Офіційні веб-сайти державних органів, інформаційних порталів є важливим джерелом офіційної, достовірної інформації, особливо для аналітиків, експертів, міжнародних партнерів. Такі ресурси мають забезпечувати повноту, актуальність, доступність інформації, бути адаптованими для різних пристроїв та користувачів з особливими потребами.

— Особиста комунікація (зустрічі, брифінги, прес-конференції, публічні виступи) залишається важливим каналом, особливо для взаємодії з лідерами думок, експертами, міжнародними партнерами. Особиста комунікація дозволяє встановити більш довірчі відносини, отримати зворотний зв'язок, адаптувати меседжі відповідно до реакції аудиторії.

— Культурні продукти (фільми, серіали, музика, література, мистецтво) є потужним каналом формування ціннісних установок, національної ідентичності, емоційного зв'язку з аудиторією. В умовах інформаційної війни

культурна дипломатія стає важливим інструментом просування українських наративів на міжнародній арені.

— Освітні заходи (лекції, тренінги, семінари, курси) є ефективним каналом формування критичного мислення, медіаграмотності, розуміння механізмів інформаційних впливів. Особливого значення набувають освітні програми для молоді, вчителів, журналістів, громадських активістів, які можуть виступати як мультиплікатори знань.

Ефективна комунікаційна стратегія передбачає використання різноманітних інструментів та технологій, які дозволяють підвищити ефективність комунікації, забезпечити більш точне таргетування аудиторій, вимірювати результати, адаптувати підходи відповідно до зворотного зв'язку.

Серед ключових інструментів та технологій стратегічних комунікацій варто відзначити:

— Контент-стратегія – системний підхід до планування, розробки, управління та оцінки контенту, який забезпечує його відповідність цілям комунікації, потребам аудиторії, особливостям каналів розповсюдження. Контент-стратегія включає визначення типів контенту (інформаційний, освітній, розважальний, мотиваційний), форматів (текст, відео, аудіо, графіка), тональності (офіційна, неформальна, емоційна, гумористична), періодичності публікацій, підходів до вимірювання ефективності.

— Мультимедійні формати – використання різних типів медіа (текст, зображення, відео, аудіо, інтерактивні елементи) для більш ефективного донесення інформації до різних аудиторій. Мультимедійний підхід дозволяє задіяти різні канали сприйняття, підвищити залученість аудиторії, зробити складну інформацію більш доступною та зрозумілою. Особливо ефективними є відеоформати, інфографіка, інтерактивні карти, які дозволяють візуалізувати дані, процеси, зв'язки.

— Системи моніторингу та аналітики – інструменти відстеження інформаційного простору, аналізу медіаполя, вимірювання ефективності комунікацій. Такі системи дозволяють оперативно виявляти дезінформацію,

маніпуляції, інформаційні операції, відстежувати поширення наративів, оцінювати їхній вплив на різні аудиторії, коригувати комунікативні стратегії відповідно до результатів аналізу.

– Таргетовані комунікації – підхід, який передбачає адаптацію повідомлень, каналів, форматів відповідно до характеристик конкретних цільових груп. Таргетування може здійснюватися за демографічними (вік, стать, освіта), географічними (регіон, тип населеного пункту), психографічними (цінності, інтереси, спосіб життя), поведінковими (споживання медіа, активність в соціальних мережах) параметрами.

– Комунікативні кампанії – комплексні, скоординовані заходи, спрямовані на досягнення конкретних цілей через систематичний вплив на цільові аудиторії. Кампанії можуть мати різні цілі – інформування, просвітництво, зміна установок, мобілізація підтримки, протидія дезінформації. Ефективна кампанія базується на чіткому розумінні цільової аудиторії, використанні різних каналів та інструментів, системному підході до планування, реалізації та оцінки результатів.

Окремої уваги заслуговують кризові комунікації, які набувають особливого значення в умовах гібридної війни, коли суспільство постійно стикається з кризовими ситуаціями різного масштабу – від локальних надзвичайних подій до масштабних атак на критичну інфраструктуру, дезінформаційних кампаній, терористичних актів.

Особливого значення для України набуває система спростування дезінформації, яка є одним із ключових елементів протидії гібридним загрозам. Російська пропаганда та дезінформація є системним, масштабним, добре організованим та ресурсно забезпеченим явищем, яке потребує адекватної відповіді.

Ефективна система спростування дезінформації має включати:

– Моніторинг та виявлення дезінформації – систематичне відстеження інформаційного простору, виявлення потенційних фейків, маніпуляцій, дезінформаційних кампаній. Для цього можуть використовуватися як

автоматизовані системи на основі AI, так і мережі експертів, аналітиків, факт-чекерів.

- Аналіз та верифікація – перевірка достовірності інформації, встановлення джерел, контексту, мотивації, оцінка потенційного впливу дезінформації на різні аудиторії. Ця робота вимагає залучення фахівців з різних галузей – журналістів, аналітиків, експертів з інформаційної безпеки, психологів, соціологів.

- Спростування та контрнарратив – розробка та поширення інформації, яка спростовує фейки, надає достовірні факти, пояснює механізми маніпуляції, формує альтернативний, позитивний наратив. Спростування має бути своєчасним, зрозумілим, переконливим, адаптованим до різних аудиторій та каналів комунікації.

- Превентивна комунікація – випереджальне інформування про потенційні дезінформаційні кампанії, роз'яснення їхніх цілей, механізмів, ознак. Цей підхід базується на принципі «щеплення» аудиторії проти дезінформації через формування критичного мислення, медіаграмотності, стійкості до маніпуляцій.

- Міжнародна співпраця – взаємодія з іноземними партнерами, міжнародними організаціями, глобальними платформами у протидії транснаціональній дезінформації. Це дозволяє обмінюватися досвідом, координувати зусилля, використовувати спільні ресурси та інструменти, формувати єдиний фронт проти дезінформаційних кампаній.

Практичне впровадження комплексної комунікаційної стратегії протидії гібридним загрозам вимагає системного підходу, який передбачає інтеграцію різних елементів – цільових аудиторій, наративів, каналів, інструментів – у єдину, узгоджену систему. Ключовими етапами розробки та впровадження такої стратегії є:

- Аналіз ситуації – оцінка поточного стану інформаційного простору, виявлення наявних та потенційних загроз, аналіз цільових аудиторій, їхніх преференцій, потреб, вразливостей, оцінка доступних ресурсів та обмежень.

- Визначення цілей та пріоритетів – формулювання конкретних, вимірюваних, досяжних, релевантних, обмежених у часі (SMART) цілей комунікаційної стратегії, визначення ключових пріоритетів, часових рамок, критеріїв успіху [20].

- Розробка стратегічних наративів та меседжів – формування ключових наративів, які відображають стратегічні цілі та цінності держави, розробка конкретних меседжів для різних цільових аудиторій, каналів комунікації, ситуацій.

- Планування каналів та інструментів – визначення оптимальних каналів комунікації для різних аудиторій, розробка контент-стратегії, планування використання мультимедійних форматів, інтерактивних інструментів, технологічних рішень.

- Координація та управління – створення ефективної системи координації комунікативних зусиль різних суб'єктів, розподіл ролей та відповідальності, встановлення механізмів оперативного реагування на зміни інформаційної ситуації.

- Моніторинг та оцінка – впровадження систем моніторингу інформаційного простору, вимірювання ефективності комунікацій, аналізу реакцій різних аудиторій, коригування стратегії відповідно до отриманих результатів.

- Розвиток спроможностей – підготовка кадрів, розвиток технологічної інфраструктури, впровадження інноваційних інструментів та методик, забезпечення сталого фінансування, розвиток партнерств з громадським сектором та міжнародними організаціями.

Розробка та впровадження ефективної комунікаційної стратегії протидії гібридним загрозам вимагає системного, міждисциплінарного підходу, залучення фахівців з різних галузей – комунікацій, безпеки, психології, соціології, технологій, культури. Ця робота має бути безперервною, адаптивною, чутливою до змін інформаційного середовища, нових технологій, еволюції загроз та викликів.

3.2 Оцінка ефективності та рекомендації щодо вдосконалення комунікаційних стратегій

Оцінка ефективності комунікаційних стратегій є критично важливим елементом системи стратегічних комунікацій, який дозволяє визначити результативність комунікативних заходів, виявити проблеми та недоліки, адаптувати підходи відповідно до змін інформаційного середовища та реакцій аудиторій. В умовах протидії гібридним загрозам, коли комунікаційні стратегії виконують безпосередні безпекові функції, їхня ефективність набуває особливого значення.

Методи моніторингу та метрики ефективності комунікаційних кампаній мають бути комплексними, охоплювати різні аспекти комунікативної діяльності, враховувати як кількісні, так і якісні показники. Систематичний підхід до оцінки ефективності передбачає використання різних методів та інструментів, які доповнюють один одного та дають можливість сформувати цілісну картину результативності комунікацій.

Серед ключових методів моніторингу та оцінки ефективності можна виділити:

- Контент-аналіз медіа – систематичне дослідження змісту повідомлень у різних медіа (ЗМІ, соціальні мережі, блогосфера) з метою виявлення тенденцій, наративів, тональності, джерел інформації. Контент-аналіз дозволяє оцінити присутність державних наративів у інформаційному просторі, їх співвідношення з альтернативними або ворожими наративами, характер висвітлення ключових подій та процесів.

- Моніторинг соціальних мереж – відстеження згадувань, обговорень, реакцій на певні теми, події, меседжі в соціальних мережах. Цей метод дозволяє оперативно виявляти зміни в настроях аудиторії, появу нових наративів, джерела та шляхи поширення інформації, активність ботів та тролів, ефективність контрконтенту [32].

– Медіа-метричні дослідження – аналіз кількісних показників охоплення, залучення, впливу медіа на аудиторію. Включає вимірювання рейтингів, відвідуваності, часу перегляду, кількості підписників, коментарів, репостів, згадувань. Ці метрики дозволяють оцінити масштаб та інтенсивність комунікативного впливу, ефективність різних каналів та форматів.

– Соціологічні дослідження – опитування, фокус-групи, глибинні інтерв'ю, які дозволяють вивчити думки, установки, переконання, поведінкові патерни різних аудиторій. Соціологічні методи дають можливість оцінити, як комунікативні заходи впливають на свідомість та поведінку людей, як змінюються їхні погляди, цінності, преференції.

– Експертні оцінки – залучення фахівців з різних галузей (комунікації, безпека, психологія, соціологія, технології) для аналізу та оцінки комунікаційних стратегій, їхньої відповідності цілям, ефективності методів та інструментів, потенційних ризиків та можливостей вдосконалення.

– Експериментальні методи – проведення контрольованих експериментів для вивчення впливу різних комунікативних підходів, меседжів, форматів на поведінку та установки аудиторії. Ці методи дозволяють тестувати різні гіпотези, порівнювати ефективність альтернативних стратегій, виявляти причинно-наслідкові зв'язки.

– Аналіз великих даних – використання алгоритмів машинного навчання, нейромереж, статистичних методів для аналізу масивів даних з різних джерел (медіа, соціальні мережі, пошукові запити, онлайн-активність користувачів). Цей підхід дозволяє виявляти приховані паттерни, тренди, зв'язки, які можуть бути невидимими при традиційному аналізі [35].

Ефективність комунікаційних стратегій може оцінюватися за різними метриками, які відображають різні аспекти комунікативного процесу – від охоплення аудиторії до зміни її поведінки. Серед ключових метрик можна виділити:

– Метрики охоплення – показники, які відображають кількість людей, які потенційно мали контакт з повідомленням: кількість переглядів, показів,

унікальних відвідувачів, підписників, слухачів, глядачів. Ці метрики дають уявлення про масштаб комунікативного впливу, але не про його глибину або результат.

— Метрики залученості – показники активної взаємодії аудиторії з контентом: кількість лайків, коментарів, репостів, збережень, часу перегляду, глибини прокрутки, кліків. Ці метрики відображають рівень інтересу та уваги аудиторії до повідомлення, її готовність взаємодіяти з ним.

— Метрики сприйняття – показники, які відображають, як аудиторія сприймає та інтерпретує повідомлення: рівень розуміння, запам'ятовування, емоційна реакція, сприйняття тональності, достовірності, важливості. Ці метрики вимірюються переважно через опитування, інтерв'ю, фокус-групи.

— Метрики переконання – показники зміни установок, переконань, поглядів аудиторії під впливом комунікації: зміна ставлення до певних питань, формування нових переконань, коригування існуючих поглядів. Ці метрики також вимірюються через соціологічні дослідження, порівняння ставлень «до» і «після» комунікативного впливу.

— Поведінкові метрики – показники зміни поведінки аудиторії під впливом комунікації: участь у певних заходах, підписання петицій, пожертви, волонтерство, голосування, зміна споживчих практик, інформаційної поведінки. Ці метрики відображають найбільш глибокий рівень впливу комунікації.

— Медіа-метрики – показники присутності та впливовості в медіа-просторі: кількість та якість згадувань, тональність висвітлення, цитованість, присутність ключових меседжів, вплив на порядок денний. Ці метрики відображають, наскільки ефективно комунікаційна стратегія формує медіа-дискурс.

— Метрики ефективності протидії дезінформації – показники, які відображають результативність заходів з виявлення та спростування дезінформації: кількість виявлених та спростованих фейків, швидкість реагування, охоплення спростувань порівняно з охопленням фейків, зміна рівня довіри до дезінформації.

Аналіз охоплення, залученості та впливу на громадську думку є особливо важливим для оцінки ефективності комунікаційних стратегій. Цей аналіз дозволяє визначити, наскільки успішно комунікація досягає своїх цільових аудиторій, взаємодіє з ними та впливає на їхні установки, переконання, поведінку. Для проведення такого аналізу використовуються різні інструменти та підходи.

Аналіз охоплення, залученості та впливу має бути систематичним, регулярним, багатовимірним, враховувати різні канали комунікації, типи контенту, цільові аудиторії. Важливо не лише збирати дані, а й інтерпретувати їх у контексті стратегічних цілей комунікації, порівнювати з попередніми періодами, з показниками конкурентів або опонентів, з очікуваними результатами.

Особливу увагу слід приділяти порівнянню ефективності різних типів контенту, каналів комунікації, форматів, тональності, часу публікації, щоб визначити оптимальні підходи для різних аудиторій та цілей. Наприклад, аналіз може показати, що візуальний контент ефективніший для молодшої аудиторії, а аналітичні матеріали – для експертів; що публікації в ранковий час мають більше охоплення, а вечірні – вищу залученість; що емоційні повідомлення краще запам'ятовуються, а раціональні – більше впливають на переконання.

Важливим аспектом оцінки ефективності є також аналіз співвідношення затрат та результатів, який дозволяє визначити найбільш ефективні з точки зору ресурсів підходи та оптимізувати розподіл бюджету, кадрів, технічних засобів. Цей аналіз особливо важливий в умовах обмежених ресурсів, коли необхідно максимізувати результат при мінімальних затратах [19].

Довгострокова стратегія інформаційної стійкості суспільства є невід'ємною складовою забезпечення національної безпеки в умовах гібридних загроз. Ця стратегія має бути спрямована на формування здатності суспільства протистояти інформаційним атакам, критично оцінювати інформацію, зберігати стійкість в умовах кризових ситуацій, відновлюватися після інформаційних травм.

На основі аналізу стану системи стратегічних комунікацій України, міжнародного досвіду, характеру гібридних загроз можна сформулювати низку практичних рекомендацій щодо вдосконалення комунікаційних стратегій:

Вдосконалення інституційної архітектури стратегічних комунікацій:

- Створити єдиний міжвідомчий координаційний орган з питань стратегічних комунікацій при РНБО або Кабінеті Міністрів України, який би мав достатні повноваження для координації дій різних державних органів, розробки та впровадження єдиної комунікаційної політики, розподілу ресурсів, моніторингу та оцінки ефективності.

- Забезпечити чіткий розподіл функцій та повноважень між різними суб'єктами стратегічних комунікацій (Центр стратегічних комунікацій, Центр протидії дезінформації, підрозділи стратегічних комунікацій міністерств та відомств), уникаючи дублювання та конкуренції, забезпечуючи взаємодоповнюваність та синергію.

- Створити ефективні механізми міжвідомчої координації та обміну інформацією, включаючи спільні інформаційно-аналітичні системи, регулярні координаційні наради, спільні навчання та тренування, єдині стандарти та протоколи реагування на інформаційні загрози.

Підготовка фахівців у сфері стратегічних комунікацій:

- Розробити та впровадити систематичні програми підготовки, перепідготовки та підвищення кваліфікації фахівців зі стратегічних комунікацій для державних органів, включаючи формальну освіту (бакалаврські та магістерські програми, курси підвищення кваліфікації) та неформальні практики (тренінги, семінари, стажування).

- Забезпечити інтеграцію сучасних знань та практик у сфері стратегічних комунікацій у програми підготовки державних службовців, військовослужбовців, дипломатів, фахівців з інформаційної безпеки.

- Розвивати міжнародне співробітництво у сфері підготовки фахівців зі стратегічних комунікацій, включаючи обмін досвідом, спільні освітні програми, стажування в структурах НАТО та ЄС, залучення міжнародних

експертів [14].

Міжнародна співпраця у сфері стратегічних комунікацій:

- Активізувати співпрацю з Центром передового досвіду НАТО зі стратегічних комунікацій (NATO StratCom COE) у Ризі, включаючи участь у спільних дослідженнях, конференціях, тренінгах, обмін експертами, доступ до аналітичних матеріалів та ресурсів.
- Розвивати двосторонню співпрацю з країнами-партнерами, які мають успішний досвід протидії гібридним загрозам (США, Велика Британія, країни Балтії, Польща, Фінляндія), включаючи спільні проєкти, обмін інформацією та кращими практиками, координацію комунікативних зусиль.
- Інтегруватися в міжнародні механізми протидії дезінформації, включаючи системи раннього виявлення та реагування, бази даних фейків та маніпуляцій, мережі факт-чекерів та аналітиків.

Залучення громадянського суспільства до стратегічних комунікацій:

- Розвивати систематичне партнерство між державними органами та організаціями громадянського суспільства у сфері стратегічних комунікацій, включаючи спільні проєкти, консультації, обмін інформацією, координацію зусиль.
- Підтримувати незалежні ініціативи з протидії дезінформації, розвитку медіаграмотності, моніторингу інформаційного простору через гранти, технічну допомогу, експертну підтримку, створення спільних платформ.
- Залучати громадські організації до розробки, впровадження та оцінки комунікаційних стратегій, використовуючи їх експертизу, мережі, довіру різних аудиторій, інноваційні підходи.

Технологічний розвиток системи стратегічних комунікацій:

- Впроваджувати сучасні технологічні рішення для моніторингу інформаційного простору, виявлення дезінформації, аналізу даних, візуалізації, автоматизації процесів, включаючи системи на основі ШІ, великих даних, машинного навчання.
- Розвивати власні технологічні спроможності у сфері стратегічних

комунікацій, включаючи розробку програмного забезпечення, алгоритмів, платформ, які відповідають специфічним потребам та викликам України.

- Забезпечити кібербезпеку інформаційних систем та каналів комунікації, захист персональних даних, протидію технічним атакам та маніпуляціям.

Розвиток системи моніторингу та оцінки ефективності:

- Розробити та впровадити комплексну систему моніторингу інформаційного простору, яка дозволяє оперативно виявляти дезінформацію, маніпуляції, інформаційні операції, аналізувати їх джерела, цілі, методи, аудиторії, оцінювати потенційний вплив.

- Впровадити систему оцінки ефективності комунікаційних стратегій, яка включає чіткі, вимірювані, адекватні метрики, охоплює різні аспекти комунікативного процесу – від охоплення до зміни поведінки, враховує специфіку різних каналів та аудиторій.

- Забезпечити регулярний, систематичний аналіз результатів моніторингу та оцінки, їх інтеграцію в процеси планування та реалізації комунікаційних стратегій, адаптацію підходів відповідно до отриманих даних.

Правове забезпечення стратегічних комунікацій:

- Розробити та прийняти комплексний закон про стратегічні комунікації, який би визначив статус, функції, повноваження, механізми координації, ресурсне забезпечення, стандарти діяльності суб'єктів стратегічних комунікацій.

- Гармонізувати законодавство у сфері інформаційної політики, медіа, реклами, телекомунікацій, кібербезпеки, захисту персональних даних, інтелектуальної власності з урахуванням потреб стратегічних комунікацій.

- Імплементувати норми та стандарти ЄС та НАТО у сфері стратегічних комунікацій, інформаційної безпеки, протидії дезінформації, забезпечуючи правову основу для міжнародного співробітництва.

Імплементация цих рекомендацій дозволить суттєво підвищити ефективність системи стратегічних комунікацій України, зміцнити її

спроможність протидіяти гібридним загрозам, забезпечити стійкість суспільства до дезінформації та маніпуляцій, сформувати позитивний імідж держави на міжнародній арені.

Ефективна система стратегічних комунікацій є невід’ємною складовою загальної системи національної безпеки, інтегрується з іншими її компонентами — військовим, економічним, політичним, соціальним, забезпечуючи комплексний, системний, збалансований підхід до протидії гібридним загрозам та зміцнення національної стійкості.

Розвиток ефективних комунікаційних стратегій в умовах гібридних загроз вимагає постійних зусиль, адаптації до мінливого інформаційного середовища, врахування нових викликів та можливостей, впровадження інноваційних підходів та технологій, співпраці різних суспільних акторів та міжнародних партнерів. Україна, яка перебуває на передовій гібридної війни, має унікальний досвід протидії комплексним інформаційним загрозам, і цей досвід може бути корисним для інших демократичних держав, які стикаються з подібними викликами.

ВИСНОВКИ

За результатами дослідження можна зробити такі узагальнені висновки:

1. Стратегічні комунікації є системною, цілеспрямованою діяльністю із формування та просування ключових наративів держави, координації комунікаційних зусиль та досягнення інформаційного впливу на цільові аудиторії, що набуває особливого значення в умовах сучасних гібридних загроз. Концепт стратегічних комунікацій пройшов значну еволюцію – від суто військового інструменту до комплексного підходу, що охоплює всі аспекти взаємодії держави із внутрішніми та зовнішніми аудиторіями. Основними характеристиками стратегічних комунікацій є стратегічний характер, системність та координованість, наративний підхід, мультиканальність та мультиінструментальність, цільовий підхід, єдність слів та дій. Структура системи стратегічних комунікацій включає такі компоненти, як публічна дипломатія, зв'язки з громадськістю, інформаційно-психологічні операції, військові комунікації, кризові комунікації, громадські заходи та залучення.

2. Міжнародний досвід формування комунікаційних стратегій у контексті протидії гібридним загрозам демонструє різноманітність підходів та моделей, які формуються з урахуванням специфічних умов та викликів різних країн та організацій. НАТО розглядає стратегічні комунікації як ключовий елемент своєї діяльності, інтегруючи їх в усі аспекти політики та операцій. Ефективні практики НАТО включають постійне вдосконалення методів роботи з соціальними мережами та цифровими платформами, тісну співпрацю з національними структурами держав-членів, протидію дезінформації та фейкам. Національні моделі та практики стратегічних комунікацій, розроблені та впроваджені країнами, такими як США, Велика Британія, Польща, країни Балтії та Скандинавії, мають свою специфіку, але спільними рисами є інтеграція стратегічних комунікацій у загальну систему національної безпеки, розвиток інституційної спроможності, акцент на формуванні суспільної стійкості до

інформаційних впливів, проактивний підхід до протидії дезінформації, тісна співпраця між державним та недержавним секторами, використання інноваційних технологій та рішень.

3. Система стратегічних комунікацій України почала формуватися як відповідь на гібридну агресію Російської Федерації, що розпочалася у 2014 році. Інституційна архітектура стратегічних комунікацій України включає різні органи та структури, такі як Рада національної безпеки і оборони України, Міністерство культури та інформаційної політики України, Міністерство закордонних справ України, Міністерство оборони України та Збройні Сили України, Служба безпеки України, Міністерство цифрової трансформації України, Державна служба спеціального зв'язку та захисту інформації України. Важливу роль у системі стратегічних комунікацій України відіграють також недержавні актори – громадські організації, аналітичні центри, медіа. Нормативно-правове забезпечення стратегічних комунікацій в Україні включає такі документи, як Доктрина інформаційної безпеки України, Стратегія національної безпеки України, Стратегія комунікації у сфері європейської інтеграції, Концепція стратегічних комунікацій Міністерства оборони України та Збройних Сил України, Положення про Центр стратегічних комунікацій та інформаційної безпеки.

4. Формування ефективної комунікаційної стратегії протидії гібридним загрозам вимагає системного підходу, врахування специфіки різних цільових аудиторій, використання різноманітних каналів комунікації та інструментів впливу. Ключовими цільовими аудиторіями стратегічних комунікацій є внутрішні аудиторії (загальне населення України, молодь, старша вікова група, мешканці прикордонних регіонів та територій, наближених до зони бойових дій, внутрішньо переміщені особи, військовослужбовці та їхні родини, лідери думок та експертне середовище), зовнішні аудиторії (міжнародні партнери та союзники України, громадськість країн Заходу, населення глобального півдня, населення Росії та Білорусі, українська діаспора) та вразливі групи (мешканці тимчасово окупованих територій, національні меншини, соціально вразливі верстви

населення). Для кожної цільової аудиторії необхідно формувати відповідні наративи та меседжі, використовувати адекватні канали комунікації, враховувати специфічні потреби та особливості сприйняття інформації.

5. Оцінка ефективності комунікаційних стратегій є критично важливим елементом системи стратегічних комунікацій, який дозволяє визначити результативність комунікативних заходів, виявити проблеми та недоліки, адаптувати підходи відповідно до змін інформаційного середовища та реакцій аудиторій. Методи моніторингу та метрики ефективності комунікаційних кампаній включають контент-аналіз медіа, моніторинг соціальних мереж, медіа-метричні дослідження, соціологічні дослідження, експертні оцінки, експериментальні методи, аналіз великих даних. Ефективність комунікаційних стратегій може оцінюватися за різними метриками, які відображають різні аспекти комунікативного процесу – метрики охоплення, залученості, сприйняття, переконання, поведінкові метрики, медіа-метрики, метрики ефективності протидії дезінформації. Особливу увагу слід приділяти аналізу охоплення, залученості та впливу на громадську думку різних типів контенту, каналів комунікації, форматів, тональності, щоб визначити оптимальні підходи для різних аудиторій та цілей.

6. Практичні рекомендації щодо вдосконалення комунікаційних стратегій України включають вдосконалення інституційної архітектури стратегічних комунікацій, підготовку фахівців у цій сфері, розвиток міжнародної співпраці, залучення громадянського суспільства, технологічний розвиток системи стратегічних комунікацій, впровадження ефективної системи моніторингу та оцінки, удосконалення правового забезпечення. Імплементація цих рекомендацій дозволить суттєво підвищити ефективність системи стратегічних комунікацій України, зміцнити її спроможність протидіяти гібридним загрозам, забезпечити стійкість суспільства до дезінформації та маніпуляцій, сформувати позитивний імідж держави на міжнародній арені.

СПИСОК ВИКОРИСТАНИХ ДЖЕРЕЛ

1. Алексєєв С. В. Гібридна війна в Україні: стратегії протидії. Харків: Право, 2022. 240 с.
2. Баровська А. В. Стратегічні комунікації в діяльності Міністерства оборони України та Збройних Сил України. *Стратегічні пріоритети*. 2020. № 4. С. 65-74.
3. Бойко О. Д. Пропаганда: теорія, методи, практика. Київ: Наукова думка, 2019. 326 с.
4. Бурячок В. Л. Інформаційна та кібербезпека: соціотехнічний аспект. Київ: КНУСА, 2021. 288 с.
5. Горбулін В. П. Світова гібридна війна: український фронт. Київ: НІСД, 2017. 496 с.
6. Гусаров В. І. Інформаційно-психологічні операції Російської Федерації в Україні: моделі впливу та напрями протидії. *Національна безпека і оборона*. 2019. № 1-2. С. 57-64.
7. Додонов Р. О. Світ пропаганди і пропаганда світу: філософські нариси. Вінниця: ДонНУ імені В. Стуса, 2018. 294 с.
8. Дрешпак В. М. Комунікації в публічному управлінні. Дніпро: ДРІДУ НАДУ, 2019. 218 с.
9. Дубов Д. В. Державна інформаційна політика України в умовах гібридного миру та війни. *Стратегічні пріоритети*. 2019. № 1. С. 11-17.
10. Еляшевська Н. Ф. Медіаосвіта як інструмент протидії інформаційно-психологічним операціям. *Інформаційна безпека людини, суспільства, держави*. 2020. № 2(26). С. 68-76.
11. Жилияєв І. Б. Моніторинг інформаційного простору як складова системи національної безпеки. *Стратегічна панорама*. 2021. № 1-2. С. 103-111.
12. Іващенко А. М. Еволюція концептуальних підходів до розуміння стратегічних комунікацій. *Вісник НАДУ. Серія "Державне управління"*. 2018. №

4. С. 5-11.

13. Калініченко Б. М. Превентивні стратегії протидії деструктивному інформаційному впливу. *Політикус*. 2020. № 4. С. 60-65.

14. Капштик О. В. Кадрове забезпечення системи стратегічних комунікацій: проблеми та перспективи. *Публічне адміністрування: теорія та практика*. 2021. № 2(26). С. 87-95.

15. Квіт С. М. Масові комунікації. Київ: Києво-Могилянська академія, 2018. 352 с.

16. Кіслов Д. В. Система протидії інформаційним операціям в Україні: проблеми формування та розвитку. *Інвестиції: практика та досвід*. 2021. № 23. С. 79-85.

17. Компанцева Л. Ф. Стратегічні наративи: проблематика, структура та функціональність. *Стратегічні пріоритети*. 2019. № 2. С. 89-96.

18. Косюк О. М. Теорія масової комунікації: навчальний посібник. Луцьк: ВНУ ім. Лесі Українки, 2019. 186 с.

19. Кушнір О. В. Стратегічні комунікації в системі публічного управління України: виклики та можливості. *Наукові перспективи*. 2022. № 3(21). С. 25-33.

20. Литвиненко О. В. Гібридні загрози для національної безпеки України: сутність та механізми протидії. Київ: НІСД, 2021. 178 с.

21. Макаренко Є. А. Стратегічні комунікації в міжнародних відносинах. *Міжнародні відносини*. Серія "Політичні науки". 2019. № 1. С. 12-23.

22. Макарова Е. Т. Особливості кризових комунікацій в умовах гібридних загроз. *Вісник Національного університету оборони України*. 2021. № 3(61). С. 68-75.

23. Магда Є. В. Гібридна агресія Росії: уроки для Європи. Київ: Каламар, 2017. 268 с.

24. Малик Я. Й. Інформаційна війна і Україна. *Демократичне врядування*. 2018. Вип. 21. URL: http://nbuv.gov.ua/UJRN/DeVr_2018_21_4 (дата звернення: 10.10.2024).

25. Почепцов Г. Г. Сучасні інформаційні війни. Київ: Києво-Могилянська академія, 2018. 504 с.
26. Саєнко О. Г. Механізм інформаційно-психологічного впливу в умовах гібридної війни. *Вісник Національної академії Державної прикордонної служби України*. 2020. № 5. С. 46-57.
27. Стратегія національної безпеки України "Безпека людини – безпека країни": затв. Указом Президента України від 14 вересня 2020 року № 392/2020. Офіційний вісник України. 2020. № 75. С. 7.
28. Стратегія комунікації у сфері європейської інтеграції на 2018-2021 роки: схвал. розпорядженням Кабінету Міністрів України від 25 жовтня 2017 р. № 779-р. *Урядовий кур'єр*. 2017. № 206.
29. Сніцаренко П. М. Роль стратегічних комунікацій у протидії гібридним загрозам. *Стратегічна панорама*. 2020. № 1-2. С. 67-74.
30. Сивак Т. В. Стратегічні комунікації в системі публічного управління України: монографія. Київ: НАДУ, 2020. 400 с.
31. Тодоров І. Я. Проблеми протидії інформаційній агресії Російської Федерації в умовах гібридної війни. *Інформаційна безпека людини, суспільства, держави*. 2021. № 2. С. 51-60.
32. Ткач В. Ф. Спецпропаганда як інформаційна складова гібридної війни Росії проти України. *Стратегічні пріоритети*. 2018. № 1. С. 99-109.
33. Фролова Н. М. Особливості використання соціальних мереж у стратегічних комунікаціях. *Міжнародні відносини: теоретико-практичні аспекти*. 2020. № 5. С. 84-93.
34. Хилько М. І. Міжнародна співпраця у протидії гібридним загрозам: досвід для України. *Стратегічна панорама*. 2021. № 1. С. 32-39.
35. Шевченко М. М. Цифрові технології в системі стратегічних комунікацій: проблеми та перспективи. *Вісник НАДУ*. 2022. № 1. С. 60-68.
36. Шевченко М. І. Досвід протидії гібридній агресії в країнах Європейського Союзу. *Інвестиції: практика та досвід*. 2021. № 15. С. 91-97.
37. Штрмаєр Г. В. Політика і мас-медіа. Київ: Академія, 2019. 303 с.

38. Яворська Г. М. Концептуальні засади протидії гібридним загрозам: досвід ЄС і НАТО. *Стратегічні пріоритети*. 2019. № 3. С. 76-83.
39. Bentzen N. Strategic Communications: The EU, NATO and Countering Disinformation. European Parliamentary Research Service, 2022. 35 p.
40. Bradshaw S., Howard P. The Global Disinformation Order: Global Inventory of Organised Social Media Manipulation. Oxford: Oxford Internet Institute, 2020. 25 p.
41. Cunningham T. Strategic Communications in the Digital Age: Understanding Influence in an Era of Information Warfare. London: RUSI, 2021. 48 p.
42. Goldman E. Strategic Communication: A Tool for Asymmetric Warfare. *Small Wars Journal*. 2020. Vol. 13. P. 61-71.
43. Harris S. War by Other Means: Russia's Strategy of State Capture. CSIS Report. Washington: CSIS, 2019. 42 p.
44. Jankowicz N. How to Lose the Information War: Russia, Fake News, and the Future of Conflict. London: I.B. Tauris, 2020. 266 p.
45. Johnson M. Russian Hybrid Warfare and Extended Deterrence in Eastern Europe. *International Affairs*. 2018. Vol. 94. № 1. P. 71-94.
46. Lange-Ionatamishvili E. The Role of Strategic Communication in Countering Hybrid Warfare. *The Landscape of Hybrid Threats: A Conceptual Model*. European Centre of Excellence for Countering Hybrid Threats, 2021. P. 65-78.
47. Laity M. NATO Strategic Communications – The Next Decade. NATO StratCom COE, 2020. 28 p.
48. NATO Strategic Communications Policy. PO(2009)0141. Brussels: NATO HQ, 2009. 6 p.
49. Nemr C., Gangware W. Weapons of Mass Distraction: Foreign State-Sponsored Disinformation in the Digital Age. Washington: Park Advisors, 2019. 42 p.
50. Paul C. Strategic Communication: Origins, Concepts, and Current Debates. Santa Barbara: Praeger, 2018. 240 p.
51. Hoffman F. Conflict in the 21st Century: The Rise of Hybrid Wars. Arlington: Potomac Institute for Policy Studies, 2007. 72 p.

52. Ringsmose J., Böller I. Trust at the Heart of NATO Strategic Communications. NATO StratCom COE, 2021. 32 p.
53. McCuen J. J. Hybrid Wars. *Military Review*. 2008. Vol. 88. № 2. P. 107-113.
54. Shearer E., Grieco E. Americans Are Wary of the Role Social Media Sites Play in Delivering the News. Pew Research Center, 2019. URL: <https://www.journalism.org/2019/10/02/americans-are-wary-of-the-role-social-media-sites-play-in-delivering-the-news/> (last accessed: 10.10.2024).
55. Sweijjs T., Zilincik S. The Essence of Cross-Domain Deterrence. The Hague: The Hague Centre for Strategic Studies, 2020. 26 p.
56. Wardle C., Derakhshan H. Information Disorder: Toward an interdisciplinary framework for research and policy making. Council of Europe, 2017. 109 p.
57. Wigell M. Hybrid Interference as a Wedge Strategy: A Theory of External Interference in Liberal Democracy. *International Affairs*. 2019. Vol. 95. № 2. P. 255-275.