Міністерство освіти і науки України
Національний університет «Острозька академія»
Навчально-науковий центр заочно-дистанційного навчання
Кафедра національної безпеки та політології

Кваліфікаційна робота
на здобуття освітнього ступеня магістра на тему:

«Медіаконтент про російсько-українську війну як загроза для національної безпеки України»

Виконав студент ІІ курсу, групи ЗМНб-21,
спеціальності 256 Національна безпека (за окремими сферами забезпечення і видами діяльності)
Онуфер Михайло Андрійович

Керівник – кандидат наук з державного управління, доцент
Шершньова Олена Володимирівна

Рецензент – доктор філософських наук, професор
Шевчук Катерина Сергіївна

Острог, 2025

ЗМІСТ

ВСТУП

Актуальність теми дослідження. В умовах сучасних гібридних війн (конфліктів) медійна складова постає одним із вирішальних інструментів впливу на суспільство, органи державної влади та на процеси прийняття ключових рішень. Російсько-українська війна, яка триває з 2014 року та істотно масштабувалася у 2022 році, супроводжується потужними інформаційними атаками російської сторони, які, в першу чергу, спрямовані на дестабілізацію суспільно-політичної ситуації в Україні та її дискредитацію на міжнародній арені. В цьому контексті мас-медіа й соціальні платформи (Telegram, Facebook, Instagram, мережа «Х») стали полем битви не менш важливим, аніж битви у фізичній площині.

В 21 столітті, в період інформаційної епохи, суттєво зросла швидкість та кількість каналів поширення різноманітного контенту. Це надає можливість зовнішнім гравцям, тобто іншим країнам, оперативно та цілеспрямовано впливати на громадську думку в інших державах, поширюючи дезінформацію й маніпулятивні наративи. Таким чином, російська пропаганда активно використовує медійні платформи для формування потрібного їй інформаційного порядку денного, що сприяє легітимізації агресивних дій рф та підриває довіру до українських державних інституцій. У таких умовах життєво необхідною постає здатність українського суспільства критично оцінювати інформацію та протистояти ворожим інформаційним атакам.

На сьогоднішній день характерною ознакою сучасної російської інформаційної війни проти України є використання складної системи пропагандистських методів. Ця система включає не лише пряме викривлення фактів чи публікації фейкових новин, а й застосовує більш специфічні механізми впливу: маніпуляції історичним фактами, розпалювання релігійної та мовної ворожнечі, суб’єктивний підбір фактів, а також використанням так званих «експертних» думок, що нібито підтверджують російські тези. Саме під час цього і відбувається поступове проникнення потрібних агресору меседжів у

свідомість аудиторії через неочевидні канали: розважальний контент, популярні блоги, соціальні мережі абощо. Усе це створює потужний резонанс у суспільстві й перешкоджає формуванню об’єктивного погляду на події війни.

Подібний медіаконтент, з огляду на національну безпеку, може стати серйозним викликом для держави й суспільства, оскільки він впливає не лише на громадську думку, а й на мобілізаційну готовність населення, довіру до владних структур, міжнародну підтримку України та в цілому на здатність країни ефективно протистояти збройній агресії. Наповненість медійного простору дезінформацією, міжнаціональною ворожнечею та підривними меседжами, призводить до зниження бойового духу в суспільстві, поширення панічних настроїв та наростання недовіри між різними соціальними групами. Згодом подібні процеси підривають єдність громадян і сприяють реалізації сценаріїв, які вигідні агресорові.

Метою дослідження є аналіз суті, характеру, способів і методів впливу пропаганди російської федерації через медіаконтент як на внутрішньоукраїнського споживача, так і на закордонну аудиторію.

З огляду на дану мету відбувається постановка і пропонується вирішення наступних **дослідницьких завдань:**

- проаналізувати ключові нормативно-правові акти національного законодавства та регуляторні акти НАТО та ЄС спрямовані на нейтралізацію ворожих інформаційних (кібер) загроз;
- визначити основні типи відповідальності за порушення пов’язані з інформаційною безпекою;
- виокремити роль та місце інформаційно-психологічних операцій рф як елементу ведення гібридної війни проти України;
- дати характеристику найбільш поширеним меседжам російської пропаганди в українському медіапросторі в періоди 2014-2022 та 2022-2024 років;
- дослідити російські наративи в українському медіапросторі періоду російсько-української війни;

- проаналізувати методи просування українських та російських наративів в західноєвропейському інформаційному просторі;

- вивчити наслідки впливу російської пропаганди на формування українського іміджу закордоном.

Об'єктом дослідження є інформаційний вплив та пропаганда російської федерації спрямовані на український та закордонний інформаційний простір.

Предметом дослідження є російський медіаконтент (російські меседжі та наративи), спрямований на підрив національної та інформаційної безпеки України.

Джерельна база дослідження. Проблематика дослідження впливу російського медіаконтенту на українське суспільство як елементу ведення гібридної війни в період російсько-української війни є предметом дослідження багатьох вітчизняних та закордонних наукових розвідок, однак їх дослідження у розрізі поняття «національної безпеки» є досі малодослідженим та опосередковано згадується в роботах українських науковців. З поміж усіх досліджень крізь призму національної безпеки вплив російського медіаконтенту в період російсько-української війни (2014-2024) важливими для дослідження є праці теоретиків масової комунікації та національної безпеки, зокрема Г. Почепцова, В. Горбуліна, В. Бокача, С. Бремен, А. Вайтгеда, В. Крутія, П. Гая-Нижника, М. Чабанної, В. Ковалевського, П. Померанцева, які проаналізували типологію й методологію впливів різноманітних інформаційних стратегій на суспільну свідомість та їх взаємозалежність із напрямами внутрішньої та зовнішньої державної політики.

Нормативною основою дослідження є положення вітчизняних нормативно-правових актів (стратегії, Закони України) та зарубіжних регуляторних документів (резолюції, директиви, регламенти) спрямованих на забезпечення інформаційної безпеки та протидії дезінформації.

Методологія дослідження утворюється з сукупності загальнонаукових та спеціально-наукових методів. Методи дослідження були обрані з урахуванням мети, завдань, а також об'єкта і предмета дослідження.

Ключовими методами дослідження є:

- теоретичний аналіз та узагальнення (здійснювався з метою дослідження літературних джерел та ЗМІ задля виявлення ключових меседжів російської пропаганди в українському інформаційному просторі та їх впливу на національну безпеку України);
- теоретична інтерпретація (дозволив тлумачити та пояснювати дані про передумови та причини виникнення проросійських меседжів в українському інформаційному полі);
- історичний метод (використовувався для співставлення російських наративів в різні періоди російсько-української війни, 2014-2022 та 2022-2024 років);
- метод спостереження (дозволив виокремити характерні ознаки проросійських меседжів та наративів в українському інформаційному просторі, а також їх вплив на формування іміджу України закордоном);
- метод синтезу (використовувався для проведення комплексної оцінки нормативного регулювання інформаційних відносин в площині захисту національної безпеки України).

Практичне значення отриманих результатів полягає в можливості їх подальшого застосування: в науково-дослідній діяльності, задля подальшої наукової розробки та дослідження медіаконтенту періоду російсько-української війни як загрози для національної безпеки України; в тренінговій діяльності у сфері аналізу гібридних загроз в частині ворожої пропаганди та дезінформації.

Структура й обсяг дослідження. Робота складається зі вступу, трьох розділів, що сукупно охоплюють вісім підрозділів, висновків, переліку використаних джерел (налічує 109 позиції).

РОЗДІЛ І. ПРАВОВІ ОСНОВИ РЕГУЛЮВАННЯ ЗАКОНОДАВСТВА У СФЕРІ ІНФОРМАЦІЙНОЇ БЕЗПЕКИ

1.1. Забезпечення інформаційної безпеки в секторі національної безпеки та оборони України

На сьогоднішній день інформаційна безпека в Україні постає важливою складовою національної безпеки, особливо в умовах агресії з боку російської федерації, яка активно використовує інформаційні технології для ведення гібридної війни з Україною починаючи з 2014 року. Беззаперечним є той факт, що інформація є одним із основних інструментів сучасної гібридної війни, і саме тому забезпечення захисту інформації постає важливим викликом для України.

На початку цього дослідження варто визначитися з дефініцією «інформаційної війни» на протидію якій і будуть спрямовуватися заходи інформаційної безпеки. Так, Є. Магда зазначає, що в інформаційна війна – це узгоджена діяльність з використання інформації як зброї для ведення бойових дій. Головним стратегічним національним ресурсом для нього постає інформаційний простір, тобто інформація, мережева інфраструктура та інформаційні технології [1]. Науковець Д. Прокоф'єв наводить власне визначення: «інформаційна війна – це дії, розпочаті для досягнення інформаційної переваги шляхом завдання шкоди інформації, процесам, що базуються на інформації та інформаційних системах супротивника при одночасному захисті власної інформації, процесів, що базуються на інформації та інформаційних системах. Основні методи інформаційної війни – блокування або спотворення інформаційних потоків та процесів прийняття рішень супротивника» [2].

Дослідниця І. Боднар у своєму дослідженні «Інформаційна безпека як основа національної безпеки» зазначає, що «інформаційну безпеку слід розуміти як сукупність засобів забезпечення інформаційного суверенітету України, захист інформаційної сфери від зовнішніх і внутрішніх інформаційних загроз» [3].

Власне, поняття інформаційної безпеки в Україні охоплює різні рівні захисту: починаючи від безпеки персональної інформації громадян до захисту критичних інформаційних систем держави, що забезпечують стабільність її щоденного функціонування, включаючи енергетику, фінансовий сектор та оборону. Захист інформаційної безпеки визначений як пріоритетний у ст. 17 Конституції України в якій зазначено, що «захист суверенітету і територіальної цілісності України, забезпечення її економічної та інформаційної безпеки є найважливішими функціями держави, справою всього українського народу» [4].

Варто відзначити, що в Україні питання інформаційної безпеки регулюється цілим рядом нормативно-правових актів, які визначають стратегію інформаційної безпеки та пропонують заходи щодо її забезпечення.

Один з ключових документів, який регулює питання інформаційної безпеки в Україні є Закон України «Про національну безпеку України», який визначає інформаційну безпеку як одну з ключових складових національної безпеки. Цей закон вимагає від державних установ запровадження заходів для захисту важливих інформаційних ресурсів, надаючи чітке правове підґрунтя для забезпечення їхнього захисту від несанкціонованого доступу. В законі зазначається, що «державна політика у сферах національної безпеки і оборони спрямовується на забезпечення воєнної, зовнішньополітичної, державної, економічної, інформаційної, екологічної безпеки, безпеки критичної інфраструктури, кібербезпеки України та на інші її напрями» [5].

Важливо, що вищезгаданий Закон окреслює різноманітні загрози в інформаційному просторі та визначає механізми для протидії їм та їх нейтралізації. Основними з них є:

- *Інформаційна агресія з боку інших держав:* включає активні спроби впливу на політичну, економічну та соціальну ситуацію в країні через розповсюдження хибної інформації, пропаганди, кібератак та інші форми маніпуляцій громадською думкою.

- *Кіберзагрози*: однією з ключових загроз є кібератаки на критичну інфраструктуру, державні органи, організації та військові формування. Це

можуть бути як атаки на інформаційні системи з метою їх руйнування, так і крадіжки даних, поширення вірусів, шахрайство через мережу. Вищезгадані загрози можуть мати серйозні наслідки, зокрема під час планування та здійснення військових операцій та для підтримки економічної стабільності країни під час ведення бойових дій.

- *Терористичні загрози*: інформаційний тероризм включає використання Інтернету для вербування, координації та реалізації терористичних актів. Ця загроза також включає формування та поширення фейкових новин або дезінформаційних кампаній, що сприяють ескалації насильства.

- *Використання інформаційних технологій для здійснення шкідливої діяльності:* до цієї групи загроз належать різні види інформаційних диверсій, зокрема маніпулювання результатами виборів, спроби впливу на політичні процеси через медіа, здійснення атак на державні інформаційні системи для отримання доступу до конфіденційної інформації.

- *Внутрішні загрози:* до цієї категорії відносяться загрози, пов’язані з використанням інформації всередині країни, такі як несанкціонований доступ до державних баз даних та реєстрів, виведення важливих для безпеки даних за межі держави, а також недотримання конфіденційності в органах державної влади, що може призвести до витоків інформації [6].

Іншим важливим для нашого аналізу нормативно-правовим актом є Закон України «Про інформацію». Він врегульовує права і обов’язки суб’єктів інформаційної діяльності, чим забезпечуючи баланс між доступом до інформації і необхідністю її захисту. Цим законом визначаються правила доступу до інформації та інструменти для боротьби з дезінформацією. Для цього встановлюються спеціальні юридичні механізми контролю і санкції за порушення правил розповсюдження інформації, зокрема в умовах війни або загроз національній безпеці. Так, в статті 6 Закону визначено, що «право на інформацію може бути обмежене законом в інтересах національної безпеки, територіальної цілісності або громадського порядку, з метою запобігання заворушенням чи кримінальним правопорушенням…» [7].

З метою забезпечення захисту інформаційних систем, що використовуються державними установами, Верховною Радою України був прийнятий Закон України «Про захист інформації в інформаційно-комунікаційних системах». Цей Закон визначає стандарти і вимоги для забезпечення безпеки даних і систем, що мають стратегічне значення, зокрема і в оборонному секторі. Він охоплює технічні та організаційні заходи, які використовуються для захисту інформації, важливої для функціонування військових органів управлінь. В статті 10 Закону визначається, що «Міністерство оборони України та Служба безпеки України в порядку, встановленому Кабінетом Міністрів України, розробляють і затверджують галузеві та/або цільові профілі безпеки для інформаційних, електронних комунікаційних та інформаційно-комунікаційних систем, власником (розпорядником) яких є відповідно Міністерство оборони України та/або Збройні Сили України і Служба безпеки України» [11]. До найбільш відомих публічних інформаційно-комунікаційних систем, які перебувають у віданні Міністерства оборони України, відносяться:

- «Єдиний державний реєстр призовників, військовозобов’язаних та резервістів» (ІКС «ОБЕРІГ») – інформаційно-комунікаційна система, яка призначена для збирання, зберігання, обробки та використання даних про призовників, військовозобов’язаних та резервістів. Ця система створена для забезпечення військового обліку громадян України [8];
- Державний інтернет-портал електронних публічних послуг у сфері національної безпеки та оборони «Армія+»;
- Платформа ситуаційної обізнаності «Delta» – інформаційно-комунікаційна система, які інтегрує інформацію про розташування сил та засобів ворога і дозволяє в масштабі реального часу відстежувати положення військ противника та оперативно обліковувати виявлені об’єкти для їх подальшого вогневого ураження [9];

- Система електронного документообігу (СЕДО) – сукупність програмно-технічних засобів, призначених для автоматизованого виконання завдань щодо організації роботи з електронними документами [10];
- ІКС «Імпульс» – інформаційно-комунікаційна система призначена для ведення електронного обліку особового складу підрозділами персоналу та адміністративного складу військових частин [20].

Окремим блоком варто розглянути дві ключові стратегії, які врегульовують проблематику інформаційної безпеки. До них відносяться «Стратегія інформаційної безпеки» (2021) та «Стратегія кібербезпеки України» (2021).

Наприкінці 2021 року на державному рівні було затверджено «Стратегію інформаційної безпеки», яка була прийнята як захід реагування на поширення гібридних загроз в Україні. Цей фундаментальний нормативно-правовий акт визначає ключові завдання та напрями державної політики, спрямованої на запобігання кризовим явищам в інформаційному просторі та зміцнення інформаційної безпеки. Дана стратегія визначає «актуальні виклики та загрози національній безпеці України в інформаційній сфері, стратегічні цілі та завдання, спрямовані на протидію таким загрозам, захист прав осіб на інформацію та захист персональних даних» [12].

Згідно зі Стратегією, основною загрозою національній безпеці України в інформаційній сфері є інформаційна політика російської федерації, яка включає використання дезінформації, пропаганди та спеціальних інформаційно-психологічних операцій. Головною метою Стратегії є підвищення спроможності держави у сфері інформаційної безпеки, захист національного інформаційного простору, забезпечення соціальної та політичної стабільності, підтримка обороноздатності країни, а також збереження суверенітету, територіальної цілісності та демократичного конституційного ладу. Для досягнення цієї мети передбачено комплекс заходів, спрямованих на протидію інформаційним загрозам, запобігання інформаційній агресії, зокрема спеціальним інформаційно-психологічним операціям, що реалізуються державою-агресором [12].

Дослідник В. Новицький у своєму дослідженні «Стратегічні засади забезпечення інформаційної безпеки в сучасних умовах» зазначає, що цим декларативним документом визначено 7 важливих перспективних цілей. Перша ціль передбачає протидію дезінформації та інформаційно-психологічним операціям. Друга – забезпечення всебічного розвитку української культури та утвердження української ідентичності. Третя – підвищення рівня медіакультури та медіаграмотності суспільства. Четверта – забезпечення дотримання прав осіб на збір, зберігання, використання і поширення інформації, свободу вираження своїх поглядів і переконань, захист приватного життя, доступ до об'єктивної та достовірної інформації, а також забезпечення захисту прав журналістів. П'ята – інформаційна реінтеграція громадян України, які проживають на тимчасово окупованих територіях та на прилеглих до них територіях України. Шоста – розвиток інформаційного суспільства та підвищення рівня культури діалогу. Сьома ціль – створення ефективної системи стратегічних комунікацій [13].

Другою стратегією, яка визначає стратегічні пріоритети держави у сфері кібербезпеки та враховує сучасні виклики пов'язані з активною інформаційною війною та кібератаками є «Стратегія кібербезпеки України».

Дана Стратегія охоплює всі аспекти інформаційної безпеки в інтернет-просторі, включаючи заходи щодо захисту державних інформаційних систем, регулювання доступу до інформаційних ресурсів, а також контроль за використанням мережевих технологій, які можуть становити загрозу для національної безпеки. Окрім цього, у Стратегії передбачено розширення національних спроможностей із кіберзахисту, створення спеціалізованих центрів моніторингу кіберзагроз, а також розробку механізмів взаємодії між державними структурами та приватними компаніями для ефективного обміну інформацією про потенційні та дійсні загрози. Зокрема, на виконання цієї Стратегії було сформовано об'єднану команду реагування на кіберзагрози Міністерства оборони України та Збройних сил України «MILCERT» у складі Центру реагування на кіберзагрози Міністерства оборони України, Центру інновацій та розвитку оборонних технологій Міністерства оборони України та Центру

масштабування та розвитку оборонних технологій Міністерства оборони України [14].

Стратегія кібербезпеки України передбачає посилення нормативно-правової бази у сфері кібербезпеки, що включає розширення відповідальності за кіберзлочини, посилення контролю за цифровими платформами та впровадження стандартів безпеки для приватного та державного сектору. Одним із ключових напрямків документу є створення механізмів міжнародної взаємодії у сфері кібербезпеки. У рамках Стратегії передбачено налагодження співпраці з такими міжнародними партнерами як НАТО та ЄС, обмін досвідом щодо кіберзахисту, а також розробку колективних механізмів протидії кібератакам. Вищезгадана співпраця включає залучення України до міжнародних проєктів, які займаються питаннями кібероборони, наприклад: Програма НАТО з посилення кіберзахисту України «NATO Cyber Defence Trust Fund», ініціатива ЄС «Європейський центр передового досвіду з протидії гібридним загрозам» (European Centre of Excellence for Countering Hybrid Threats), ініціатива «Кібер-коаліція» (Cyber Coalition), ініціатива «Кіберщит» (Cyber Shield) і т.д.

Окрім вищенаведених нормативно-правових актів науковиця А. Савченко у своїй статті «Правове регулювання інформаційних ризиків в законодавстві України» [15] зазначає, що комплекс заходів щодо забезпечення інформаційної безпеки частково чи опосередковано врегульовують наступні законодавчі акти:

- Закон України «Про державну таємницю». «Цей закон регулює суспільні відносини, пов’язані з віднесенням інформації до державної таємниці, засекречуванням, розсекречуванням її матеріальних носіїв та охороною державної таємниці з метою захисту національної безпеки України» [16];
- Закон України «Про захист персональних даних» [17] визначає правові та організаційні засади захисту персональних даних, які обробляються в інформаційно-комунікаційних системах. Він також встановлює права суб’єктів персональних даних, обов’язки власників та розпорядників персональних даних, а також порядок здійснення контролю за обробкою персональних даних;

- Закон України «Про доступ до публічної інформації» визначає порядок здійснення та забезпечення права кожного на доступ до інформації, що знаходиться у володінні суб'єктів владних повноважень, інших розпорядників публічної інформації та інформації, що становить суспільний інтерес [18].
- Закон України «Про основні засади забезпечення кібербезпеки України» визначає термінологічні рамки таких понять як кіберпростір, кіберрозвідка, кібершпигунство, кібертероризм та спрямований на захист інтересів людини і громадянина, суспільства та держави, а також національних інтересів України у кіберпросторі [19]. Цей закон надає можливості для здійснення комунікацій та/або реалізації суспільних відносин, утворених в результаті функціонування сумісних комунікаційних систем та забезпечує електронні комунікації з використанням мережі Інтернет та/або інших глобальних мереж передачі даних [21].

Важливо зазначити, що захист інформаційного простору України забезпечується кількома спеціалізованими державними органами, серед яких ключовими є Рада національної безпеки і оборони України (РНБО), Служба безпеки України (СБУ) і Державна служба спеціального зв'язку та захисту інформації України (ДССЗЗІ).

РНБО є основним органом, що визначає стратегічні напрямки розвитку політики інформаційної безпеки в Україні. Вона координує діяльність усіх інших органів державної влади у цій сфері, а також здійснює контроль за виконанням заходів по забезпеченню національних інтересів в інформаційному просторі.

Окрему роль у боротьбі з інформаційними загрозами відіграє Центр протидії дезінформації при РНБО України, який був створений у 2021 році для моніторингу, аналізу та запобігання поширенню фейкової інформації, маніпуляцій та деструктивного контенту. Центр займається ідентифікацією інформаційно-психологічних операцій, які використовуються ворогом для впливу на суспільну думку, підриву довіри до державних інституцій та створення панічних настроїв серед населення [22].

Своєю чергою, СБУ відіграє ключову роль у забезпеченні інформаційної безпеки країни, виконуючи завдання із запобігання, виявлення та нейтралізації загроз, пов'язаних із кіберзлочинністю та іншими небезпечними явищами в інформаційному просторі. Одним із ключових напрямів роботи СБУ є протидія деструктивним інформаційним впливам, спрямованим на маніпуляцію громадською думкою, підрив довіри до державних інституцій, а також на розпалювання міжетнічної та міжконфесійної ворожнечі [23].

ДССЗЗІ України спеціалізується на захисті державних інформаційних систем і баз даних. Вона відповідає за впровадження сучасних технологій шифрування та кіберзахисту для інформаційних систем, що використовуються в критичній інфраструктурі України. Це включає в себе як технічні, так і організаційні заходи для забезпечення конфіденційності, цілісності та доступності інформації, які є необхідними для захисту та управління державними процесами [24].

Підсумовуючи даний підрозділ варто відзначити, що станом на 2025 рік в Україні активно розробляються та впроваджуються внутрішні регламенти, стандарти безпеки, а також плани оперативного реагування на інформаційні атаки на усіх рівнях із залученням різних відомств та органів. Забезпечення інформаційної безпеки в оборонному секторі залишається важливим елементом національної безпеки.

1.2. Нормативне регулювання інформаційної безпеки в НАТО та ЄС

Як вже зазначалося раніше, інформаційна безпека є важливим аспектом національної безпеки кожної держави, особливо в умовах зростання кількості цифрових загроз та кібератак, які можуть паралізувати ключові галузі економіки, викликати масові витоки інформації або дестабілізувати політичну ситуацію всередині держав. Власне тому країни-учасники ЄС та НАТО вживають заходів для зміцнення власних кіберсистем та протидії ворожій дезінформації

створюючи нормативно-правову базу, яка б відповідала сучасним викликам у цифровій сфері.

Варто розпочати з того, що політика інформаційної безпеки є складним системним явищем, тому важливо з'ясувати, який зміст в розуміння цього поняття закладено в офіційних документах ЄС та НАТО. Так, узагальнюючи результати аналізу ключових європейських документів за темою можна відзначити, що політика інформаційної безпеки в ЄС розглядається у нерозривному зв'язку з безпекою інформаційних та комунікаційних систем, так званих «Communication and information systems».

У Резолюції Ради Європейського Союзу (ЄС) «План дій Електронна Європа: мережева та інформаційна безпека» (2001), поняття мережевої та інформаційної безпеки охоплює наступні критерії: забезпечення доступності сервісів і даних; недопущення зламу та несанкціонованого перехоплення в комунікаційних системах; фіксація факту, що дані, які були відправлені, отримані або збережені, є повними і незмінними; забезпечення конфіденційності даних; захист інформаційних систем від несанкціонованого доступу; захист від атак із застосуванням шкідливого програмного забезпечення; забезпечення надійної аутентифікації [25].

ЄС намагається послідовно розвивати законодавство у сфері інформаційної безпеки, зосереджуючи свою увагу на кіберзахисті, захисті персональних даних та боротьбі з дезінформацією. Це відображається в ухвалених директивах, регламентах та стратегіях, які встановлюють єдині стандарти інформаційної безпеки для всіх країн-членів ЄС.

Відзначимо, що основу формування політики інформаційної безпеки ЄС закладено в низці ключових документів. Одним з них є прийнята Радою ЄС у 2002 році «Резолюція про єдиний підхід та конкретні дії у галузі інформаційної безпеки» (Resolution on a common approach and specific actions in the area of network of information security), яка спрямована на активізацію зусиль щодо підвищення інформаційної безпеки. В 2004 році було створене Європейське агентство з мережевої та інформаційної безпеки (European Network and

Information Security Agency, ENISA), в подальшому перейменоване на Агентство ЄС з кібербезпеки (European Union Agency for Cybersecurity). У 2013 році Європейською Комісією було оприлюднено першу Стратегію ЄС з кібербезпеки, під заголовком «Відкритий, безпечний та захищений кіберпростір» (Cybersecurity Strategy of the European Union: An Open, Safe and Secure Cyberspace). У 2016 році держави-члени ЄС та Європейський парламент прийняли перше в ЄС горизонтальне законодавство про кібербезпеку, а саме «Директиву про мережеву та інформаційну безпеку» (Directive concerning measures for a high common level of security of network and information systems across the Union, NIS1). Пізніше, у 2022 році впроваджено «Директиву про мережеву та інформаційну безпеку №2» (Network and Information Security Directive 2, NIS2). Вона замінила першу директиву і стала відповіддю на зростаючі загрози у кіберпросторі [27].

На відміну від попередньої директиви, NIS2 запровадила більш жорсткі вимоги до державного та приватного сектору, зокрема розширила перелік секторів, на які поширюється дія директиви. Таким чином, Директива NIS2 поширила вимоги кібербезпеки на ширший перелік секторів, включаючи:

- енергетичний сектор (електростанції, газові компанії, операції з відновлюваними джерелами енергії);
- фінансовий сектор (банки, страхові компанії, біржі);
- медицина та охорона здоров'я (лікарні, лабораторії, фармацевтичні компанії);
- цифрові інфраструктури (хмарні сервіси, дата-центри, телекомунікаційні компанії);
- транспорт (авіація, залізниці, морські порти, громадський транспорт) [26].

Розширення переліку секторів було зумовлене тим, що цифровізація багатьох сфер призвела до взаємопов'язаності інфраструктур, і атака на один сегмент може мати ланцюговий ефект на інші.

Важливою новацією Директиви NIS2 є боротьба з недостатнім рівнем звітування про кіберінциденти. Таким чином у NIS2 були впроваджені механізми, що стимулюють компанії відкрито повідомляти про загрози, а саме: були веденні

санкцій за приховування кіберінцидентів або несвоєчасне їхнє звітування, а також надавався захист компаніям від юридичних наслідків, якщо вони сумлінно звітують про інцидент.

Іншим важливим нормативно-правовим актом у сфері інформаційної безпеки ЄС є Регламент GDPR (General Data Protection Regulation), який набув чинності у 2018 році. Регламент GDPR визначає суворі правила збору, обробки та зберігання персональних даних громадян ЄС, що має велике значення для кібер- та інформаційної безпеки [28].

Регламент GDPR замінив попередні Директиви про захист даних 1995 року, встановлюючи більш суворі вимоги до компаній, урядових установ та інших організацій, що працюють із персональною інформацією.

Основні принципи Регламенту GDPR включають:

- прозорість і справедливість (компанії повинні чітко пояснювати, які дані вони збирають і з якою метою);
- мінімізація обробки (дозволяється збирати лише ті дані, які необхідні для певної цілі);
- конфіденційність та безпека (компанії зобов’язані вживати заходів для захисту персональних даних від несанкціонованого доступу);
- обмеження зберігання (персональні дані не можуть зберігатися довше, ніж це необхідно для їхньої обробки) [29].

Регламент GDPR має значний вплив не лише в межах ЄС, а й на міжнародному рівні, оскільки будь-яка компанія, що працює з персональними даними громадян ЄС, зобов’язана дотримуватися його положень. Саме тому багато країн, включаючи США, Великобританію, Канаду та Австралію, адаптують своє національне законодавство відповідно до його вимог.

Окремим блоком варто розглянути яким чином ЄС бореться з інформаційними маніпуляціями та дезінформацією, оскільки вони становлять серйозну загрозу для багатьох демократичних країн, де існує свобода слова.

ЄС почав активно боротися з дезінформаційними проявами у 2015 році. Наступного року він оприлюднив спільне повідомлення «Спільні рамки протидії

гібридним загрозам: відповідь ЄС» (Joint Framework on Countering Hybrid Threats a European Union Response). У цьому документі відзначається, що масові кампанії поширення неправдивих відомостей, використання соцмереж для формування політичного порядку денного, процеси радикалізації та вербування можуть слугувати інструментами гібридних загроз. Запропонована вище ініціатива мала забезпечити комплексний підхід з протидії дезінформації у тісній координації з державами-членами ЄС, поєднати всі наявні механізми та налагодити тісну взаємодію між дотичними структурами, щоб ефективно протидіяти подібним викликам.

На початку 2018 року, Європейська комісія сформувала експертну групу, яка мала на меті протидіяти дезінформації, ця група отримала назву «High Level Expert Group on Fake News and Online Disinformation» (HLEG). До складу цієї експертної групи увійшли 39 фахівців, які представляли інтернет-платформи, медіа-сектор, громадянське суспільство та наукові кола [31].

У квітні ж 2018 року Європейська комісія передала до Європейського парламенту документ під назвою «Боротьба з дезінформацією в Інтернеті: європейський підхід» (Tackling Online Disinformation: A European Approach). У цьому документі підкреслювалося, що дезінформація руйнує довіру до установ, цифрових та традиційних засобів масової інформації, шкодить демократії, перешкоджаючи можливості громадян приймати обґрунтовані рішення. Дезінформаційні кампанії також часто підтримують радикальні та екстремістські ідеї та діяльність.

Підсумком діяльності HLEG став аналітичний звіт, у якому експерти окреслили багатовимірну стратегію протидії дезінформації, що спирається на п’ять ключових напрямів:

1. Підвищення прозорості онлайн-новин (від дотримання вимог конфіденційності до обміну даними про алгоритми й системи, які забезпечують їхнє поширення в мережі);

2. Розвиток медіаосвіти та інформаційної грамотності, з метою посилити здатність громадян протистояти дезінформаційним впливам і впевнено орієнтуватися у цифровому медіапросторі;

3. Створення інструментів, що розширюють можливості користувачів і журналістів у викритті та нейтралізації недостовірного контенту й заохочують конструктивну взаємодію з новітніми інформаційними технологіями;

4. Захист різноманіття та стійкості європейської медіаекосистеми;

5. Поглиблення досліджень впливу дезінформації в Європі для оцінювання ефективності запроваджених заходів і своєчасного корегування відповідних політик [34].

Відповідно до рекомендацій HLEG, одним із пріоритетів політики ЄС має стати розгортання та підтримка національних європейських центрів, що спеціалізуються на дослідженні й протидії дезінформації. Такі осередки покликані здійснювати мапування цифрової інформаційної екосистеми, окреслюючи домінуючі технології, інструменти та практики поширення недостовірних повідомлень. Вони також проводять систематичний моніторинг достовірності контенту, спираючись на найсучасніші методи фактчекінгу, штучний інтелект, мовні технології та аналіз великих масивів даних.

З метою протидії поширенню дезінформації у цифровому середовищі, ЄС у 2018 році ініціював створення першого добровільного документа такого типу, а саме «Code of Practice on Disinformation», який мав на меті об’єднати зусилля цифрових платформ у боротьбі з маніпулятивним контентом. Пізніше цей документ став частиною ширшої стратегії ЄС щодо забезпечення інформаційної безпеки та прозорості цифрових платформ. Він містить набір заходів, які технологічні компанії, зокрема Meta (Facebook), Google, Twitter, Microsoft, TikTok, зобов’язалися виконувати для обмеження поширення дезінформації [30].

Цей Кодекс став відповіддю на зростаючу загрозу фейкових новин, які можуть впливати як на виборчі процеси, так і на громадську безпеку та демократичні інституції Європи. Він зосереджується на п’яти ключових аспектах:

1. Розширення прозорості онлайн-реклами (компанії зобов'язуються ідентифікувати політичну рекламу та надавати дані про рекламодавців);

2. Посилення відповідальності платформ за дезінформацію (компанії мають зменшувати видимість фейкового контенту та підвищувати авторитетність перевірених джерел);

3. Боротьба з ботами та фейковими акаунтами (соціальні мережі повинні виявляти та блокувати автоматизовані акаунти, які поширюють неправдивий контент);

4. Підтримка незалежних фактчекерів (компанії погоджуються співпрацювати з незалежними організаціями, які перевіряють факти та ідентифікують маніпуляції);

5. Звітування перед Європейською комісією (платформи мають регулярно надавати звіти про реалізацію заходів спрямованих на протидію дезінформації) [31].

У 2022 році Європейська комісія оновила Кодекс, додавши жорсткіші вимоги для технологічних компаній, зокрема зобов'язала компанії розкривати алгоритми, що просувають або блокують контент.

Ще однією ключовою структурою в ЄС є «Оперативна робоча група зі стратегічних комунікацій» (East Stratcom Task Force), вона має на меті протидію російській зовнішній інформаційній політиці та боротьбу з дезінформацією. Ця робоча група згадується у різноманітних офіційних документах, зокрема в резолюціях, що стосуються протидії пропаганді з боку третіх держав. У таких документах російські установи та медіа, зокрема «Спутник», «Россотрудничество», «Русский мир», а також пропагандистські ЗМІ, визначаються як основні джерела російської дезінформації [32].

East Stratcom Task Force стала організацією, яка сприяє просуванню комунікацій ЄС в країнах Східного партнерства та підтримує розвиток незалежних засобів масової інформації. Пріоритетними напрямками зовнішньої політики ЄС стали питання урегулювання військової агресії російської федерації в Україні, а також фінансова підтримка українських реформ, яка стало частиною

зовнішньополітичних завдань Європейської Комісії з 2015 року. Із цим, власне, тісно пов'язана і активна боротьба з російською дезінформацією [33].

East Stratcom Task Force використовує різноманітні інструменти для протидії дезінформації, зокрема взаємодію з пресою, комунікацію в інтернет-просторі, публікацію статей та аудіовізуальних матеріалів. Крім того, ця організація активно моніторить діяльність російських пропагандистських медіа та, у разі необхідності, публікує спростування. Інформація, підготовлена East Stratcom Task Force часто знаходить своє відображення у міжнародних ЗМІ, таких як The Guardian, Welt, Zeit, Independent, USA Today тощо.

Важливою для дослідження залишається позиція НАТО щодо протидії інформаційним загрозам. Власне, НАТО розглядає вплив на інформаційний та кіберпростір як одні із ключових елементів сучасного ведення гібридної війни, поряд із сухопутними, повітряними, морськими та космічними операціями.

Незвичним кроком у сфері політики інформаційної безпеки НАТО було визнання того факту, що інформаційні загрози є рівними за наслідками до воєнних загроз. Тому країни-члени Альянсу вживають відповідних технічних заходів для боротьби зі зловмисною інформаційною діяльністю як на оперативному, так і на стратегічному рівнях. Визнання рівності інформаційних та воєнних загроз відбулось на Лісабонському саміті НАТО у 2010 році. Власне, такий крок передбачив можливість застосування національних збройних сил у відповідь на інформаційну атаку щодо країни-члена НАТО [35].

Такі авторитарні режими, як в росії, Китаї та Ірані, активно використовують маніпулятивну та неправдиву інформацію для впливу на громадську думку як у межах своїх країн, так і закордоном. Ворожа інформаційна діяльність може призвести до серйозних наслідків, таких як погіршення репутації країни, розкол у суспільстві та зниження довіри до державних інституцій. Вона також здатна спотворити реальність і створити хаос в суспільстві через дезінформацію та розповсюдження ворожих наративів.

Згідно з підходами НАТО у боротьбі з дезінформацією, можна виокремити наступні інструменти ворожої інформаційної діяльності:

- дезінформація (навмисне поширення неправдивої або недостовірної інформації з метою введення в оману та маніпулювання цільовою аудиторією);
- мізінформація (випадкове розповсюдження неправдивої та/або неточної інформації без злого умислу);
- ворожий наратив (спеціально створена історія, яка спрямована на дискредитацію або приниження певного суб'єкта);
- пропаганда (тривалий інформаційний вплив, спрямований на маніпулювання аудиторією з метою формування певної поведінки або переконань для досягнення політичних цілей державним суб'єктом);
- зовнішнє маніпулювання інформацією та втручання (формування моделей поведінки, що можуть загрожувати цінностям, процедурам і політичним процесам у цільовій країні. Така діяльність здебільшого не порушує законодавство, але є маніпулятивною, цілеспрямованою та узгодженою як з боку державних, так і недержавних акторів, як усередині країни, так і за її межами) [37].

У структурі НАТО діє низка спеціалізованих підрозділів, діяльність яких спрямована на реалізацію політики інформаційної безпеки:

1. Центр стратегічних комунікацій, що розташований в м. Рига, Латвія (NATO Strategic Communications Centre of Excellence). Метою цього центру є вдосконалення комунікаційних можливостей Альянсу. Він здійснює дослідження щодо пошуку варіантів вирішення наявних проблем та проводить підготовку операцій інформаційного характеру. Діяльність даної структури спрямована на пошук шляхів розв'язання проблем, в тому числі щодо інформаційної агресії російської федерації проти України.

2. Школа комунікаційних та інформаційних систем НАТО (NATO Communications and Information Systems School, NCISS), яка розташована в м. Латина, Італії. Це навчальна установа для стратегічного командування НАТО, яка проводить технічну підготовку інформаційних та комунікаційних систем Альянсу, які застосовуються в навчаннях та операціях НАТО.

3. Об’єднаний центр передових технологій з кібероборони НАТО (NATO Cooperative Cyber Defence Centre of Excellence), розташований в м. Таллінн, Естонія. Цей центр забезпечує обмін інформацією в Альянсі та співпрацю щодо кібербезпеки та кібероборони за допомогою проведення навчань, наукових досліджень, аналізу отриманих результатів та консультування.

У стратегічній концепції «НАТО-2030» стратегічні комунікації визначено як основний інструмент для забезпечення безпеки та стійкості держав-членів у боротьбі з гібридними загрозами, а також надано рекомендації для впровадження цієї стратегії в усіх країнах-членах Альянсу:

- НАТО повинно посилити та прискорити трансформацію своїх стратегічних комунікацій для більш ефективної конкуренції, що включає інвестиції в персонал, бюджет та технології, орієнтовані на досягнення цілей STRATCOM. Зокрема, важливо підтримувати сильний і чітко визначений бренд НАТО, що сприятиме громадській підтримці Альянсу;
- НАТО повинно надати особливий пріоритет цифровим технологіям у процесі трансформації своїх комунікацій. Особливо важливим є протидія дезінформації та пропаганді, що становлять серйозну загрозу в умовах стрімкого технологічного прогресу;
- члени Альянсу мають вжити додаткових активних заходів для інформування своїх громадян і підтримки політики НАТО, сприяючи формуванню правильної громадської думки;
- НАТО повинно продовжувати посилювати співпрацю з країнами-партнерами та неурядовими організаціями для ефективного вирішення проблеми дезінформації, зокрема через спільні зусилля всіх зацікавлених сторін.
- Альянс повинен стратегічно та більш дисципліновано використовувати публічні заяви як інструменти комунікації, зокрема, відновивши практику короткострокових заяв, що сприятимуть ефективному обміну інформацією з громадськістю [39].

Основними ж пріоритетами НАТО в сфері інформаційної безпеки залишається: забезпечення належних умов для захисту об'єктів інформаційної та комунікаційної інфраструктури, здійснення заходів для нейтралізації загроз інформаційного характеру, а також надання допомоги державам-членам, які стали жертвами атак у інформаційному просторі, для відновлення та нормалізації роботи уражених інфраструктурних об'єктів.

Дезінформація в НАТО визнана серйозною інформаційною загрозою. Для ефективної протидії цьому явищу застосовується двостороння модель, що полягає у глибокому аналізі інформаційного середовища та взаємодії з громадськістю. Оцінка інформаційного середовища дозволяє своєчасно виявляти дезінформацію, тоді як комунікація з населенням сприяє поширенню достовірної інформації. В результаті політика інформаційної безпеки НАТО являє собою всебічну та результативну стратегію, засновану на принципах міжнародного права та демократичних цінностях. Важливу роль у її реалізації відіграє розгалужена структура суб'єктів і органів, що забезпечують інформаційну безпеку як для НАТО загалом, так і для країн-учасниць зокрема [38].

Одним із основних документів, що регулюють питання кібербезпеки в рамках Альянсу, є прийнята у червні 2021 року Політика кібероборони НАТО (NATO Cyber Defence Policy). Нова політика кібероборони НАТО змістила акцент із пасивного захисту до активного стримування, що означає, що Альянс готовий не лише оборонятися, а й проводити наступальні кібероперації у відповідь на загрози. Також однією з ключових змін у новій політиці кібероборони стало включення цифрового середовища до загальної військової стратегії НАТО. У документі наголошується на необхідності посилення кіберрозвідки та інтеграції кіберзасобів у військові операції, розвитку кіберкомандування (Cyber Command), яке відповідає за оборонні та наступальні операції в цифровій сфері, створення резерву кіберфахівців у країнах-членах НАТО, які будуть використовуватися у випадку масштабних кібератак.

1.3. Відповідальність за порушення законодавства у сфері інформаційної безпеки

Захист інформаційних ресурсів, конфіденційної інформації та інформаційної інфраструктури є одним із найважливіших та ключових аспектів національної безпеки України. Беручи до уваги збільшення кількості кібератак, витоків даних та порушень конфіденційності інформації, українське законодавство потребує чіткої правової бази для врегулювання цієї сфери. Важливо розуміти, що правова відповідальність за порушення в сфері інформаційної безпеки має на меті не лише покарання винних осіб, але й попередження порушень, а також створення правових механізмів для забезпечення ефективного захисту цифрового середовища в подальшому.

На початку цього дослідження варто відзначити, що притягнення осіб до відповідальності за поширення пропаганди та наративів є дуже складним процесом через труднощі в доказуванні конкретної шкоди та юридичних меж, які визначають такі дії як злочин. Пропаганда і наративи часто можна трактувати як частину свободи вираження думок, навіть якщо вони мають маніпулятивний характер, саме це і ускладнює їх кваліфікацію як кримінальних діянь. Водночас, кібератаки є більш чітко визначеними та відчутними порушеннями, оскільки вони завдають конкретної шкоди, яку можна відслідкувати та виміряти, а також мають явні юридичні наслідки, зокрема порушенням безпеки державних і приватних секторів. Таким чином, кібератаки часто є більш очевидними порушеннями, що дозволяє притягнути винних до відповідальності з використанням існуючих міжнародних норм та законодавства, власне про таку категорію правопорушень і йтиме мова далі.

Базовими принципами інформаційної безпеки є забезпечення цілісності інформації, її конфіденційності і водночас доступності для всіх авторизованих користувачів. З цього погляду основними випадками порушення безпеки інформації можна назвати такі:

- несанкціонований доступ (доступ до інформаційних ресурсів, що здійснюється з порушенням встановлених процедур і обмежень);
- витік інформації (наслідок дій особи, який призводить до того, що інформація стає доступною для осіб, які не мають прав на її отримання);
- втрачена інформація (ситуація, коли інформація стає недоступною для фізичних або юридичних осіб, які мають на неї право власності (повністю або частково));
- підробка інформації (умисні дії, що призводять до спотворення або змінення інформації, яка повинна оброблятися чи зберігатися в інформаційних системах);
- блокування інформації (дії, які спричиняють припинення доступу до інформаційних ресурсів);
- порушення роботи інформаційної системи (дії або обставини, що викликають спотворення процесу обробки даних або порушення нормальної роботи системи) [40].

Правова відповідальність за порушення інформаційної безпеки включає не лише кримінальну та адміністративну, але і цивільно-правову відповідальність. Кожен з цих видів відповідальності відповідає різним типам правопорушень та забезпечує різні механізми правової реакції на них.

Кримінальна відповідальність за порушення у сфері інформаційної безпеки є важливим елементом правового захисту від кіберзлочинності, що має величезний вплив на безпеку держави та її громадян. Законодавство України активно розвивається у відповідь на нові гібридні загрози, включно з огляду на загрози у цифровому середовищі, зокрема через кіберзлочини, які можуть призвести до серйозних наслідків для економіки та національної безпеки.

Проблематику питання кримінальної відповідальності за злочини в сфері інформаційної безпеки досліджували велика кількість українських науковців, серед яких Ю. Батурин, С. Кузьмін О. Радутний та інші. Однак, незважаючи на значний внесок цих і багатьох інших дослідників, в судовій та слідчій практиці наразі існує низка проблем. Ці проблеми стосуються як розмежування одних

кримінальних правопорушень від інших, так і правильної кваліфікації злочинів в цій галузі. Крім того, досі існують певні розбіжності в поглядах щодо визначення покарань для осіб, що вчинили зазначені правопорушення [41].

Кіберзлочини завжди вчиняються за допомогою комп'ютерних пристроїв та шкідливого програмного забезпечення. «До таких засобів належать різноманітні комп'ютери, зокрема ноутбуки, планшети та смартфони, які використовують сучасні телекомунікаційні технології, такі як бездротові мережі Wi-Fi, Bluetooth, WiMAX тощо. Крім того, до них відноситься програмне забезпечення, яке може бути як загального призначення (наприклад, браузери Opera, Google Chrom), так і спеціалізоване, яке використовується для незаконних цілей, як, наприклад, шкідливі програми SpyEye, Zeus, Carberp та інші» [42].

Кримінальний кодекс України (ККУ) містить низку статей, які стосуються кримінальної відповідальності за порушення в сфері інформаційної безпеки. Ці статті визначають санкції за несанкціонований доступ до інформаційних систем, пошкодження або модифікацію даних, а також за створення шкідливих програм, які можуть порушити роботу комп'ютерних систем. Покарання за вищезгадані порушення можуть включати штрафи, позбавлення волі, виправні роботи та інші кримінальні санкції.

Основними статтями ККУ, які передбачають санкції за порушення в сфері інформаційної безпеки та за якими суди виносять судові рішення є стаття 361 «Несанкціоноване втручання в роботу інформаційних (автоматизованих), електронних комунікаційних, інформаційно-комунікаційних систем, електронних комунікаційних мереж», стаття 361-1 «Створення з метою протиправного використання, розповсюдження або збуту шкідливих програмних чи технічних засобів, а також їх розповсюдження або збут», стаття 361-2 «Несанкціоновані збут або розповсюдження інформації з обмеженим доступом, яка зберігається в електронно-обчислювальних машинах (комп'ютерах), автоматизованих системах, комп'ютерних мережах або на носіях такої інформації», стаття 362 «Несанкціоновані дії з інформацією, яка оброблюється в електронно-обчислювальних машинах (комп'ютерах), автоматизованих

системах, комп'ютерних мережах або зберігається на носіях такої інформації, вчинені особою, яка має право доступу до неї» та стаття 363 «Порушення правил експлуатації електронно-обчислювальних машин (комп'ютерів), автоматизованих систем, комп'ютерних мереж чи мереж електрозв'язку або порядку чи правил захисту інформації, яка в них оброблюється».

В Україні найбільш поширеним злочином у сфері використання електронно-обчислювальних машин та систем є злочин, відповідальність за який передбачена статтею 361 ККУ. Розвиток мережі Інтернет призвів до того, що однією з основних проблем користувачів постає надлишок інформації та анонімізація її відправника. Це стосується, передусім, явища, відомого як «спам», тобто масованої розсилки електронних повідомлень без попереднього погодження з отримувачем. Через великий обсяг таких листів інформаційні системи можуть зазнавати надмірного навантаження, що в окремих випадках призводить до порушення їхньої стабільної роботи або повного збою.

Стаття 361 ККУ передбачає відповідальність за несанкціоновані дії, що призводять до пошкодження або знищення даних, а також за порушення роботи автоматизованих інформаційних систем. Наприклад, здійснення несанкціонованого доступу до банківських систем, програмного забезпечення або баз даних, що може призвести до великих фінансових та репутаційних втрат.

Дана стаття окреслює правові межі таких понять як:

- несанкціонований доступ до автоматизованих систем (йдеться про дії, які здійснюються без дозволу власників або адміністраторів систем. Це може бути проникнення в інформаційну систему через Інтернет або фізичний доступ до обладнання);
- пошкодження або знищення інформації (порушник може пошкодити чи знищити дані, що містяться в інформаційних системах або комп'ютерних мережах);
- порушення функціонування систем (включає будь-які дії, які можуть призвести до тимчасового або постійного виходу з ладу системи, таких як

встановлення шкідливого програмного забезпечення (вірусів, троянів) або інші види атак [43].

За цією статтею поліцейські Департаменту Кіберполіції Національної поліції України оголосили підозру київському нотаріусу, який в період з 2022 по 2024 роки здійснив підробку довіреностей, заповітів та інших нотаріальних документів задля отримання неправомірної вигоди. Окрім цього, зловмисник за винагороду оформлювали право власності на спадщину та вносив інформацію в реєстри, в тому числі для осіб, які не були спадкоємцями померлих власників майна за законом [44].

Стаття 362 ККУ передбачає кримінальну відповідальність за несанкціоноване змінення, знищення чи блокування інформації в інформаційних системах. Однак, у порівнянні зі статтею 361 ККУ, така дія часто має менше конкретних проявів або й взагалі може залишатись невиявленою до моменту виявлення значних порушень або шкоди. Відповідно, кримінальні справи за цією статтею часто потребують більш детальних і складних розслідувань, що включають аналіз змін у даних, можливу затримку виявлення злочину, а також складність у доведенні самого факту зміни чи знищення інформації без належних технічних доказів. Саме тому фахівці правоохоронних органів України доволі обмежено кваліфікують кримінальні справи за ознаками статті 362 ККУ.

Стаття 363 ККУ «Порушення правил експлуатації електронно-обчислювальних машин (комп’ютерів), автоматизованих систем, комп’ютерних мереж чи мереж електрозв’язку або порядку чи правил захисту інформації, яка в них оброблюється» охоплює несанкціонований доступ до інформаційних систем або баз даних, які містять державну таємницю, персональні дані чи іншу важливу інформацію, адже така інформація є критично важливою для забезпечення національної безпеки.

Дана стаття врегульовує та охоплює наступні аспекти:

- незаконний доступ до конфіденційної інформації (будь-які дії, що порушують правила доступу до інформації, що є конфіденційною. Це може бути як

доступ до персональних даних, так і до даних, що належать підприємствам чи організаціям);

- здійснення доступу через комп'ютерні системи або інші технічні засоби (включає не лише хакерські атаки, а й зловживання правами доступу в рамках організацій);
- незаконне використання або поширення інформації (це також включає передачу конфіденційної інформації третім особам без дозволу власника або її публікацію).

Збір доказів у кіберпросторі є значною складністю для правоохоронних органів, що пов'язано з унікальними характеристиками цифрових злочинів. По-перше, кіберзлочини часто здійснюються анонімно, що ускладнює ідентифікацію злочинців. Зловмисники використовують методи анонімізації, такі як VPN, проксі-сервери та анонімні мережі, що приховують їх реальне місце розташування та ідентифікаційні дані.

По-друге, динамічність інформаційних систем створює додаткові проблеми для збирання доказів. Інформація, що може стати важливим доказом, часто швидко змінюється або стирається після атаки. Це стосується, зокрема, зловмисного програмного забезпечення (вірусів, троянів, шкідливих скриптів), яке може автоматично очищатися після виконання своїх функцій, що ускладнює процес відновлення інформації.

Третім важливим аспектом є необхідність спеціалізованих знань для аналізу цифрових доказів. Порушення у сфері інформаційної безпеки часто потребують експертних знань у галузі програмування, криптографії та комп'ютерних мереж, щоб правильно інтерпретувати отримані дані. Недостатня кваліфікація правоохоронців або суддів, що займаються розглядом таких справ, може призвести до помилок у тлумаченні доказів. Це вказує на потребу розширення навчання та залучення спеціалізованих фахівців для ефективного збору та аналізу цифрових доказів у кіберзлочинах.

Важливо звернути увагу на той факт, що досить багато кіберзлочинів мають транскордонний характер, зловмисники можуть перебувати та вчиняти

злочини за кордоном, водночас фактичне кримінальне правопорушення вчиняється на території України, що створює юрисдикційну невизначеність.

Важливим для автора категорією є дослідження адміністративної відповідальності за порушення в сфері інформаційної безпеки. В Україні адміністративна відповідальність за порушення у сфері інформаційної безпеки регулюється Кодексом України про адміністративні правопорушення (КУпАП). Адміністративні санкції застосовуються за порушення, що не завдають значної шкоди, але порушують вимоги щодо захисту персональних даних, кібербезпеки та інформаційних систем.

Дослідник О. Шевчук наголошує на «необхідності зосередження на тих адміністративних правопорушеннях, які перешкоджають ефективному забезпеченню інформаційної безпеки органам виконавчої влади» [45].

Ретельне вивчення всіх складів адміністративних правопорушень у сфері інформаційної безпеки, які містяться в КУпАП, дозволяє розділити їх на три основні групи:

- забезпечення доступу фізичних та юридичних осіб до публічної інформації, необхідної для здійснення їхніх прав, свобод та законних інтересів;
- обмеження доступу до інформації, поширення якої може негативно вплинути на права та свободи громадян, законну діяльність юридичних осіб і національну безпеку;
- підтримка безпеки в сфері медіа-інформації [45].

Так, статтею 212-3 КУпАП «Порушення права на інформацію та права на звернення» врегульовується питання доступу до публічної інформації. Згідно цієї статті, «порушення Закону України «Про доступ до публічної інформації», а саме: «необґрунтоване віднесення інформації до інформації з обмеженим доступом, ненадання відповіді на запит на інформацію, ненадання інформації, неправомірна відмова в наданні інформації, несвоєчасне або неповне надання інформації, надання недостовірної інформації» призводить до притягнення особи до адміністративної відповідальності [46].

Своєю чергою, стаття 212-6 КУПАП «Здійснення незаконного доступу до інформації в інформаційних (автоматизованих) системах, незаконне виготовлення чи розповсюдження копій баз даних інформаційних (автоматизованих) систем» врегульовує питання «здійснення незаконного доступу до інформації, яка зберігається, обробляється чи передається в інформаційних (автоматизованих) системах» [46].

Обмеження доступу до певних відомостей, розповсюдження яких може негативно вплинути на права та свободи громадян, законну діяльність юридичних осіб чи національну безпеку, регулюється рядом законодавчих актів. Зокрема, згідно з ч. 2 ст. 34 Конституції України, реалізація прав на вільне збирання, зберігання, використання та поширення інформації може бути обмежена в окремих випадках, визначених законом.

Аналізуючи положення КУпАП, можна виділити наступні склади адміністративних правопорушень у сфері інформаційної безпеки основним об’єктом яких є медіа-простір: порушення Правил надання та отримання телекомунікаційних послуг (ст. 148-1); порушення порядку та умов надання послуг зв’язку в мережах загального користування (ст. 148-2); використання засобів зв’язку з метою, що суперечить інтересам держави, з метою порушення громадського порядку та посягання на честь і гідність громадян (ст. 148-3); демонстрування і розповсюдження фільмів без державного посвідчення на право розповсюдження демонстрування фільмів (ст. 164-6); недотримання квоти демонстрування національних фільмів при використанні національного екранного часу (ст. 164-8); незаконне розповсюдження примірників аудіовізуальних творів, фонограм, відеограм, комп’ютерних програм, баз даних (ст. 164-9) та інші [47].

Окремим блоком варто розглянути інші проступки спрямовані на захист сфери інформаційної безпеки: – незаконне зберігання спеціальних технічних засобів негласного отримання інформації (ст. 195-5 КУпАП); – порушення законодавства про державну таємницю (ст. 212-2 КУпАП); – порушення порядку

обліку, зберігання і використання документів та інших носіїв інформації, що містять службову інформацію (ст. 212-5 КУпАП) [48].

Цивільно-правова відповідальність у сфері інформаційної безпеки виникає у випадках, коли порушення призводять до збитків або порушення прав осіб або організацій. Цей вид відповідальності застосовується, коли особа або організація порушує умови договорів або не виконує зобов'язання щодо захисту інформації, що може привести до витоку даних чи пошкодження інформаційних систем.

До типових порушень, що підлягають цивільно-правовій відповідальності можна віднести неавторизоване використання або передачу персональних даних без згоди суб'єкта даних або ж невиконання зобов'язань за контрактами на постачання програмного забезпечення або технічної підтримки.

Цивільно-правові наслідки можуть включати відшкодування збитків, повернення майна або грошових коштів, а також виплату моральної шкоди. У випадках витоку персональних даних чи порушення прав на інформацію, компанії можуть бути зобов'язані компенсувати витрати на відновлення даних та покриття витрат на правовий захист.

Так, згідно статті 22 Цивільного кодексу України (ЦКУ) «Відшкодування збитків та інші способи відшкодування майнової шкоди» особи, що спричинили збитки через порушення їхніх обов'язків щодо забезпечення безпеки даних (зокрема в разі втрати чи несанкціонованого доступу до інформації), можуть бути зобов'язані відшкодувати шкоду постраждалій стороні. Зокрема, це може стосуватись неналежного забезпечення захисту даних від доступу третіх осіб.

Згідно статті 1212 ЦКУ «Загальні положення про зобов'язання у зв'язку з набуттям, збереженням майна без достатньої правової підстави» особа, яка незаконно володіє майном або грошовими коштами іншої особи, зобов'язана повернути їх на вимогу власника. У випадку порушення інформаційної безпеки (наприклад, при крадіжці або несанкціонованому використанні грошей) особа має право на повернення цих коштів.

Відповідно до статті 1167 ЦКУ «Підстави відповідальності за завдану моральну шкоду» особа, яка порушила цивільні права іншої особи, зокрема

внаслідок порушення конфіденційності даних або кіберзлочинів, може бути зобов'язана відшкодувати моральну шкоду. Це стосується ситуацій, коли порушення права призвело до моральних страждань особи (наприклад, через витік персональних даних або порушення її приватності).

Підсумовуючи даний підрозділ варто зазначити, що відповідальність за порушення українського законодавства у сфері інформаційної безпеки є важливим елементом правової системи України, що дозволяє забезпечити належний захист від кіберзагроз, захистити персональні дані громадян та, разом з тим, не обмежити їх в доступі до публічної інформації. Дана відповідальність включає як кримінальну, адміністративну, так і цивільно-правову відповідальність, що дозволяє застосовувати різні підходи в залежності від тяжкості порушення. Попри певні труднощі у застосуванні законодавчих норм, зокрема через недостатню кваліфікацію фахівців та несвоєчасне виявлення порушень, українське законодавство активно удосконалюється для боротьби з новими загрозами у сфері інформаційної безпеки та кіберпросторі.

Висновки до розділу 1

Очевидним постає той факт, що інформаційна безпека визнається фундаментальним та ключовим елементом забезпечення національної безпеки, яка безпосередньо пов'язана з безпековою, оборонною та політичною стабільністю держави. Значення інформаційної безпеки для України суттєво зросло з 2014 року, у зв'язку з гібридною агресією з боку російської федерації та впливом угорської влади на українське та європейське інформаційне поле.

Провівши аналіз національних законодавчих актів автор дослідження виокремлює кілька категорій інформаційних загроз, до яких можна віднести: зовнішні (інформаційна агресія, кібератаки), внутрішні (витоки даних, службова недбалість), терористичні (використання мереж для координації нападів), а також технологічно зумовлені (вплив деструктивних ІТ-рішень). Автор підкреслює, що законодавство України передбачає превентивні механізми реагування та

мінімізації наслідків подібних інформаційних загроз, однак ефективність їх реалізації потребує подальшого зміцнення та покращення.

Огляд українського законодавства демонструє наявність розгалуженої правової системи, яка включає в себе як базові закони («Про інформацію», «Про захист персональних даних», «Про доступ до публічної інформації», «Про державну таємницю», так і спеціалізовані нормативно-правові акти («Про основні засади забезпечення кібербезпеки України», «Про захист інформації в інформаційно-комунікаційних системах»), а також два стратегічні документи («Стратегія інформаційної безпеки», «Стратегія кібербезпеки України»).

Однак, реальна імплементація цих правових норм у практичній площині все ще стикається з проблемами нормативної фрагментарності та міжвідомчої неузгодженості. Своєю чергою, європейські та євроатлантичні інституції формують високі стандарти інформаційної безпеки, акцентуючи увагу на кіберзахисті критичної інфраструктури (NIS2, GDPR); протидії дезінформації (East Stratcom Task Force, Code of Practice on Disinformation); захисті демократичних процесів від зовнішнього впливу.

Україна намагається враховувати передові міжнародні підходи в сфері кібербезпеки, долучаючись до відповідних ініціатив і проєктів, зокрема в рамках співпраці з НАТО (наприклад, Cyber Defence Policy, CCDCOE). Водночас ефективне впровадження подібних практик на національному рівні потребує посилення інституційного потенціалу, належного фінансування та врахування специфіки внутрішнього середовища.

Аналіз відповідальності за порушення у сфері інформаційної безпеки дозволяє зробити висновок про наявність трьох взаємопов’язаних правових механізмів: кримінального, адміністративного та цивільно-правового. Водночас, практика їх застосування свідчить про складність у доказуванні злочинів в цифровому середовищі, потребу у кваліфікованих кадрах, а також про недостатній рівень правосвідомості суб’єктів інформаційних правовідносин.

Автор дослідження вважає, що в подальшому українському державному та приватному секторам необхідно спільно працювати над розробкою механізмів

раннього виявлення та реагування на інформаційні загрози, включаючи моніторинг соціальних мереж та аналіз інформаційних потоків, а також масштабувати кількість персоналу в органах відповідальних за протидію дезінформації.

РОЗДІЛ ІІ. ПРОРОСІЙСЬКІ НАРАТИВИ ЯК ІНСТРУМЕНТ ВПЛИВУ ЧЕРЕЗ РОСІЙСЬКИЙ МЕДІАКОНТЕНТ

2.1. Ключові меседжі російської пропаганди в українському медіапросторі в період 2014-2022 років

На початкових етапах формування національної інформаційної політики в Україні не було передбачено ефективних механізмів захисту від зовнішніх інформаційних загроз, спрямованих на дестабілізацію суспільно-політичного устрою держави. Однією з головних небезпек для українського медіапростору після здобуття незалежності стало поширення російських імперських наративів, які нав'язували уявлення про меншовартість української культури та її абсолютну залежність від російського культурного середовища. Власне, це негативно впливало на розвиток національного інформаційного простору, ускладнюючи формування та поширення власних державних меседжів з освітньою та просвітницькою функцією.

Досліджуючи хронологію формування та проникнення російських пропагандистських меседжів в український інформаційний простір, можна виокремили чотири умовні періоди: 1991-1999 рр., 2000-2013 рр., 2014-2022 рр., 2022-2025 рр.

Важливо зазначити, що ми відокремили періоди 2014-2022 та 2022-2025 років, оскільки анексія півострову Крим, окупація окремих територій Донецької та Луганської областей та початок повномасштабного вторгнення російської федерації в Україну призвели до появи нової категорії наративів російської пропаганди в українському інфопросторі та активно активізували їх поширення.

Для розуміння загального контексту поширення проросійських наративів в Україні все ж варто розглянути передумови, які стали ґрунтом для російського «інформаційного наступу» у 2014 році. Так, перша умовна «хвиля» проникнення російських наративів в український інфопростір почалася з проголошенням Незалежності України та розпадом СРСР. У період з 1991 по 1999 роки російська

федерація не провадила агресивної інформаційної ескалації в українському медіапросторі. На тлі розпаду СРСР російські меседжі були спрямовані в першу чергу на «відновлення партнерства України, Росії та Білорусі задля збереження/відновлення потужностей СРСР». Саме цей наратив у майбутньому російська федерація трансформує в агресивний меседж про «братні народи» та «Україну імені В. Леніна».

Кінець 90-х років був трансформаційним для українських ЗМІ, оскільки в медіапросторі з'явилося місце для плюралізму думок, висловлення різних точок зору та свободи слова загалом. Ці зміни і зіграли «на руку» російській пропаганді, бо разом зі свободою слова пропорційно зростав рівень споживання та поширення російського контенту [49].

В наступне десятиріччя проросійські меседжі потрапляли в український простір переважно через культурну та розважальну сфери. Це було обумовлено, зокрема, низьким рівнем фінансування українського культурного сектору, а також пострадянським наративом про «єдину спільну культуру». Після 90-х, коли на екрани вийшло кілька україномовних серіалів, наступила десятирічна пауза, а російський контент став домінувати, зокрема через співпрацю українських телеканалів з російськими медіа. До 2014 року російські передачі займали значну частину ефірного часу на українському телебаченні, що сприяло поширенню наративу про «меншовартість» української культури. Окрім того, в цей час медіапростір України контролювався великими фінансово-промисловими групами з проросійською орієнтацією, що підтримували політичний курс на співпрацю з росією. До цих груп можна віднести:

- Group DF (Д. Фірташ, С. Льовочкін) – ключові медіа-активи телеканал Інтер, NTN, K-1, K-2;
- System Capital Management (Р. Ахметов) – ключові медіа-активи телеканал Україна та регіональні мовники;
- Фінансово-промислова група В. Медведчука – ключові медіа-активи телеканали 112 Україна, NewsOne, ZIK [50].

У 1999-2004 та 2008-2012 роках в Україні посилилася прихована цензура, зокрема через поширення так званих «темників» для медіа. Після того як В. Медведчука призначили головою Адміністрації Президента у 2002 році, вони почали надходити всім провідним телеканалам. Паралельно російські наративи поширювалися через «джинсу», яку замовляли партії проросійського спрямування, як-от «Партія регіонів», «Блок Литвина» та «КПУ» [51]. Згодом, у 2012 році, так званий «мовний закон Колесніченка-Ківалова» став приводом для медійних суперечок і сприяв утвердженню меседжу про «захист російськомовних», котрий використовувала російська пропаганда під час анексії Криму та війни на Донбасі.

В першу декаду 2000-х років російська пропагандистська машина діяла приховано: підтримувала проросійські політичні сили в Україні, контролювала значну частину медіапростору й нав'язувала меседжі про меншовартість української культури та українського народу загалом. Брак власного розважального контенту у 2000-2010-х роках та відсутність конкуренції тільки посилювали залежність від російського медійного продукту. Період, коли латентна пропаганда перейшла у відкриту та агресивну інформаційну війну, настав із початком Революції Гідності у 2013 році. Зрив тодішнім президентом України В. Януковичем підписання угоди про євроінтеграцію спричинив суспільний протест, результатом якого стала реорганізація керівних органів законодавчої та виконавчої влади й поступове усунення проросійських політиків та держслужбовців від управління державою.

Власне, умовно наступний етап трансформації російських меседжів в українських медіа бере свій початок після повалення диктаторського режиму В. Януковича, після чого російська пропаганда зображувала Революцію Гідності як «заворушення», організоване «неонацистами» та «радикалами, яких нібито не контролює влада». Революцію Гідності висвітлювали як «проєкт Заходу», а 20 лютого 2014 року розповсюдили дезінформацію, що активісти захопили Верховну Раду, хоча фактично вони цього не робили. Російські ЗМІ

звинувачували у «фінансуванні Майдану» ЄС, НАТО, США та Д. Сороса, підтримуючи наратив про Україну як проєкт Заходу [52].

В період Революції Гідності українські медіа в регіонах продемонстрували серйозне розшарування. Це було прямим наслідком відмінності редакційних політик, заснованих або на ґрунті політичних та ідеологічних переконань власників ЗМІ. У Львові більшість ЗМІ висвітлювали Євромайдан позитивно, за винятком окремих проросійських видань, що були малопоширеними. Харківські медіа, навпаки, часто вдавалися до нейтральної або негативної оцінки, що відповідало позиції місцевої влади та загальному дефіциту незалежної преси.

Прикметно, що нові меседжі російської пропаганди посилювали сформовані раніше історичні наративи. Їхнє основне призначення – зобразити Україну як «другорядну» державу, з незначною історичною та культурною спадщиною. У 2019 році ГО «Інтерньюз-Україна» оприлюднила аналітичну довідку «Ревізія історії: російська історична пропаганда та Україна», яка базувалася на основі моніторингу російських соцмереж, а також російського сегмента міжнародних соціальних платформ. У роботі дослідники визначили ключові наративи російської історичної пропаганди, серед яких:

- «Україна – це невдала копія Росії»;
- «Україна – штучний проєкт Заходу»;
- «Крим, Донбас і південний схід України – російські території»;
- «СРСР – могутня імперія, а Сталін – герой»;
- «Українські націоналісти – фашисти»;
- «Україна спотворює пам’ять про перемогу над нацизмом» [53].

Після початку анексії Криму 20 лютого 2014 року розпочалася нова хвиля російської дезінформації. Уже 27 лютого 2014 року в Криму створили нелегітимну Раду міністрів, а 16 березня відбувся псевдореферендум, після якого російська федерація оголосила про «включення» півострова до свого складу. До цього в Криму відключили українські телеканали, замінивши їх російськими пропагандистськими ресурсами [54].

Після так званого кримського «референдуму» російські ЗМІ запустили масштабну кампанію з легітимізації анексії, поширюючи наративи про «повернення Криму в рідну гавань», «історичну справедливість» та «утиски російськомовного населення». Видання «Вести.ру» називало анексію «історичною подією», стверджуючи, що «росіяни в Україні втомилися від примусової асиміляції» [55].

Дезінформаційні кампанії формували виправдання російської агресії для внутрішньої та зовнішньої аудиторії. Журналісти «Радіо Свобода» визначили 9 міфів «про повернення Криму», які активно поширювали російські медіа щодо анексії Криму:

«1. У Криму пригнічували російську мову і культуру;

2. Референдум – це реалізація права кримчан на самовизначення;

3. Крим самовизначився за прикладом Косово;

4. Росія не здійснила анексію, оскільки Крим вже став незалежною державою;

5. Без захисту російських військ Крим розділив би долю Донбасу;

6. Приєднання Криму було мирним, «без єдиної краплі крові»;

7. Більшість кримчан були за приєднання до Росії;

8. Кримчани в основному не чинили спротив окупації Криму, лише Меджліс виступив проти;

9. Захід рано чи пізно визнає російський суверенітет над Кримом» [56].

З початком російської агресії на Донбасі пропагандистська машина рф змінила свій інформаційний дискурс. На Захід поширювалися тези про відсутність підтримки України серед населення захоплених територій, яке нібито прагнуло відокремлення. Паралельно для проросійських прихильників конструювався зовсім інший наратив – про те, що Київ «кинув» Донбас, метою чого було знищити довіру до української влади.

З метою протидії російській дезінформації у 2014 році лідерами ЄС було прийнято рішення про створення Оперативної робочої групу зі стратегічних комунікацій при Європейській дипломатичній службі. Так, команді фахівців із

досвідом роботи в галузі комунікацій, журналістики, соціальних наук і досліджень ситуації в росії, було проведено власний аналіз меседжів в російських медіа. До ключових меседжів не згаданих раніше в дослідженні було віднесено наступні:

1. «Україна – неспроможна держава під зовнішнім управлінням». Україну послідовно описували як «failed state», що нібито не здатна самостійно ухвалювати рішення, перебуває під «протекторатом» США та ЄС і приречена на економічний колапс без «братньої» допомоги російської федерації.
2. «Геноцид населення Донбасу». З весни 2014 року російські медіа просували твердження про «масові вбивства» та «етнічні чистки» проросійського населення Збройними силами України. Концепт «геноциду» виконував функцію морально-правового виправдання для військової та дипломатичної інтервенції росії.
3. «Секретні біолабораторії Пентагону». Починаючи з 2020 року активно поширювалася конспірологічна теорія про мережу американських «біологічних лабораторій» на українській території, де буцімто створювали зброю проти російської федерації. Цей меседж посилює тезу про «екзистенційну загрозу» з боку Заходу та готував ґрунт для звинувачень Києва у потенційних хімічних або біологічних провокаціях.
4. «Україна обстрілює сама себе». Згідно цього меседжу будь-які ракетні удари по цивільних об’єктах у прифронтових регіонах подавалися як наслідок «помилок української ППО» чи «інсценувань», покликаних дискредитувати російську армію та посилити санкційний тиск на російську федерацію.
5. «НАТО провокує війну». Будь-які ініціативи щодо поглиблення співпраці України з НАТО інтерпретувалися як пряме порушення «червоних ліній» безпеки росії. В такий спосіб легітимізувалася теза про необхідність «превентивної» російської операції, особливо після внесення змін в 2019 році до Конституції України та закріплення українського курсу на членство в НАТО та ЄС.

6. «Санкції б'ють по Європі, а не по росії». Із 2014 року і особливо у 2021 році прокремлівські медіа-майданчики стверджували, що обмежувальні заходи Заходу спричиняють енергетичну та соціальну кризу в ЄС, тоді як економіка російської федерації «адаптується» до неї. Власне цей наратив мав на меті розколоти санкційну коаліцію.
7. «Українські наступи приречені на провал». Після Іловайської та Дебальцевської операцій російські медіа усюди звітували про «катастрофічні втрати» та «непрофесійність» української армії, щоб деморалізувати суспільство й посіяти сумніви серед міжнародних партнерів [57].

Не менш важливим для автора дослідження є завдання відобразити релігійні російські меседжі, які російська федерація активно транслювала в Україні через підконтрольні їй церкви УПЦ МП до початку повномасштабного вторгнення. Так званий концепт «русского міра» був репрезентований в Україні не лише як культурна, а й як богословська категорія: Російська Православна Церква (РПЦ) постулювала себе «єдиним духовним центром» для всіх православних пост-радянського простору. Україна в цьому дискурсі позиціонувалася як «канонічна територія» Москви, а будь-які кроки Києва до автокефалії оголошувалися «розколом» і «відступом від істинної віри» [58].

Згодом, російські ЗМІ й політики системно заявляли про переслідування УПЦ МП. Ця російська риторика мала на меті мобілізацію прихожан УПЦ МП з метою протидії так званій «Київській владі» та закріплювала геополітичну опозицію «сакральної» росії до «здеградованої» Європи. Разом з тим зі зростанням інтенсивності бойових дій на Донбасі меседжі РПЦ дедалі частіше посилалися до «священної війни» за збереження «Святої Русі».

Підсумовуючи даний підрозділ варто зазначити, що російські медіа для власної аудиторії намагаються інтерпретувати образ України крізь призму власних інтересів, позиціонуючи її як територію, що перешкоджає подальшій експансії російської федерації. Разом з тим російська «наукова думка» розглядає Україну крізь призму різних історичних епох, де центральною залишається концепція «особливого історичного шляху» росії та заперечення Заходу як

рівнозначної цивілізаційної моделі. Також у медійному дискурсі активно експлуатуються символічні символи минулого: православна традиція, радянський сталінізм, комуністична ідеологія та імперський шовінізм, які покликані підкреслити спадкоємність російської державності й виокремити «унікальність» російської цивілізації. Через інформаційні маніпуляції й акцентування на ідеологічних суперечностях російські медіа намагаються формують образ України як держави, яка перебуває у стані постійних внутрішніх конфліктів.

2.2. Проросійські наративи в українському інфопросторі в період 2022-2024 років

Повномасштабне вторгнення військ російської федерації в Україну 24 лютого 2022 року ознаменувало новий етап конфронтації не лише на лінії бойового зіткнення, яка була окреслена під час проведення Антитерористичної операції у 2014 році та згодом трансформувалась в Операцію об'єднаних сил у 2018 році, а й в інформаційному просторі. Інформаційна війна перейшла в нову агресивну фазу та супроводжувалась скоординованими дезінформаційними кампаніями, потужними кібератаками, використанням діпфейків та штучного інтелекту. Інформаційний вплив російської федерації на внутрішньо-українського споживача та намагання подати інформацію в правильному світлі для закордонної аудиторії стали ключовими пріоритетами діяльності російських дипломатичних відомств та державних структур загалом.

Стратегія пропаганди, яку використовує Кремль, зберігає антизахідний наратив, однак використання певних термінів та інтерпретацій не завжди викликає такий же ж рівень підтримки, як у попередніх агресивних інформаційних кампаніях. Російська пропагандистська машина формує спрощену чорно-білу модель світу, розділяючи його на «ми» та «вони», що дозволяє виправдовувати власні дії як необхідну реакцію на «загрози» з боку зовнішніх «ворогів» [66].

Дослідник О. Горун звертає увагу, що для підтримки у росіян ілюзії їхньої невинності під час повномасштабного вторгнення росія активно залучає своїх пропагандистів. Проросійські блогери та медійні особи, серед яких Соловйов, Симоньян, Прилєпін, Скабєєва та інші, проявляють найбільшу активність у своїх телеграм-каналах, де вони поширюють деструктивну інформацію. Крім того, активно використовуються такі державні медіаресурси рф як РИА «Новости», ТАСС, ZVEZDANEWS і RT. Російські пропагандисти протягом багатьох років фактично підштовхують до вчинення геноциду проти українців, дегуманізуючи цілий народ і закликаючи до його фізичного знищення. Основний наратив, що озвучується в медійному просторі, стверджує, що українці не заслуговують на існування, і що саме вони винні в усіх скоєних злочинах [69].

Відзначимо, що російська дезінформація у період повномасштабного вторгнення охоплює різні цільові групи залежно від поставлених цілей. Так, керівник Центру стратегічних комунікацій та інформаційної безпеки, урядової організації при Міністерстві культури та стратегічних комунікацій, І. Соловей в інтерв'ю виданню «RFI» у 2024 році заявив, що основна ціль рф в інформаційному протистоянні в Україні це мінімізація опору з боку цивільного населення, військових та військово-політичного керівництва, а у роботі на західну аудиторію головною ціллю є ізоляція України та її обмеження в отриманні західної допомоги [59].

У 2023 році у своєму дослідженні російських наративів Ukraine War Disinfo Working Group виявило ключові дезінформаційні меседжі, які просуває російська пропаганда в Центральній та Східній Європі. Даний аналіз охопив понад 200 проросійських медіа, соцмереж і Telegram-каналів у 12 країнах, зокрема в Україні, Польщі, Грузії, Білорусі та країнах Балтії.

На підставі усіх проаналізованих повідомлень дослідники розділили їх на наступні категорії:

- антизахідні наративи;
- наративи, що дискредитують Україну;
- події на полі битви;

- негативні економічні наслідки санкцій;
- українські біженці;
- положення росіян і російськомовних меншин за кордоном;
- загроза війни виходить за межі України;
- допомога Україні;
- теорії змови [60].

Цим дослідженням було встановлено, що найбільша кількість меседжів стосується дискредитації України та антизахідної пропаганди. Так, наприклад, поширеним був наратив про те, що «українська влада не дбає про народ», а «всередині керівництва держави немає згоди». Разом із тим поширювався меседж про те, що «українці не підтримують чинне керівництво держави», зокрема президента Володимира Зеленського. Такі меседжі спрямовані на дестабілізацію суспільно-політичної обстановки в країні. Вони також потрібні для того, щоб делегітимізувати український демократичний устрій і українську державність загалом.

Російська пропаганда постійно працює над формуванням негативного іміджу України за кордоном, де представляє її як корумповану та нестабільну державу. Власне це і впливає на рівень міжнародної довіри, підтримки та солідарності з Україною. Метою таких кампаній є спроби обмежити західну допомогу для України та зменшити її присутність в міжнародному інформаційному порядку денному [61].

Теза про агресію з боку західних держав залишалася незмінною протягом першого року війни в Україні. Ця ідея активно поширювалася через різні інформаційні канали, зокрема через телеграм. Наприклад, у червні 2022 року подібні заяви було розповсюджено за участі лідера російської комуністичної партії Г. Зюганова, який стверджував, що «бандерівська наволоч» в Україні контролюється представниками США [67].

На початку повномасштабного вторгнення найпоширенішим наративом російських інформаційних атак стало твердження, що «Україна програє війну». Дослідження ДетекторМедіа та консорціуму з 11 аналітичних центрів

закордоном в дослідженні «Analysis of Russian propaganda in 11 European countries» показало, що в Україні цей меседж поширюють активніше, ніж у Європі. Подібні тези про успіхи російської армії та про те, що Захід визнає перемогу росії, поширювали в Угорщині, Болгарії, Грузії та Північній Македонії. Також активно поширювали меседж «Росія не воює на повну силу», особливо в Україні та країнах Балтики [62].

Окремо варто звернути увагу на те, що інформаційні кампанії рф у період 2022-2024 років показують високий рівень скоординованості з воєнними діями, що засвідчує цілісну стратегію ведення гібридної війни. Напередодні та під час активних наступальних операцій фіксувалося значне нарощення дезінформаційної активності, зокрема з поширенням неправдивої інформації про нібито «геноцид російськомовного населення» на тимчасово окупованих територіях Донбасу. Подібні меседжі застосовувалися для легітимізації збройної агресії та деморалізації цивільного населення України й особового складу Сил оборони України [63].

У жовтні та листопаді 2022 року російська пропаганда значно посилила свою активність під час масованих ракетних обстрілів України, збільшивши кількість фейкових новин у медіапросторі вдвічі. До середини грудня 2022 року в інформаційному просторі активно поширювалися такі фальшиві повідомлення, як «Пункти незламності вбивають людей», «Зеленський хоче використати європейців як живий щит на об’єктах критичної інфраструктури», та «Передача храмів від Московського патріархату до Православної церкви України – це боротьба за вплив на розум людей». Застосовуючи подібні маніпуляції, російські пропагандисти, через анонімні телеграм-канали, намагалися відвести увагу від питання захисту національного суверенітету та територіальної цілісності, переключаючи акценти на корумпованість української влади [69].

Одним з ключових наративів, які поширюються росіянами для внутрішнього споживача опісля 2022 року є наратив про «кровожерливих нацистів». Цей наратив має на меті посилення антиукраїнських настроїв та розпалювання мілітаризму серед вже підготовлених до пропаганди росіян.

Кожного разу їм надаються нові «аргументи», що нібито пояснюють причини «спеціальної військової операції в Україні». Росіяни постійно чують наратив, що, якщо російська армія не знищить українців, то «бандерівці», «неонацисти», як їх називають окупанти, будуть вбивати їх та їхніх дітей. З початку повномасштабного вторгнення російська пропаганда активно поширює твердження, що Україна сама готувалася до нападу на Донбас і росію, а дії російської армії є лише превентивними, спрямованими на запобігання цій агресії [73].

Наративи щодо ядерної та радіологічної зброї, поширювані росією, включають твердження, що Україна прагне отримати ядерну зброю, має технічні можливості для створення ядерних або радіоактивних пристроїв, а також використовує західну допомогу для досягнення цих цілей. Основою для таких звинувачень є окремі висловлювання українських лідерів, які неодноразово висловлювали незадоволення Будапештським меморандумом 1994 року, який гарантував Україні безпеку в обмін на відмову від ядерної зброї [75].

Доволі незвичним наративом було зображення російських військових невдач як турбота про захист цивільного населення. Наприклад, скорочення темпів наступу в серпні 2022 року в анонімних телеграм-каналах було представлене як свідомий вибір командування російських військ, зумовлений бажанням зменшити кількість жертв серед цивільного населення. Крім того, ці меседжі служать виправданням війни, описуючи її як благородний захід, метою якого є забезпечення безпеки і благополуччя як для українців, так і для росіян. Використовуючи ці та інші аргументи російська пропаганда намагається ігнорувати численні людські жертви, спричинені війною в Україні.

Згідно з даними генерального прокурора України А. Костіна, протягом першого року війни загинуло понад 9 тисяч цивільних осіб, серед яких 461 дитина. Таким чином, важко говорити про «порятунок цивільних», оскільки російські ракети постійно обстрілюють житлові райони та торгові центри. Проте кожного разу, коли трапляється подібний випадок, російська пропаганда переконує аудиторію, що жертви серед цивільних виникають через те, що

українські військові використовують житлові будинки та навчальні заклади як укриття або ж самі українські військові обстрілюють цивільні об’єкти аби згодом звинуватити в цьому росію [68].

Російська пропагандистська машина також намагається створити образ України як загрози для всієї Європи. Кремль активно поширює твердження, що Україна є терористичною державою, яка не заслуговує на підтримку з боку Заходу. Російські медіа активно намагаються переконати польське суспільство, що приймання українських біженців є надмірно дорогим і створює проблеми для економіки Польщі. Вони часто розповсюджують інформацію про те, як європейці нібито втомилися від українців і навіть виганяють їх на вулицю. Водночас, російська пропаганда також працює у зворотному напрямку, намагаючись переконати українців у тому, що Польща є небезпечною для іноземців. Іншим наративом, який постійно просувається російськими медіа протягом усього конфліктує ідея про можливий поділ України між різними країнами.

Крім того, росія почала застосовувати нові специфічні тактики в інформаційній війні, серед яких є метод «віддзеркалювання наративів» і «присвоєння» української мови. Перший метод полягає в тому, що росія використовує заяви, які спершу були озвучені Україною, а потім поширює їх у своєму контексті. Наприклад, коли Україна заявила, що росія не забирає тіла своїх військових, незабаром російські пропагандисти почали поширювати відповідний наратив, що Україна нібито не забирає тіла своїх загиблих бійців. Цей метод спрямований на те, щоб посіяти сумніви щодо рішень української влади та дій ЗСУ [70]. Іншим методом є «присвоєння» української мови та культури: російські медіа та користувачі соцмереж почали активно використовувати українські слова в своїх матеріалах або навіть писати пропагандистські тексти українською мовою. Цей підхід має на привласнити українську мову та культуру, намагаючись нав’язати власні наративи в її контексті [71].

Після визволення Київської області в 2022 році стали відомі факти численних військових злочинів, скоєних російськими військами проти мирних українців. Однак російська пропаганда намагалася відвести увагу від цих звірств, пропонуючи різні версії того, що насправді відбулося, з метою дезорієнтації української аудиторії. Російські пропагандисти намагалися створити враження, що встановити правду надзвичайно складно. В рамках цієї кампанії пропагандисти вигадували різноманітні наративи, зокрема стверджували, що злочини були скоєні не російськими військами, а українськими чи британськими спецслужбами, або що звірства є інсценізацією, а «жертви» були акторами, які грали мертвих людей. Міністерство оборони росії заявляло, що «за час перебування російських Збройних Сил у Бучі жоден місцевий мешканець не постраждав від насильницьких дій». Згодом цю заяву активно поширювали пропагандистські ЗМІ [72].

Підкреслимо, що російські інформаційно-психологічні операції спрямовані не лише на дискредитацію Сил оборони України, а й на деморалізацію цивільного населення та зменшення опору всередині українського суспільства. Насадження відчуття безвиході та зневіри реалізується шляхом постійного поширення меседжів, котрі формують переконання в невідворотності негативних перспектив. Зокрема щодо розвалу української державності з середини, зради союзників або неможливості перемогти у війні.

У фахових виданнях розповсюдження зневіри й деморалізації серед громадян трактується як невід’ємний компонент стратегічних комунікацій у контексті гібридної війни. Наприклад, НАТО визначає стратегічні комунікації як узгоджене застосування інформаційних інструментів з метою впливу на сприйняття, погляди та дії цільових аудиторій, з метою досягнення політичних та військових цілей. У такому ракурсі дезінформаційні кампанії, націлені на підрив суспільної довіри до державних органів та зниження морального духу населення, є типовими рисами гібридної війни [64].

Власне ці меседжі проявляються у вигляді дезінформаційних матеріалів, маніпулятивних заголовків, емоційно насичених фейкових новин чи свідомо

перекручених висловлювань публічних осіб. Найчастіше застосовуються наративи про так зване «возз'єднання з росією», як про неминучий крок, що нібито підтримується частиною суспільства, або про «зміну орієнтирів Заходу», що, на переконання пропагандистів, повинно спонукати до зневіри в підтримці міжнародних партнерів [65].

Цікаво, що в контексті гібридної війни російська федерація регулярно послуговується тематикою мирних переговорів як засобом інформаційно-психологічного впливу. Метою цього є сформувати у цільової аудиторії уявлення про нібито конструктивну та миролюбну позицію росії, яка супроводжується постійними звинуваченнями України у блокуванні процесу врегулювання конфлікту. Наративи цього типу адаптуються відповідно до актуальної військово-політичної ситуації. У періоди загострення бойових дій переважають меседжі на кшталт «Київ відмовляється від переговорів», «Україна навмисно затягує війну» або «Захід не дозволяє Україні досягти миру». У такий спосіб російська сторона прагне створити спотворене сприйняття України як головного противника мирного процесу, водночас посилюючи інформаційний тиск як на внутрішнє українське суспільство, так і на міжнародну спільноту.

Отже, російська інформаційна війна у період з 2022 по 2024 рік була вибудувана навколо комплексної серії меседжів. Вони мали чітку взаємозалежність та виконували конкретні задачі: дискредитувати український уряд та Сили оборони України, піддавати критиці західні країни та їх підтримку для України, формувати уявлення про роз'єднане та дезорієнтоване українське суспільство, а також виправдовувати військову агресію, прикриваючись «захистом російськомовних».

Інформаційна пропаганда демонструвала вражаючу адаптивність, адже її меседжі коригувалися відповідно до фази конфлікту, суспільного сприйняття та політичної ситуації. Найбільш інтенсивні інформаційні удари фіксувалися під час загострення бойових дій, що вказує на координацію цих зусиль з воєнною стратегією. Особливу активність росія виявляла, працюючи із західною аудиторією, поширюючи наративи про втому від війни, неефективність

підтримки України та неспроможність її уряду. Ці та інші меседжі мали на меті ізоляцію України на міжнародній арені та зниження рівня її підтримки.

Згадані вище фактори підкреслюють необхідність всебічного перегляду підходів до інформаційної політики України, включаючи посилення стратегічних комунікацій, розвиток медіаосвіти, підтримку незалежної журналістики та активнішу інтеграцію проблематики захисту інформаційної безпеки в структуру національної безпеки України.

2.3. Інформаційно-психологічні операції як елемент ведення гібридної війни російської федерації проти України

Інформаційно-психологічні операції (ІПСО) є однією з найважливіших складових сучасної гібридної війни, яку тривалий час веде російська федерація проти України. ІПСО включають в себе різноманітні методи та технології, які спрямовано впливають на свідомість і поведінку людей, маніпулюють їхніми переконаннями, емоціями та настроями за допомогою різноманітних інформаційних каналів, психологічних технік і медіа. ІПСО можуть бути як стратегічними, тобто націленими на досягнення глобальних політичних цілей, так і тактичними, що здійснюються на короткотермінову перспективу для зміни ситуації в певний момент часу. ІПСО не обмежуються лише інформаційним простором і можуть включати психологічний вплив на суспільство в цілому, а також на окремі його групи. Власне, ІПСО дозволяють російській федерації маніпулювати громадською думкою, дестабілізувати внутрішню політичну ситуацію в Україні та послабляти рівень нашої національної безпеки, не здійснюючи традиційних прямих військових дій.

У процесі інформаційної війни ворог, прагнучи підривати інформаційну безпеку суспільства, часто використовує ІПСО. Вони здійснюються за допомогою ретельно розроблених планів впливу на суспільство, що спрямовані на зміну життєвих установок і поведінки людей з метою досягнення конкретних політичних чи стратегічних цілей.

ІПСО відіграють також важливу роль у міжнародному середовищі, в той час коли росія намагається створити загальне враження, що конфлікт в Україні є внутрішнім, а не результатом збройної агресії з боку рф. Російські ІПСО включають в себе стратегічні кампанії на дипломатичному рівні, маніпуляції інформацією для створення ілюзії підтримки серед населення або міжнародної спільноти для виправдання своїх дій.

Власне цей підрозділ має на меті дослідити методи, які використовує російська федерація для здійснення своїх ІПСО, їхній вплив на національну безпеку України, зокрема на політичну стабільність, соціальну єдність і довіру до державних інститутів. Також автор аналізує, яким чином ІПСО впливають на суспільну думку в Україні, підсилюють внутрішні конфлікти та знижують ефективність державних органів влади та органів місцевого самоврядування.

Для ґрунтовного аналізу варто все ж визначитись що таке ІПСО. Так, інформаційно-психологічні операції можна визначити як комплекс заходів, спрямованих на маніпулювання громадською думкою, вплив на індивідуальні та колективні уявлення і поведінку з використанням медіа та психологічних засобів. ІПСО можуть бути направлені на створення певного образу ворога, дестабілізацію в суспільстві чи підрив довіри до державних органів. Дослідниця А. Мегель надає наступну дефініцію терміну ІПСО «це попередньо спланований та послідовно реалізований вплив на думки, настрої, світоглядні позиції людей з метою реалізації особистих цілей організатора» [76].

Дослідник В. Горбулін зазначає, що основною метою ІПСО є маніпулювання масовою свідомістю для досягнення кількох стратегічних цілей: по-перше, це впровадження певних ідей і поглядів у суспільну свідомість та свідомість окремих осіб; по-друге, це сприяння дезорієнтації та поширенню дезінформації серед населення; по-третє, ослаблення стійких переконань, які є основою суспільства; по-четверте, це використання залякування як інструменту впливу.

ІПСО є невід’ємним елементом ведення гібридної війни, яка, своє чергою, вибудовує стратегією, що включає в себе комбінацію традиційних військових

методів ведення бойових дій і нетрадиційних, таких як кібератаки, економічний тиск, інформаційні маніпуляції, сприяння внутрішнім конфліктам і створення політичного хаосу. Основною метою ІПСО є досягнення своїх політичних цілей без прямої військової ескалації, що дозволяє зменшити міжнародні наслідки (санкції), уникнути повномасштабного конфлікту та не допустити втрат в живій силі.

У польовому статуті Збройних сил США FM 33-1 дається таке визначення спеціальних інформаційних операцій: «У загальному сенсі це сплановане застосування засобів, форм і методів поширення інформації для впливу на настанови та поведінку людей. У більш вузькому значенні СІО використовуються збройними силами для деморалізації та дезорієнтації супротивника». Тобто основною метою спеціальних психологічних операцій є забезпечення змін у поведінці як союзників, так і супротивників США в напрямку, вигідному для країни [77].

Одним з найбільш поширених методів ІПСО є створення фальшивих наративів, які мають на меті сформувати негативне ставлення до українського уряду, військових та західних партнерів. Росія активно використовує пропагандистські медіа для розповсюдження інформації, яка в спотвореному вигляді відображає реальні події. Одним із прикладів є інформація, що стосується подій на Майдані у 2014 році, де російські медіа поширювали фальшиві новини про те, що на Майдані були «фашисти» та «радикали», які нібито брали участь у насильницьких діях. Цей наратив мав на меті не лише дискредитувати українських протестувальників, але й створити враження, що боротьба за євроінтеграцію була організована небезпечними екстремістами.

Науковець М. Дмитренко підкреслює, що об’єктами системи інформаційно-психологічного забезпечення є наступні складові:

1. «Система формування громадської думки.
2. Система ухвалення політичних рішень.
3. Психіка та поведінка людини.

4. Інформаційно-психологічне середовище українського суспільства, яке є частиною світового інформаційного простору.

5. Інформаційні ресурси, зокрема духовні, культурні, історичні, національні цінності та традиції.

6. Система формування суспільної свідомості, що включає світогляд, політичні погляди та духовні цінності» [78].

Як вже було сказано раніше, ІПСО є важливими інструментами так званої «м'якої сили» та гібридної війни, оскільки дозволяють державам реалізовувати свої стратегії з мінімальними витратами порівняно з традиційними військовими методами. Враховуючи це, концепція ІПСО, яка охоплює дії, спрямовані на зміну сприйняття й поведінки людей для підтримки національних інтересів через контроль над інформацією, тісно переплітається з поняттями гібридних війн (поєднання військових і невійськових засобів, таких як кібератаки, дезінформація і економічний тиск) та «м'якої сили» (спроможність держави впливати на інші через культурні та політичні цінності без застосування сили чи примусу).

Основними методами впливу в цьому контексті є:

- дезінформація та пропаганда (використання неправдивої інформації або маніпуляцій з даними для зміни громадської думки та послаблення противника);
- психологічний вплив (застосування різноманітних психологічних технік для зміни ставлення та переконань населення);
- кібероперації (використання кіберпростору для розповсюдження пропаганди, проведення кібератак на інформаційні системи та збір розвідувальної інформації);
- цільове використання соціальних мереж (поширення наративів та здійснення масового впливу через соціальні платформи, що вигідні для держави) [79].

Типовими рисами ІПСО є узгодженість публікацій, наявність помилок на рівні фактів, логіки та мови, а також відсутність реальних авторів контенту, які зазвичай маскуються під псевдонімами на кшталт User 1991. У інтернет-просторі працівники підрозділів ІПСО, що діють на користь ворожої держави, отримали

назву «інтернет-тролі». Протягом перших тижнів війни пропагандисти активно розповсюджували повідомлення, покликані викликати паніку серед цивільного населення, зокрема закликаючи українців покидати країну. Вони поширювали такі тези, як «Люди з Києва продовжують масово виїжджати в Житомирському напрямку та на Західну Україну» або «Народні депутати та силовики СБУ залишають Київ». Також регулярно транслювались провокативні заяви про те, що українське політичне командування нібито «здало країну», а президент В. Зеленський вже покинув Україну. Хоча ці фальшиві новини швидко спростовувалися офіційними джерелами або були заздалегідь розкриті як фальшиві. Протягом року війни в Україні неодноразово поширювались чутки про можливу підготовку наступу з території Білорусі, які з кожним разом набували більш емоційного забарвлення, однак вони вже не викликають у населення такого страху, як це було на початку [80].

Науковець С. Гриняєв наводить наступні форми антиукраїнського дискурсу, який застосовують росіяни в своїх ІПСО в соцмережах та ЗМІ:

1. Створення атмосфери бездуховності й аморальності опонента, негативного ставлення до культурної спадщини противника (опис українців як фашистів, бандерівців, хунти, карателів. Формування образу України як держави без історії та військових перемог);
2. Виявлення та посилення протиріч (росіяни і українці є одним народом, разом з тим, так звані «новороси» – це не українці. Поділ на лівобережну та правобережну Україну. Формування тез, що Галичина «керує» Україною, а Томос є неканонічним);
3. Маніпулювання суспільною свідомістю соціальних груп населення країни з метою створення політичної напруженості та хаосу (як приклад «захист російськомовного населення», образ «західної» України, «Крим – наш»).
4. Підрив політичної стабільності через посилення суперечностей між партіями, громадськими об’єднаннями та рухами може стати інструментом провокації внутрішніх конфліктів, поширення недовіри між суб’єктами політичного процесу, ескалації боротьби за владу, що в окремих випадках

здатне призвести навіть до репресивних дій проти опозиційних сил або спричинити ризики внутрішньодержавного протистояння (сюди можна віднести фейки і тролінг однієї партії від імені іншої. Просування так званої «кишенькової соціології». Різна позиція партій щодо порушення Закону про декомунізацію);

5. Інспірація помилкових управлінських рішень (тут варто згадати поширення інформації про Іловайський котел та затягування виведення військ з Бахмуту та Авдіївки. Формування образу учасників бойових дій як основної загрози суспільству);
6. Дезінформація населення про роботу державних органів, підрив їхнього авторитету, дискредитація органів управління (наприклад, тези, що в «уряді всі злодії та корупціонери», «діти депутатів не служать у війську», «депутати під приводом відряджень їздять на відпочинок, а звичайні громадяни не можуть виїхати закордон» [81].

Як відзначає Ю. Горбань, у ході ІПСО проти України російська федерація застосовує широкий арсенал методів впливу на свідомість людей. Російські телеканали та соцмережі використовують доволі різноманітні прийоми, зокрема:

- подача дозованої інформації (постійне подавання інформації порціями з метою контролю над сприйняттям аудиторії);
- дезінформація (поєднання неправдивих тверджень з одночасним викривленням подій, створенням міксу фактів та особистих думок, вибіркове поданням інформації);
- використання інформаційного контексту (надання інформації без коментарів та фактів);
- перебільшення та замовчування (виголошення неправдивих чи перебільшених тверджень, а також утримання від аудиторії певної інформації) [82].

Важливо відзначити, що типовою ознакою російських ІПСО є вказівка на ігнорування українських офіційних джерел та їхнє знецінення. Так, доволі часто фейкові повідомлення супроводжують фрази «влада нічого не каже», «від нас усе

приховують», «офіційні ЗМІ мовчать» тощо, які не лише нагнітають зневіру серед населення, але й дискредитують державну владу. Якщо в новині поширюють думку, що офіційні джерела інформації не заслуговують на довіру, щось спотворюють або приховують, значить це є елемент ІПСО. Дієвим засобом фейкових наративів є теза про те, що нібито «всі ЗМІ брешуть, а я розповім вам правду». Ця фраза по-різному обіграна в маніпулятивних вкидах окупантів, що транслюють у мережі у вигляді так званих «інформаційних чуток». Експертами подібних псевдоновин є зазвичай родичі або знайомі в силових відомствах або «високих кабінетах» [83].

Окремо варто згадати про роль штучного інтелекту (ШІ) у проведенні інформаційно-психологічних операцій рф. За потреби ШІ може забезпечити автоматизацію та оптимізацію процесів ІПСО, разом з тим одночасно стаючи джерелом нових етичних, правових та безпекових викликів. За допомогою ШІ можна досить успішно проводити ІПСО використовуючи наявні медійні конфлікти, гіперболізуючи брехню та маніпуляції, швидко вигадуючи нові змісти. ШІ може швидко створювати якісний контент на задану тематику, і розповсюджувати його як звичайними програмними методами, так і з використанням ботів [84].

До використання ШІ боти зазвичай використовувались для просування реклами, забороненого контенту. Це були прості програми, які будучи швидшими за людину могли одразу після публікації контенту створювати коментарі з відповідним вмістом. Далі цей метод почали використовувати і у ІПСО, але особливого успіху він не мав через те, що бот не в змозі відповідати на коментарі реальних людей, а також його відповіді часто могли не збігатись з контентом. Свою чергою, сьогодні, ШІ змінює правила гри: він може швидко та доволі реалістично редагувати зображення за певним запитом, а також відповідати на коментарі попередньо проаналізувавши питання.

П. Діксіт у своїй статті «OpenAI shuts down tool to detect AI-written text due to low accuracy» прогнозує подальший вектор застосування ШІ у пропаганді:

- розробка інтелектуальних ботів, які здатні вести діалог, відповідати на запитання, наводити аргументи та спрямовувати співрозмовника;
- розробка більш реалістичного контенту за допомогою технології Deepfake та інших аудіо-візуальних інструментів (підробку голосу, відео та створення цифрових копій відомих осіб);
- написання статей на задану тему, використання згенерованих зображень, приховане впровадження пропагандистських наративів у тексті;
- перенавантаження цифрового простору застосуванням ботів різних типів і рівнів, з метою ускладнення фільтрації інформації для користувачів [85].

Отже, методи впливу, що використовуються в ІПСО, є настільки досконалими, що об’єкти такого впливу можуть навіть не помічати та не усвідомлювати його. У сучасній гібридній війні російська федерація активно залучає різні методи інформаційного протистояння проти України. Серед них особливе місце займає масштабне використання підконтрольних медіаресурсів, ведення контрінформаційної діяльності, поширення пропаганди через соціальні мережі та спеціальні інформаційні підрозділи, а також вплив через місцевих агентів серед цивільного населення.

Ефективна протидія таким формам впливу потребує комплексного підходу. Зокрема, важливо забезпечити широке впровадження просвітницьких програм, підвищення рівня медіаосвіти, медіаграмотності та розвиток критичного мислення серед громадян. Окремої уваги заслуговує формування сталого патріотичного світогляду, насамперед серед військовослужбовців та інших соціальних груп.

Висновки до розділу 2

Аналіз історичної динаміки поширення проросійських меседжів в Україні засвідчує факт їхньої системної та цілеспрямованої присутності в українському інформаційному просторі ще з початку 1990-х років. Ідеологічний та культурний вплив, який транслювався через російські та проросійські українські медіа, мав

на меті утвердження російського імперського образу «спільного минулого», «братніх народів» та меншовартісного статусу української культури. Згодом, після Революції Гідності, цей підхід поступово еволюціонував у потужну дезінформаційну кампанію, яка набула відкрито ворожого характеру.

Власне, після 2014 року проросійські наративи набули нових рис: вони перестали бути лише латентними і трансформувалися в відкриті інформаційно-психологічні операції, які стали частиною широкомасштабної гібридної війни росії проти України. Цей вплив ознаменувався поширенням фейкових новин, конструюванням «паралельних реальностей», делегітимізацією українських державних інституцій, а також деморалізацією та демотивацією суспільства. Особливо інтенсивним щодо поширення російського деструктивного впливу став період після російського повномасштабного вторгнення в лютому 2022 року, коли російські інформаційно-психологічні операції тісно координувалися з реальними бойовими діями.

Проведений аналіз проросійських меседжів та наративів дозволяє ідентифікувати ключові з них та умовно поділити на наступні категорії:

- про українську державність та український народ (вигаданість та штучність);
- про українське військо та сили оборони загалом (слабкість та неспроможність);
- про українську культуру та мову (відсутність самобутності);
- про російську мову, культуру та віру в Україні (гоніння та обмеження);
- про українську владу та державні органи (нелегітимність та корумпованість).

Проросійська пропаганда все ще активно використовує сакральні та історико-культурні коди, зокрема образ «русского міра», релігійне підґрунтя УПЦ МП, а також історичні алюзії на «велич СРСР». Разом з тим, у 2014-2024 роках російська інформаційна стратегія активно використовувала такі нові цифрові інструменти як штучний інтелект, діпфейки, боти тощо.

Умовно, за цільовими групами, російські пропагандистські наративи можна розділити: для внутрішньої російської аудиторії (культивація образу ворога, «священна війна», дегуманізація українців), для української аудиторії (насадження безнадії, деморалізація, викликання паніки) та для західної аудиторії (формування сумнівів у доцільності допомоги Україні, підрив довіри до українського керівництва).

РОЗДІЛ ІІІ. ПРОСУВАННЯ РИТОРИКИ ПРО РОСІЙСЬКО-УКРАЇНСЬКУ ВІЙНУ В ЗАХІДНОМУ ІНФОПРОСТОРІ

3.1. Вплив російської пропаганди на формування іміджу України закордоном

Інформаційний простір у 21 столітті перетворився на поле боротьби за емоції та людські переконання. У цьому контексті війна між росією та Україною, яка триває з 2014 року, набуває не лише військового, а й потужного комунікаційного характеру. Особливого значення набуває інформаційно-психологічний вплив росії, спрямований на формування або спотворення міжнародного іміджу України. Сьогодні російська федерація, як держава-агресор, активно використовує інструменти пропаганди та дезінформації для формування негативного іміджу України у свідомості закордонної аудиторії та закордонних партнерів. Власне ці кроки і дозволяють росії виправдовувати власні дії, послаблювати міжнародну підтримку України та, як наслідок, просувати власну геополітичну риторику.

Для аналізу впливу російської пропаганди на формування іміджу України спершу варто розібратися з терміном «імідж». Так, у контексті держави термін «імідж» широко застосовується в дослідженнях міжнародних відносин з 1950-х років. Одним із перших, хто запровадив це поняття в розрізі аналізу ворожих відносин між країнами, був К. Боулдінг. На його думку, імідж – це певний стереотип поведінки, що формується не на основі реальних фактів, а через уявлення, ілюзії та думки, які люди створюють про себе, своє минуле і майбутнє. Такий образ може впливати як на індивідуальну, так і на колективну поведінку цілих націй [86].

Слово «імідж» походить з англійської мови і перекладається як «образ» (англ. «image»). Його можна трактувати як «цілеспрямовано сформований образ», «емоційно забарвлене уявлення, що склалося у масовій свідомості та набуло стереотипного характеру», або як «усвідомлене сприйняття чогось

побаченого раніше – конкретного чи абстрактного». Ф. Котлер визначає імідж країни як сукупність переконань, ідей і вражень, які виникають у людей щодо конкретної держави [87].

Науковець Т. Нагорняк в своїй роботі «Публічний імідж України в умовах невизначеності» підкреслює, що у колективній свідомості населення можуть фікстуватися різні аспекти іміджу держави, серед яких виокремлюються наступні:

- *уявлення про державну владу та її очільників*, що включає сприйняття лідерів як ефективних або неефективних, харизматичних або відчужених від народу;

- *образ політичної системи*, що охоплює рівень демократичності, стан дотримання громадянських прав, ефективність правових і соціальних гарантій, прозорість виборчих процесів та легітимність інститутів влади;

- *імідж економічної стабільності*, що визначається економічними показниками, зокрема рівнем інфляції, стабільністю національної валюти, доступністю інвестицій і загальним інвестиційним кліматом;

- о*браз обороноздатності держави*, включаючи стан збройних сил, військово-промислового комплексу, ефективність стратегічної комунікації, інформаційної політики та системи національної безпеки;

- *зовнішньополітичне позиціонування*, яке пов’язане з активністю на міжнародній арені, захистом національних інтересів, присутністю в глобальних медіа, репутацією дипломатичних представників;

- *соціокультурна репрезентація*, яка базується на автентичних рисах країни, культурному багатстві, локальних традиціях, а також сучасних досягненнях у мистецтві, науці, спорті;

- *уявлення про якість життя та перспективність розвитку,* що включає умови для проживання, самореалізації, екологічний стан, рівень освітніх та інфраструктурних послуг [97].

Для України, власне, ключовим завданням є формування публічного образу країни безпосередньо її офіційними інституціями, адже за умови відсутності

цілісної державної стратегії у сфері брендингу чи іміджевої політики, виникає ризик того, що уявлення про державу формуватимуть сторонні політичні актори.

Як зауважує С. Гуцал, до 2015 року в українському науковому та експертному середовищі фактично не існувало чітко артикульованого змісту понять «публічна дипломатія» та «стратегічні комунікації». Ці концепти залишались не до кінця зрозумілими навіть для представників органів державної влади. Таку ситуацію можна пояснити насамперед тим, що впродовж тривалого часу в Україні була відсутня послідовна інформаційна політика, спрямована на підтримку та просування національних інтересів закордоном. Всі подібні ініціативи мали фрагментарний, несистемний характер та не були інтегровані у загальнодержавну політику, також часто були реакцією на зовнішні події, а не проактивним інструментом [98].

Сучасні дослідники дедалі більше звертають увагу на роль інформаційних технологій, цифрових платформ і політичної комунікації у гібридних конфліктах. У науковому дискурсі сформувалась окрема галузь, присвячена вивченню інформаційної агресії росії. Зокрема, дослідник П. Померанцев у своїй роботі «Nothing is True and Everything is Possible» наголошує на постмодерній природі російської пропаганди, яка руйнує саму ідею правди [88]. Своєю чергою, дослідник А. Рац у своїх публікаціях акцентує увагу на стратегіях протидії гібридним загрозам з боку росії у сфері інформації, акцентуючи увагу на російському впливі на формування іміджу інших країн [89].

З українського боку, важливі внески в дослідження даної тематики зробили Я. Цифра та Н. Білоусова, які аналізували еволюцію іміджу України в міжнародному просторі до та після повномасштабного вторгнення військ рф в 2022 році [90]. Системний огляд впливу російської пропаганди на імідж України також представлений у працях Ю. Отлана, який вивчає дипломатичні сигнали і наративи на міжнародному рівні [91].

Відзначимо, що російська пропаганда має глибокий та системний вплив на формування міжнародного іміджу України. Пропагандистські наративи спрямовані на делегітимізацію української державності та української влади,

представлення війни як «внутрішнього громадянського конфлікту», а не агресії рф, і формування скептицизму щодо європейських прагнень України серед європейських кіл. Основними інструментами російської пропаганди є дезінформація, маніпуляції в соціальних мережах, використання псевдоекспертних груп і просування проросійського дискурсу через ЗМІ, дипломатію та культурні платформи.

Російська пропаганда, на відміну від класичних форм дезінформації, функціонує не лише як ретранслятор неправдивих новин, а як система, що формує альтернативну реальність, яка здатна адаптуватися до кожного регіону відповідно до його історичного, соціального та політичного контексту. Відтак, одні й ті самі меседжі можуть сприйматися по-різному в Західній Європі, на Балканах, у Латинській Америці чи в Африці.

Нижче хочемо подати кілька ключових пропагандистських наративів росії, які остання поширювала закордоном:

1. «Україна – нацистська (фашистська) держава» (Німеччина, Греція, Сербія, частково Італія, Аргентина). Цим наративом росія виправдовує своє вторгнення та називає його «денацифікацією», стверджуючи, що українська влада пов’язана із неонацистськими угрупованнями, зокрема «Азовом». Власне, у Німеччині, країні з чутливою історією щодо нацизму, такі звинувачення викликають емоційний відгук серед населення. В Греції й Сербії ж наявне політичне підґрунтя проросійських симпатій і антизахідних настроїв [92].

2. «Україна є маріонеткою Заходу» (Франція, Угорщина, Болгарія, Індонезія, Бразилія, ПАР). В цьому наративі російська пропаганда зображає Україну як «інструмент НАТО та США», який не має власного суверенітету. У Франції та Угорщині цей наратив підсилюється антиамериканськими та євроскептичними поглядами. У країнах Глобального Півдня цей меседж резонує з постколоніальними уявленнями про зовнішнє втручання та імперіалізм [91].

3. «Триває громадянська війна, а не військове вторгнення» (Італія, Словаччина, Чехія, Мексика). В цьому наративі замість визнання російської агресії, конфлікт подається як «внутрішній розкол» між Сходом і Заходом

України. Цей наратив лягає на попередні уявлення про «дві України» (західну – проєвропейську і східну – проросійську). В період до 2022 року в Чехії значна частина проросійських акаунтів просувала ідею, що «Київ бомбить власних громадян», особливо через дезінформацію кампанію про події в Одесі 2014 року [93].

4. «Україна як загроза для економічної стабільності, або біженці як безпекова проблема» (Польща, Латвія, Італія, Німеччина). Цей наратив зображує українських біженців як тягар для економік країн ЄС або навіть «провокаторів злочинності». Він підживлює ксенофобські або націоналістичні настрої, особливо у періоди економічної нестабільності. У Польщі, попри сильну підтримку України, після осені 2022 року спостерігався сплеск антиміграційних заяв [90]. Так, у Telegram-каналах, орієнтованих на Польщу, поширювалися фейки про «українських біженців, які не хочуть працювати, однак претендують на фінансову допомогу».

5. «Західна підтримка України веде до глобальної кризи» (Індія, Єгипет, Туреччина). Цим наративом просуваються думки, що саме підтримка України Заходом викликає інфляцію, а також енергетичну та продовольчу кризу, і аж ніяк не обмеження пересування українських суден з завантажених продовольством через Чорне море та ураження об’єктів енергетичної інфраструктури. Таким чином, у країнах, які залежать від імпорту зерна чи енергоносіїв, цей наратив надає просте пояснення складних економічних проблем. Наприклад, RT Arabic та RT Africa у 2022–2023 роках поширювали меседжі про те, що українська влада блокує зерно, яке «потрібне голодуючим в Африці» [94].

6. «Україна — корумпована держава» (США, Італія, Нідерланди, Індія).

Цим наративом російська пропаганда нав’язує образ України як повністю корумпованої, неефективної та мафіозної держави, що не заслуговує на підтримку Заходу. Основна мета цього меседжу – викликати зневіру у доцільності військової та фінансової допомоги Києву.

У країнах з високим рівнем податкового навантаження або де поширені антисистемні настрої (США, Італія), пропаганда апелює до «турботи про своїх»,

ставлячи питання: «Чому ми маємо платити за чужу корупцію?» У країнах, які мають власні проблеми з прозорістю влади (Індія, Аргентина), такий дискурс викликає певне віддзеркалення і знижує емпатію до України [91].

Окремо варто дослідити канали поширення російської пропаганди за кордоном. Зазвичай російська пропаганда використовує багаторівневу інфраструктуру впливу на свідомість людей, що поєднує державні медіа, дипломатичні ресурси, соціальні мережі, псевдоаналітичні центри, культурну дипломатію та цифрові платформи. Особливістю цього підходу є його адаптивність, де кожен інструмент підлаштовується під цільову аудиторію, її мову, політичні контексти й культурні коди.

До першої і найбільшої категорії джерел російської пропаганди закордоном варто віднести державні медіа, такі як «Russia Today», «Sputnik» та «РИА Новости». Вищезгадані державні російські медіа транслюють «альтернативний» погляд на міжнародні події, підтримуючи так званий «антизахідний баланс». Для розуміння масштабів поширення російської пропаганди, варто зазначити, що «Russia Today» функціонує в більш ніж 100 країнах і має власні регіональні редакції (RT Arabic, RT Africa, RT Deutsch, RT en Español), а медіа «Sputnik» в основному зорієнтоване на радіоефіри, локальні інтерв'ю та аналітичні матеріали в популярному для кожного регіону стилі.

До другої категорії джерел варто віднести пропагандистський вплив через соціальні мережі та цифрові платформи. Цей вплив спрямований на масове просування контенту та характеризується анонімністю джерел, формуванням псевдоспільнот, тролінгом, бот-атаками, кампаніями в TikTok, Telegram, Facebook та YouTube.

Так, найвідомішою «фермою тролів» згідно дослідження проведеного ГО «Інтерньюз-Україна» стала «Internet Research Agency» з дислокацією у м. Санкт-Петербург. Не менш шкідливими в плані просування пропаганди є бот-мережі, тобто автоматизовані мережі акаунтів, які лайкають, репостять і створюють ілюзію народної підтримки та співпраця з так званими лідерами думок «influencer-ами» [95]. Цікаво, що з 2022 року у TikTok поширювались відео з

хештегами *#UkraineNazis*, *#ZelenskyDictator* з мільйонними переглядами. Доволі часто ці відео публікувались через акаунти, що раніше постили розважальний контент [96].

Третьою категорією джерел російської пропаганди є дипломатія і так звана «м'яка сила». Російська влада через посольства, власні культурні центри, такі заходи як «дні російської мови», освітні програми, просуває пропаганду у вигляді «традиційних цінностей» або «антиглобалізму». Так, у Сербії, Боснії і Герцеговині, Вірменії російські посольства активно підтримували місцеві прокремлівські медіа та проводили культурні події, де Україна згадувалась як «державне утворення без власної історії» [91].

Четвертою категорією є псевдоаналітичні центри та «експерти» функцією яких є створення видимості академічної легітимності пропагандистських меседжів через звіти, конференції та експертні коментарі. У Німеччині так звані think tanks на кшталт German-Russian Forum систематично публікували матеріали про «громадянську війну в Україні», які потім цитувались в місцевих ЗМІ [89].

Загалом, варто підкреслити, що розповсюдження проросійських інформаційних наративів стосовно України є ключовим інструментом у межах сучасної гібридної війни. Таке інформаційне втручання суттєво впливає на міжнародне уявлення про Україну, формуючи викривлене сприйняття її внутрішньої ситуації та зовнішньополітичної позиції.

Один із головних механізмів дії російської пропаганди полягає у поширенні дезінформації, вигаданих сюжетів та спотворених трактувань подій. Через такі вкиди створюється негативний інформаційний фон навколо України, що супроводжується навмисним перебільшенням внутрішніх проблем, політичної нестабільності або загроз для безпеки. Разом з тим, домінування держави над вітчизняними інформаційними ресурсами забезпечує їй монопольну можливість формувати суспільну думку як всередині країни, так і на зовнішніх аудиторіях.

Інформаційна кампанія рф системно працює над дискредитацією українців як нації, нав'язуючи образ радикалізму, агресивного націоналізму чи навіть

екстремізму. Такі підходи спрямовуються, в першу чергу, на підрив міжнародної довіри до України та її громадян. Пропагандистські меседжі також мають на меті формування або зміну зовнішньополітичних рішень інших держав, які безпосередньо можуть впливати на обсяг міжнародної допомоги, підтримку України в глобальних інституціях або на рівень дипломатичної взаємодії.

Підсумовуючи варто відзначити, що активне поширення проросійських дезінформаційних наративів стосовно України закордоном суттєво впливає на те, як країна сприймається світовою спільнотою. Такий інформаційний тиск здатен не лише гальмувати процеси міжнародної інтеграції України до НАТО та ЄС, а й послаблювати її міжнародну підтримку. Протидія цим викликам вимагає подальшого зміцнення глобального партнерства в галузі інформаційної безпеки та формування спільних міжвідомчих спеціалізованих підрозділів з питань формування українського іміджу, до яких мають потрапити як представник Міністерства закордонних справ України, Міністерства культури та стратегічних комунікацій, так і представники інших державних органів, які в своїй діяльності взаємодіють з міжнародними партнерами.

3.2 Культурна дипломатія як засіб просування національних наративів закордоном

Очевидним є той факт, що оцінка успішності української «інформаційної дипломатії» повинна полягати в її спроможності диференціювати методи впливу та її здатності адаптуватися до регіональних умов та викликів. В залежності від того, які меседжі просуває російська федерація в тому чи іншому регіоні світу, українські посольства та інші дипломатичні відомства, освітні установи, українські закордонні спілки та об’єднання повинні формувати швидку відповідь, яка покликана апелювати до місцевого контексту, політичної культури та інформаційних звичок населення країни-реципієнта, інакше ця комунікація буде неуспішною.

Варто відзначити, що поняття культурної дипломатії станом на сьогодні не має єдиного тлумачення серед дослідників і часто аналізується в контексті публічної дипломатії або як складова міжкультурного та міжнародного діалогу. Ще у 1930-х роках американський аналітик Ф. Барггорн одним із перших запропонував визначення цього феномену, підкреслюючи його інструментальну функцію. Останній стверджував, що «культурна дипломатія є формою цілеспрямованого впливу, де культурні контакти використовувалися з пропагандистською метою» [99]. Згодом більш концептуалізоване трактування цього поняття запропонував політолог М. Каммінгс, який розширив розуміння культурної дипломатії, розглядаючи її як взаємний процес обміну культурними надбаннями, зокрема ідеями, знаннями, ціннісними орієнтирами, переконаннями, традиціями та інформаційними ресурсами. Такий обмін, згідно з Каммінгсом, слугує важливим інструментом для побудови міждержавного порозуміння та розвитку конструктивних міжнародних відносин [100] .

В іншій площині поняття культурної дипломатії розглядається як сукупність заходів, що ґрунтуються на міжкультурному обміні ідеями, цінностями, традиціями та іншими елементами культурної самобутності. Очевидно, що така діяльність покликана не лише налагоджувати міжнародні комунікації, але й сприяти зміцненню міждержавних відносин, поглибленню соціокультурної співпраці та просуванню стратегічних національних інтересів у глобальному контексті та протидії дезінформації та пропагандистському впливу інших зацікавлених сторін [101].

Відзначимо, що 24 березня 2021 року була затверджена «Стратегії публічної дипломатії Міністерства закордонних справ України на 2021–2025 роки», в якій публічна дипломатія розглядається як важлива складова системи стратегічних комунікацій держави. Вона трактується не лише як канал міждержавного спілкування, а як інструмент впливу на формування громадської думки закордоном, спрямований на підтримку національних інтересів і реалізацію ключових зовнішньополітичних завдань. В цьому документі одним із ключових векторів публічної дипломатії визначено культурну дипломатію, поряд

з економічною, кулінарною, спортивною, цифровою, науково-освітньою та експертною. Особлива увага приділяється її ролі у міжнародному інформаційному спротиві російській агресії. Саме через інструменти культурної та експертної дипломатії українська держава доносить до іноземної аудиторії важливі наративи про порушення прав людини на тимчасово окупованих територіях, необхідність деокупації, загрози дезінформації тощо [104].

Таким чином, культурна дипломатія постає не лише як засіб просування мистецтва чи національної ідентичності, але й як дієвий механізм «м'якої сили», покликаний формувати позитивне ставлення до України, розширювати міжнародну підтримку та сприяти глобальному розумінню української позиції в умовах затяжного геополітичного конфлікту.

Як зазначає В. Кубко, в розрізі культурної дипломатії важливе місце посідає ефективна взаємодія між закордонними дипломатичними установами України та широким колом державних і недержавних культурних інституцій. До цих інституцій дослідниця відносить Український інститут, Міністерство культури та стратегічних комунікацій, Український культурний фонд, Державне агентство з питань кіно, Державне агентство з питань мистецтв та мистецької освіти, Український інститут книги, а також Український інститут національної пам'яті. До процесу також активно залучаються іноземні культурні установи, міжнародні донорські організації та діаспорні об'єднання, що створює багаторівневу платформу для просування українських наративів за кордоном [105].

Культурна дипломатія постає одним з ключових методів протидії російській дезінформації. Україна просуває українську культурну дипломатію через Український інститут, інформаційно-культурні центри при посольствах, співпраця з книжковими видавництвами, взаємодіючи з національними засобами масової інформації, економічними, промисловими та технологічними форумами, активно взаємодіючи з українською діаспорою та емігрантами і т.д.

У контексті гібридної агресії, яку веде російська федерація проти України, культурна дипломатія стала важливим інструментом, що сприяє зміцненню національної ідентичності та міжнародного авторитету держави. Як вже

зазначалося раніше, російська гібридна війна характеризується поєднанням традиційних збройних методів із нетрадиційними підходами, зокрема інформаційними атаками, маніпуляціями свідомістю, інформаційно-психологічними операціями та нав'язуванням чужих культурних кодів. Усе це здійснюється з метою дестабілізації України, а також послаблення її суверенітету та міжнародної підтримки.

Дослідник Н. Дубовик підкреслює, що в умовах подібних викликів культурна дипломатія набуває особливої актуальності як інструмент «м'якої сили», здатний формувати позитивний міжнародний імідж України, руйнувати хибні стереотипи та протистояти зовнішнім інформаційним загрозам. Презентуючи світові багатство своєї культурної спадщини, національне мистецтво, мову, традиції та суспільні цінності, Україна конструює власний автентичний образ, який здатний конкурувати з навмисно викривленими образами, які активно просуваються через російську пропаганду [102].

Культурний обмін, креативні мистецькі проєкти, міжнародні виставки, фестивалі та інші формати міжкультурної комунікації не лише створюють умови для діалогу між країнами, а й дають можливість Україні акцентувати увагу світової спільноти на реальних загрозах, яким вона протидіє. Власне, через ці платформи відбувається не тільки популяризація української культури, але й посилення глобального розуміння природи сучасного конфлікту.

Попри значний потенціал української культури та відповідно культурної дипломатії, в Україні вона все ще реалізується переважно завдяки ініціативам окремих представників культурного середовища, а не через цілісну та системну політику з боку державних інституцій. Українські митці, письменники, музиканти, архітектори, скульптори та інші діячі культури нерідко самостійно виступають амбасадорами України закордоном, популяризуючи її культурну спадщину та привертаючи увагу до сучасних викликів, з якими зіштовхується Україна в умовах війни.

Водночас варто відзначити й приклади державної залученості до процесів культурної дипломатії. Одним із таких позитивних кейсів є діяльність першої

леді України О. Зеленської, яка стала ініціаторкою низки культурних та гуманітарних проєктів. Так, остатньою у співпраці з Офісом Президента України, Міністерством закордонних справ, Міністерством культури та інформаційної політики та Українським інститутом книги, був започаткований проєкт «Українська книжкова поличка», який був поширений на понад 46 країн. Метою цього проєкту було знайомство закордонної аудиторії з українською літературою, філософією, історією з метою протидії російській історичній пропаганді. Важливо, що усі книжки які долучають до «Української книжкової полички» намагаються перекладати національними мовами або принаймні англійською [103].

Окремо варто розглянути участь українських музичних гуртів на пісенному конкурсі «Євробачення», які стали не лише мистецьким проявом, а й потужним інструментом культурної дипломатії, зокрема в контексті анексії Криму росією. Цей міжнародний майданчик, що охоплює мільйони глядачів у різних країнах, дозволив Україні донести до світу важливі політичні та історичні меседжі через культуру, музику й символіку. Найяскравішим прикладом такого впливу стала перемога співачки Джамали у 2016 році з піснею «1944», яка зверталася до трагічної депортації кримських татар радянською владою. Попри те, що твір офіційно не мав прямого політичного підтексту, його зміст однозначно асоціювався з подіями навколо незаконної анексії Криму в 2014 році. Як результат, цей виступ не тільки нагадав світовій аудиторії про порушення прав корінного народу Криму, а й активізував обговорення теми українського суверенітету та територіальної цілісності на європейських політичних майданчиках.

Згодом у 2022 році перемога гурту «Kalush Orchestra» з піснею «Stefania», присвяченою матері, у поєднанні з яскравими елементами українського фольклору, набула нового змісту в умовах повномасштабної війни. Після свого фінального виступу гурт відкрито закликав допомогти захисникам з «Азовсталі», що стало прикладом поєднання культурного виступу з політичним меседжем у гуманітарному ключі. Таким чином, «Євробачення» перетворилося для України

на стратегічний інструмент «м'якої сили», особливо у питанні інформаційного впливу щодо Криму та агресії з боку росії.

Ініціативи, що спочатку мали переважно просвітницький та мистецький характер, в умовах повномасштабної війни з росією набули нових змістових акцентів. Культурна дипломатія в такому форматі стала важливим інструментом зміцнення зовнішньополітичних позицій України, підтримки її позитивного іміджу у світі та протидії пропагандистському тиску з боку держави-агресора.

Важливим кроком для просування української культурної дипломатії стало заснування Українського інституту в 2017 році. Дана інституція орієнтується на п'ять ключових цілей: підвищення впізнаваності України у світі, формування стабільного попиту на експертну взаємодію з українськими суб'єктами, розширення міжнародної співпраці у сфері культури, науки та освіти, активну інтеграцію до глобальних культурних процесів і популяризацію української мови. Власне цей інституційний розвиток відбувався паралельно з появою нових гуманітарних структур, як-от створення Українського інституту книги, Національного фонду досліджень України, а також модернізацією вже існуючих платформ, таких як Мистецький Арсенал або Довженко-Центр. Це свідчить про цілеспрямовану трансформацію гуманітарної політики держави, в якій культурна дипломатія розглядається як системний інструмент просування національних інтересів і формування позитивного міжнародного іміджу України [105].

У своїй науковій роботі «Основні засади і специфіка реалізації культурної дипломатії України в умовах війни» дослідниця О. Гречко відзначає, що до 2014 року культурна дипломатія України характеризувалась низьким рівнем ефективності, що було зумовлено низкою системних чинників. Серед ключових причин є відсутність чіткої політичної волі у державного керівництва щодо розвитку цього напряму, нестача стратегічного планування, недофінансування сектору, а також відсутність комплексного бачення цілей та завдань у сфері міжнародної культурної комунікації.

Лише після анексії Криму та тимчасової окупації території Донецької та Луганської областей у 2014 році, а також повномасштабної агресії російської

федерації у 2022 році спостерігається активізація української культурної дипломатії, зумовлена зростанням уваги міжнародної спільноти до подій в Україні. Боротьба українського народу за незалежність та територіальну цілісність, а також героїзм Збройних Сил України та Сил оборони загалом, стали предметом широкого обговорення у світовому медіапросторі. Жахливі воєнні злочини та масштабні руйнування, спричинені російськими окупаційними військами, викликали співчуття та солідарність міжнародних партнерів з Україною. У таких умовах культурна дипломатія стала ефективним інструментом привернення уваги до українських наративів на міжнародному рівні [106].

У контексті повномасштабної війни особливу роль відіграє кінематограф, який стає потужним засобом репрезентації української ідентичності. Міністерство культури та стратегічних комунікацій України відзначає необхідність міжнародного представлення вітчизняного кінопродукту як одного з пріоритетів державної культурної політики. З 2014 по 2021 рік стрічки про російсько-українську війну в основному мали локальний характер з акцентом на українського глядача та слабко репрезентувалися на міжнародній арені, найбільш відомими можна назвати: «Кіборги» (2017), «Позивний «Бандерас» (2018), «Іловайськ 2014» (2019), «Черкаси» (2019), «Наші котики» (2020). Лише опісля повномасштабного вторгнення українські кінострічки акцентували свою увагу на поширенні для міжнародних глядачів.

Одним із найрезонансніших прикладів української культурної дипломатії в кінематографі став документальний фільм «20 днів у Маріуполі», режисером якого виступив М. Чернов. Стрічка була створена на основі унікальних відеоматеріалів, зафіксованих знімальною групою Associated Press у перші три тижні російської облоги Маріуполя в лютому-березні 2022 року. Фільм показує війну зсередини через зруйновані житлові квартали, переповнені лікарні, сцени відчаю та героїзму місцевого населення, яке опинилося в гуманітарному колапсі. Дана стрічка була відзначена премію «Oscar» за найкращий повнометражний документальний фільм і премією «Bafta» за найкращий документальний фільм. Дана стрічка стала не просто кінофіксацією злочинів російської армії, а символом

правдивого голосу України у світі, здатного транслювати об'єктивну інформацію, формувати глобальну думку та стимулювати моральну й політичну підтримку. Також варто відзначити кінострічку «Timestamp», яка була показана на «Berlinale» у 2025 році та розповідає про життя українських школярів під час війни, а також фільм «The Grave», який транслювався у Великій Британії та розповідає про воєнні злочини росіян в Ізюмі, Харківській області, поєднуючи свідчення жертв з коментарями українських слідчих та розвідників.

На виконання завдання щодо протидії ворожій дезінформації шляхом культурної дипломатії урядом України у 2017 році було створено нову інституцію – Український інститут. Це державна установа, діяльність якої спрямована на підвищення рівня розуміння та сприйняття України у світі, а також на розвиток культурних зв'язків із іншими державами.

Сьогоднішня діяльність Українського інституту базується на широкому залученні різних учасників – державних структур, громадянського суспільства, бізнес-кіл, міжнародних експертів та представників української діаспори. У результаті передбачається формування сучасного, унікального та привабливого образу України для потенційних партнерів, створення змістовних інформаційних повідомлень, орієнтованих на розвиток і діалог, а також впровадження механізмів трансляції українських цінностей.

Основними стратегічними цілями Українського інституту відповідно до Стратегії на 2020-2024 роки визначено:

1. Покращення обізнаності та впізнаваності України серед іноземної аудиторії. Інститут поширює знання про Україну, залучає широке коло громадян інших країн до діалогу, забезпечує постійну присутність країни в інформаційному просторі та просуває українські наративи.
2. Формування сталого попиту на фахову взаємодію з Україною. Інститут підтримує постійний інтерес до України серед міжнародних експертних і професійних спільнот, надаючи посередницьку та аналітичну підтримку.
3. Посилення потенціалу українських суб'єктів культури, освіти, науки та громадянського суспільства у міжнародному співробітництві. Через

інтеграцію культурної сфери в міжнародні процеси Інститут сприяє зростанню ефективності зовнішнього представництва країни.

4. Розширення участі України у актуальних світових культурних процесах. Програми Інституту спрямовані на зміцнення ролі України у міжнародному культурному діалозі, забезпечення її присутності на ключових культурних, наукових, освітніх і політичних платформах світу.
5. Збільшення використання української мови в міжнародному просторі. Інститут посилює присутність української мови у публічному та професійному середовищах за кордоном [106].

Важливо відмітити, що українські театральні трупи, музичні гурти та інші культурні діячі в своїх виступах закордоном мають не меті не лише «нагадати» про Україну, але й зібрати кошти на підтримку Сил оборони України. Так, у 2022 році у своєму літньому європейському турі гурту «Океан Ельзи» вдалося зібрати понад 19 мільйонів гривень, які згодом були направлені на потреби українських оборонців [107]. Інший український гурт «Курган і Агрегат» у своєму осінньому турі Європою (Польща, Угорщина, Словаччина, Австрія, Німеччина й Нідерланди) в 2024 році зібрав понад 15 мільйонів гривень, які також направив на потреби Сил оборони України [108].

Українські автори отримують міжнародне визнання і стають лауреатами престижних літературних премій. Лауреатом європейської літературної премії «Vilenica» у 2017 році став Юрій Андрухович, Центральноєвропейської літературної премії «Ангелус» у різні роки ставали Тетяна Малярчук (2021) та Сергій Жадан (2022), лауреатом літературної премії імені «Джозефа Конрада-Коженьовського» у 2024 році став Андрій Любка. Власне, як вже зазначалося раніше, переклад українських книжок наближає європейського читача до українських контекстів та змістів. Кожна перемога українського представника на спортивних змаганнях, кожна згадка в закордонному медіа примушує говорити про Україну та українців в позитивному контексті та руйнувати стіну стереотипів та наративів, яку вибудовує росія.

Варто наголосити на обмеженості розуміння українських меседжів іноземними партнерами, які не володіють контекстом, тому одним з ключових завдань Міністерства культури та стратегічних комунікацій України, на думку автора, є мотивація українських митців створювати якісний англомовний контент, який буде зрозумілий закордонним глядачам та слухачам.

Особливий інтерес для цього дослідження становить реалізація росією діяльності у сфері культурної дипломатії через свої представництва в Європі. Федеральне агентство «Росспівробітництво» реалізує цю діяльність, зокрема під брендами «Російський дім» та «Російський центр науки і культури» (РЦНК). На сьогоднішній день цей орган має 72 центри «науки та культури» в 62 країнах світу, а також представників у складі дипломатичних місій у 22 країнах. Крім того, для «просування за кордоном зовнішньополітичних інтересів росії, а також формування сприятливого для неї громадського, політичного і ділового середовища» 2 лютого 2010 року указом президента В. Путіна була створена неурядова організація – «Фонд підтримки публічної дипломатії імені Горчакова» [109].

Російська пропаганда діє за досить передбачуваною логікою: навіть якщо міжнародна спільнота рішуче засуджує воєнні злочини, скоєні росією, її культурна продукція, така як фільми, музика, література, і надалі активно циркулює в Європі, США та навіть в Україні. Використовуючи інструменти так званої «м'якої сили», Кремль прагне пом'якшити сприйняття власних дій та здобути прихильність закордонної аудиторії. У цьому контексті структури на кшталт «Росспівробітництва», «Російського миру» та Фонду Горчакова щорічно проводять культурні події, форуми, обміни й інші заходи, під час яких транслюється спотворена версія подій, зокрема щодо війни в Україні.

На останок відзначимо, що окрему роль у формуванні інтелектуального іміджу України також відіграють потужні науково-культурні центри української діаспори, які існують як відокремлені осередки чи науково-дослідні підрозділі іноземних університетів. До найбільш відомих можемо віднести: Канадський інститут українських студій, Український науковий інститут Гарвардського

університету, Український вільний університет у Мюнхені та низку інших установ, які системно працюють над просуванням української культури й академічної спадщини закордоном.

Висновки до розділу 3

Очевидним залишається той факт, що росія системно транслює свої дезінформаційні наративи, спрямовані на дискредитацію України в очах міжнародної спільноти. Поширення таких російських наративів в західному інфопросторі як «Україна – нацистська держава», «Україна – маріонетка Заходу», «громадянський конфлікт», «економічна загроза», «корупційна країна», формують негативне сприйняття України закордоном як об'єкта нестабільності, який не заслуговує на міжнародну підтримку та на своє існування загалом. Росія системно поширює вищезгадані та інші наративи через багаторівневу інфраструктуру (державні медіа, дипломатичні платформи, соціальні мережі, бізнес-форуми, бот-мережі, псевдоаналітичні центри, культурну дипломатію тощо).

Однією з найнебезпечніших рис російської інформаційної експансії залишається її гнучкість, рівень фінансування та здатність адаптуватися до політичних, історичних та культурних особливостей цільових країн. В результаті цих факторів одні й ті самі меседжі набувають різного забарвлення залежно від регіонального контексту, що доволі сильно підвищує ефективність маніпуляцій.

У межах цього розділу особлива увага була приділена потенціалу української культурної дипломатії щодо протидії російській дезінформації. З допомогою так званої «м'якої сили», тобто музики, кіно, літератури, міжкультурних обмінів, театральних вистав, Україна не лише демонструє автентичність і багатство своєї культури, а й ефективно комунікує з закордонною аудиторією, де транслює суть та передумови російсько-української війни.

Після 2014 року, а особливо після 2022 року, Україна почала формувати інституційне підґрунтя культурної дипломатії: було засновано Український

інститут, оновлено та удосконалено стратегії Міністерства закордонних справ, а також запущено проєкти на кшталт «Українська книжкова поличка», UkraineNow. Участь у конкурсі «Євробачення» та інші заходи та проєкти культурного спрямування системно посилюють глобальну впізнаваність української позиції та ідентичності. Культурна дипломатія дозволяє Україні ефективно протидіяти російській дезінформації та пропаганді закордоном.

У фокусі української культурної дипломатії опинилися такі кінострічки як, зокрема, «20 днів у Маріуполі», які доносять правду про війну до світової аудиторії та стають номінантами на престижних світових конкурсах. Як результат, такі продукти згодом перетворюються на інструменти стратегічної комунікації, що викликають емоційну реакцію та стимулюють міжнародну солідарність з Україною.

Однак, навіть попри позитивну динаміку, автор дослідження акцентує увагу на тому, що українська інформаційна політика часто залишається реактивною та доволі фрагментарною, що в першу чергу спирається на обмежене фінансування та відсутність стратегічної реалізації проєктів. Окремою проблемою залишається відсутність належної координації між державними органами, що створює інформаційні прогалини, які продовжує використовувати російська пропаганда.

Автор акцентує увагу на тому, що для ефективної протидії російському інформаційному впливу в глобальному інформаційному просторі критично необхідним є створення міжвідомчих механізмів національної інформаційної безпеки, які будуть залучати не лише дипломатичні канали, а й інституції культури, медіа, кіно, науки та власне діаспору. Водночас вкрай важливо формувати глобальні плани протидії дезінформації, які поширюють авторитарні режими.

ВИСНОВКИ

Підбиваючи підсумки варто відзначити, що в ході російсько-української війни, яка триває з 2014 року та перейшла в фазу повномасштабного вторгнення у 2022 році, український медіапростір перетворився на стратегічний фронт сучасної гібридної війни. Пропагандистські кампанії російської федерації, просуваючи свої наративи та меседжі, стали одним із ключових викликів для національної безпеки України, особливо в аспектах інформаційної стабільності, мобілізаційної готовності, цілісності громадської думки та довіри до державних органів. Через цілеспрямовану інформаційну експансію як в Україні, так і закордоном, агресор не лише деморалізує українське суспільство та намагається зломити український опір, а свідомо, формуючи хибні уявлення, обмежує підтримку України міжнародною спільнотою в військовому та економічному аспектах.

Однією з ключових проблем, зафіксованих у дослідженні, є системне використання російською федерацією дезінформації як інструменту впливу на міжнародну аудиторію. Створення викривленого іміджу України, поширення хибних трактувань російсько-української війни як «громадянської війни або конфлікту», приписування українцям нацистської ідеології, нав’язування образу «маріонетки Заходу», «корумпованої влади» та «економічної загрози для Європи», сприяє делегітимізації української державності в очах закордонних партнерів. Власне, такі російські меседжі та наративи поширюються через багаторівневу інфраструктуру передачі дезінформації, починаючи від державних медіа та анонімних Telegram-каналів, завершуючи дослідженнями псевдоаналітичних центрів та дипломатичними представництвами, що говорить про координований характер російських інформаційно-психологічних операцій.

Автор підкреслює думку, що протидія російській дезінформації має розглядатися як невід’ємна складова концепції національної та інформаційної безпеки України. В умовах гібридної війни інформаційна безпека набуває не лише правового чи технічного (захист інформації в інформаційно-

комунікаційних системах) характеру, а передусім постає політичним завданням, яке передбачає здійснення стратегічного планування, міжвідомчу координацію та активну участь громадянського суспільства. В цьому контексті критично важливими постають розвиток медіаграмотності серед населення, формування культури критичного мислення та зміцнення довіри до джерел інформації, які в свої діяльності проводять так званий «fact-checking».

Особливу увагу в цьому дослідженні приділено культурній дипломатії як одному з ключових засобів комунікаційної протидії російській дезінформації закордоном. Такі українські ініціативи, як-от діяльність Українського інституту, проєкти «Українська книжкова поличка», фільм «20 днів у Маріуполі» та інші кінострічки, музичні виступи на Євробаченні, перемоги в престижних міжнародних літературних конкурсах, демонструють надзвичайну ефективність так званої «м'якої сили» в контексті стратегічних комунікацій. Саме ці ініціативи допомагають переосмислити міжнародну позицію України, створити її позитивний образ і транслювати правдиву інформацію щодо причин, перебігу та наслідків російсько-української війни, а також покращувати український імідж не лише серед міжнародного експертного середовища, а й серед пересічних громадян, що дозволяє тиснути на уряди держав з метою збільшення військової підтримки України.

Водночас автор визнає думку, що державна інформаційна політика України досі є недостатньо системною та проактивною. Значна частина заходів у сфері протидії дезінформації має так званий «реактивний», а не стратегічний характер, тобто держава не діє превентивно та на випередження, а зазвичай реагує та розвінчує російські меседжі та наративи по факту їхнього надходження в інформаційний простір. Відсутність узгодженості між державними органами, обмеженість фінансових ресурсів та нестача комплексного планування створюють «інформаційні прогалини», які ефективно використовує в своїй діяльності наш ворог. Це підсвічує нагальну потребу в оновленні законодавчого та інституційного забезпечення інформаційної безпеки, у тому числі через створення міжвідомчих національних, а також міжнародних координаційних

центрів та впровадження національної стратегії з протидії інформаційним загрозам.

Іншою вразливою ланкою автор вказує недостатній рівень інтеграції інформаційної політики до загальної системи національної безпеки України. Враховуючи транснаціональний характер загроз та кількість способів поширення дезінформації ефективна протидія має базуватись на співпраці з такими глобальними міжнародними партнерами як НАТО та ЄС. У цьому контексті доцільним вважається створення спільних інформаційних платформ із залученням штучного інтелекту, які могли б оперативно реагувати на російські дезінформаційні меседжі та проводити роз'яснювальну роботу на зовнішніх інформаційних ринках.

Отже, сучасна російсько-українська війна засвідчила початок нової ери інформаційних конфліктів, в яких межі між журналістикою, пропагандою, експертизою і дипломатією стають дедалі розмитішими. На сьогоднішній день перемога в війні залежить не лише від збройної спроможності, але й від здатності держави до стратегічного інформаційного планування, активної присутності в глобальному медіапросторі та ефективної протидії дезінформації, що загрожує національній безпеці.

СПИСОК ВИКОРИСТАНИХ ДЖЕРЕЛ ТА ЛІТЕРАТУРИ

1. Магда Є.М. Гібридна війна: сутність та структура феномену. URL: http://journals.iir.edu.ua/index.php/pol_n/article/view/2489.
2. Прокоф'єв Д. Інформаційна війна та інформаційна злочинність / Д. Прокоф'єв, З: Вісник Запорізького юридичного інституту, 2000. С. 288-307.
3. Боднар І. Інформаційна безпека як основа національної безпеки. URL: http://mer-journal.sumy.ua/index.php/journal/article/view/529/486.
4. Конституція України. URL: https://zakon.rada.gov.ua/laws/show/254%D0%BA/96-%D0%B2%D1%80#Text.
5. Закон України «Про національну безпеку України» URL: https://zakon.rada.gov.ua/laws/show/2469-19#Text.
6. Бондаренко Р. Інформаційна безпека держави / Р. Бондаренко, В. Михальчук, К: Практика та досвід, 2021. С. 95-101.
7. Закон України «Про інформацію» URL: https://zakon.rada.gov.ua/laws/show/2657-12#Text .
8. Закон України «Про Єдиний державний реєстр призовників, військовозобов'язаних та резервістів» URL: https://zakon.rada.gov.ua/laws/show/1951-19#Text.
9. Що таке система DELTA. URL: https://mod.gov.ua/news/shho-take-sistema-delta-i-yak-vona-zadae-trendi.
10. Інструкція з діловодства та документування управлінської інформації в електронній формі в Міністерстві оборони України та Генеральному штабі Збройних Сил України URL: https://www.mil.gov.ua/content/mou_orders/370_nm_2018_instruction.pdf.
11. Закон України «Про захист інформації в інформаційно-комунікаційних системах» URL: https://zakon.rada.gov.ua/laws/show/80/94-%D0%B2%D1%80#Text.
12. Стратегія інформаційної безпеки URL: https://zakon.rada.gov.ua/laws/show/685/2021#Text.

13. В. Новицький. Стратегічні засади забезпечення інформаційної безпеки в сучасних умовах URL: http://il.ippi.org.ua/article/view/254349.
14. Computer Emergency Response Team of Ukraine URL: https://cert.gov.ua/article/6280563.
15. Правове регулювання інформаційних ризиків в законодавстві України URL: https://isu-conference.com/wp-content/uploads/2024/04/Formation_of_prospects_for_the_global_development_of_humanity_modern_problems_of_science_and_technology_April_3_5_2024_Bologna_Italy.pdf#page=97
16. Закон України «Про державну таємницю» URL: https://zakon.rada.gov.ua/laws/show/3855-12#Text.
17. Закон України «Про захист персональних даних» URL: https://zakon.rada.gov.ua/laws/show/2297-17#Text.
18. Закон України «Про доступ до публічної інформації» URL: https://zakon.rada.gov.ua/laws/show/2939-17#Text.
19. Закон України «Про основні засади забезпечення кібербезпеки України» URL: https://zakon.rada.gov.ua/laws/show/2163-19#Text.
20. ЗСУ впроваджують систему «Імпульс» URL: https://dou.ua/lenta/news/Impulse-information-and-communication-system/.
21. Кіберпростір як інтерактивне інформаційне середовище: питання щодо визначення та правового регулювання URL: https://snu.edu.ua/wp-content/uploads/2023/12/mater-ali-konferents-19.05.2023.pdf#page=103.
22. Інституційне забезпечення процесів протидії російській інформаційній експансії та пропаганді в сучасному світі URL: http://il.ippi.org.ua/article/view/243797.
23. Горун О. Протидія ворожій медіа-пропаганді в умовах правового режиму військового стану в Україні URL: http://il.ippi.org.ua/article/view/287772.
24. Землянко Ю. Принципи та порядок розробки комплексних систем захисту інформації в інформаційно-телекомунікаційних системах URL:

https://openarchive.nure.ua/server/api/core/bitstreams/23a61da8-bbc5-4d38-a379-393838b41d98/content.

25. Фролова О. Міжнародне співробітництво в галузі забезпечення інформаційної безпеки URL: http://publications.lnu.edu.ua/bulletins/index.php/intrel/article/download/10365/10492.
26. Шевчук Ю. Кібербезпека критичної інформаційної інфраструктури: практика ЄС URL: https://dspace.luguniv.edu.ua/xmlui/bitstream/handle/123456789/10209/%D0%9C%D0%B0%D0%BA%D0%B5%D1%82%20%D0%86%D0%86%20%D0%9C%D1%96%D0%B6%D0%BD%D0%B0%D1%80%20%D0%BA%D0%BE%D0%BD%D1%84%D0%B5%D1%80%D0%B5%D0%BD%D1%86%D1%96%D1%97%202024%20%D0%BF%D0%B4%D1%84.pdf?sequence=1&isAllowed=y#page=359.
27. Білоусов М. Інформаційна безпека країн ЄС: стан та перспективи розвитку URL: https://krs.chmnu.edu.ua/jspui/handle/123456789/1898.
28. What is General Data Protection Regulation URL: https://www.into.ie/app/uploads/2019/10/GDPR_FAQ.pdf.
29. Клюс М. Практичні аспекти реалізації основоположних принципів загального регламенту про захист даних (GDPR) URL: https://ekmair.ukma.edu.ua/server/api/core/bitstreams/0649daac-cc0c-4410-836d-16209af6ead8/content.
30. Monti M. The Eu Code Of Practice On Disinformation And The Risk Of The Privatisation Of Censorship URL: https://www.taylorfrancis.com/chapters/oa-edit/10.4324/9781003037385-20/eu-code-practice-disinformation-risk-privatisation-censorship-matteo-monti.
31. Звоздецька О. Протидія дезінформації в Європейському Союзі: правовий аспект URL: https://journals.chnu.edu.ua/mediaforum/article/view/115.

32. European Parliament resolution of 23 November 2016 on EU strategic communication to counteract propaganda against it by third parties URL: https://www.europarl.europa.eu/doceo/document/TA-8-2016-0441_EN.html.
33. Strategic Communications URL: https://www.eeas.europa.eu/taxonomy/term/400164_en.
34. Report of the independent High level Group on fake news and online disinformation URL: https://op.europa.eu/en/publication-detail/-/publication/6ef4df8b-4cea-11e8-be1d-01aa75ed71a1/language-en.
35. Звоздецька О. Нові підходи Північноатлантичного Альянсу (НАТО) у сфері кібербезпеки в умовах загострення інформаційного протистояння URL: https://journals.chnu.edu.ua/mediaforum/article/view/163.
36. Decoding the Information Environment: NATO's Strategic Communications Centre of Excellence URL: https://www.act.nato.int/article/stratcom-coe-2024/.
37. Паламарчук Д. Протистояння ворожій інформаційній діяльності з використанням соціальних платформ URL: https://er.chdtu.edu.ua/bitstream/ChSTU/5358/1/3%282024%29_5%d0%9f%d0%b0%d0%bb%d0%b0%d0%bc%d0%b0%d1%80%d1%87%d1%83%d0%ba%20%281%29.pdf.
38. Стьопкін А. Стратегічні комунікації НАТО як інструмент реалізації політики протидії дезінформації РФ URL: https://files.znu.edu.ua/files/Bibliobooks/Inshi72/0053085.pdf#page=377.
39. NATO 2030. United for a new era URL: https://www.ndc.nato.int/news/news.php?icode=1509.
40. Кондратьєв Я. Виявлення та розслідування злочинів, що вичиняються у сфері інформаційних технологій URL: https://www.uzhnu.edu.ua/uk/infocentre/get/4186.
41. Окремі проблемні аспекти кримінальної відповідальності та покарання за правопорушення у сфері використання ЕОМ, АС та КМ URL: http://journal-app.uzhnu.edu.ua/article/view/260148/256522.

42. Леонов Б. Методичне забезпечення заходів з класифікації, ідентифікації та фіксації кіберзлочинів URL: https://ippi.org.ua/sites/default/files/13_19.pdf.
43. Явний О. Кримінальна відповідальність за кіберзлочини в Україні URL: https://if.uu.edu.ua/wp-content/uploads/2024/08/d80c3fd6-db83-480b-b457-95bdab87db8a.pdf#page=456.
44. Організував діяльність злочинного угруповання: поліцейські оголосили підозри київському нотаріусу та чотирьом його спільникам URL: https://cyberpolice.gov.ua/news/organizuvav-diyalnist-zlochynnogo-ugrupovannya-policzejski-ogolosyly-pidozry-kyyivskomu-notariusu-ta-chotyrom-jogo-spilnykam-2081/.
45. Бортник Н. ІТ-право: проблеми та перспективи розвитку в Україні / Н. Бортник, Л: НУ «Львівська політехніка», 2017. С. 156.
46. Кодекс України про адміністративні правопорушення URL: https://zakon.rada.gov.ua/laws/show/80731-10#Text.
47. Волкова А. Особливості юридичної відповідальності за правопорушення в інформаційній сфері / А. Волкова, К: Правова інформатика, 2022. С.72-80.
48. Благодарний А. Проблеми удосконалення адміністративноюрисдикційної діяльності органів Служби безпеки України на стадії порушення справ про адміністративні проступки у сфері інформаційної безпеки URL: http://dwl.kiev.ua/art/asbu20171/zbir.pdf#page=12.
49. Дуцик Д. 21 рік Незалежності: від «пророків» до «копіпастерів» та «зливних бачків» URL: https://ms.detector.media/mediakritika/post/6389/2012-08-23-21-rik-nezalezhnosti-vid-prorokiv-do-kopipasteriv-ta-zlyvnykh-bachkiv/.
50. Державний комітет телебачення і радіомовлення України URL: http://comin.kmu.gov.ua/control/uk/publish/article?art_id=68581&cat_id=33909.
51. Матвійчук Я. БЮТ і Партія Регіонів – лідери серед замовників джинси URL: https://www.radiosvoboda.org/a/1758405.html.
52. Вокс Україна. Майдан у 2014 році – це державний переворот: огляд італійських та німецьких проросійських ЗМІ URL:

https://voxukraine.org/majdan-u-2014-rotsi-tse-derzhavnyj-perevorot-oglyad-italijskyh-ta-nimetskyh-prorosijskyh-zmi/.

53. Інтерньюз Україна. Ре-візія історії: російська історична пропаганда та Україна URL: https://internews.ua/opportunity/revision.
54. Детектор медіа. Українські телеканали в Криму вимкнули вже і в цифровому ефірі URL: https://detector.media/rinok/article/91305/2014-03-10-ukrainski-telekanaly-v-krymu-vymknuly-vzhe-i-v-tsyfrovomu-efiri/.
55. Vesti.ru. Исторический договор подписан. Крым вернулся домой URL: https://www.vesti.ru/article/1822146.
56. Радіо Свобода. Дев’ять кремлівських міфів, що виправдовують анексію Криму URL: https://www.radiosvoboda.org/a/28368765.html.
57. EUvsDISINFO. Russian aggression and disinformation in Ukraine URL: https://euvsdisinfo.eu/russian-aggression-and-disinformation-in-ukraine/.
58. Institute for religious freedom. The impact of the russian invasion on faith-based communities in Ukraine URL: https://irf.in.ua/files/publications/2024.03-IRF-Ukraine-report-ENG-web.pdf.
59. Російська пропаганда в Україні та за кордоном: чи виграє Київ інформаційну війну? URL: https://surl.li/ovtmhb.
60. Самигін Д. Дев’ять головних тем російської пропаганди URL: https://www.pravda.com.ua/columns/2023/05/5/7400790/.
61. Копинець Ю. Росія vs. правда: як кремлівська пропаганда змінює міжнародний порядок? URL: https://vilni-media.com/2025/03/09/rosiia-vs-pravda-iak-kremlivska-propahanda-zminiuie-mizhnarodnyj-poriadok/?utm_source=chatgpt.com.
62. Рябоштан І. Analysis of Russian propaganda in 11 European countries URL: https://surl.li/aiewhe.
63. Пилипенко А. Фейк Зрежисоване відео про «звірства» українських військових: чергова спроба дискредитації URL: https://surl.li/zwxwzh.
64. Tatham S. NATO strategic communication: more to be done? URL: https://surl.li/wxnfxh.

65. NATO. Hybrid threats and hybrid warfare reference curriculum URL: https://www.nato.int/nato_static_fl2014/assets/pdf/2024/7/pdf/241007-hybrid-threats-and-hybrid-warfare.pdf.
66. Дєдова А. Дезінформація в російських медіа як засіб інформаційної війни Росії проти України URL: https://essuir.sumdu.edu.ua/bitstream-download/123456789/94182/1/Diedova_masters_thesis.pdf.
67. Сейчас идет война с четвертым рейхом URL: https://kprf.ru/m/att/2022/10/38.pdf.
68. Укрінформ. За рік війни в Україні загинули 9655 цивільних, серед них - 461 дитина. URL: https://www.ukrinform.ua/rubric-ato/3673760-za-rik-vijni-v-ukraini-zaginuli-ponad-96-tisaci-civilnih-sered-nih-461-ditina.html.
69. Горун О. Протидія ворожій медіа-пропаганді в умовах правового режиму військового стану в Україні URL: https://ippi.org.ua/gorun-oyu-protidiya-vorozhii-media-propagandi-v-umovakh-pravovogo-rezhimu-viiskovogo-stanu-v-ukraini.
70. Туркова К. «Затрофеить мову». Новый нарратив в российской пропаганде URL: https://detector.media/infospace/article/200047/2022-06-11-zatrofeyt-movu-novyy-narratyv-v-rossyyskoy-propagande/.
71. Маргарита Симоньян. «Будь ласка» я говорю примерно всю жизнь, так же как «нема за що», «бачилы очи, за шо куповалы» и еще URL: https://x.com/M_Simonyan/status/1529362251811020800.
72. Лук'янчук А. Російська пропаганда під час війни російської федерації проти України як комунікаційне явище: основні меседжі та протидія URL: https://ekmair.ukma.edu.ua/server/api/core/bitstreams/3b1dd974-4e7b-4572-b1aa-c47ecccf74f4/content.
73. Шульська Н. Ворожі наративи в умовах війни в медіа: вербальні маркери, інформаційна гігієна та способи протистояння URL: https://www.philol.vernadskyjournals.in.ua/journals/2023/2_2023/part_2/26.pdf.

74. Гаврилко О. Наратив та його використання в інформаційних війнах URL: https://repository.mu.edu.ua/jspui/bitstream/123456789/3211/1/%D0%93%D0%B0%D0%B2%D1%80%D0%B8%D0%BB%D0%BA%D0%BE.pdf.
75. Максименко І. Війна рф проти України: російські ядерні наративи URL: https://onu.edu.ua/pub/bank/userfiles/files/news/podii/imidzh_ukrainy_06-11_Print.pdf#page=215.
76. Мегель А. Ворожі ІПСО. Як визначити та протистояти? URL: https://sprotyvg7.com.ua/wp-content/uploads/2023/04/IPSO-Textbook.pdf.
77. Psychological operations U.S. Army doctrine URL: https://www.psywar.org/psywar/reproductions/FM_33_1_1968.pdf.
78. Інформаційно-психологічні операції в контексті інформаційної безпеки України URL: http://il.ippi.org.ua/article/view/324704.
79. Федонюк С. Інформаційно-психологічні операції на геополітичній арені URL:https://evnuir.vnu.edu.ua/bitstream/123456789/24508/1/pos_ipo2%2021.06.pdf.
80. Шульська Н. Типологічні маркери інформаційно-психологічних операцій (ІПСО) в умовах війни в медіа URL: https://www.philol.vernadskyjournals.in.ua/journals/2023/1_2023/part_2/1-2_2023.pdf#page=278.
81. Онкович А. Соцмережа Фейсбук та інформаційно-психологічні операції URL: http://ukrinfospace.knukim.edu.ua/article/view/233974/232625.
82. Дранчук І. Інформаційно-психологічні операції рф проти України та ключові шляхи протидії в контексті забезпечення національно-патріотичної підготовки українських військовослужбовців URL: https://surl.li/piyitt.
83. Ляшенко А. Інформаційно-психологічні операції як інструмент національної безпеки США URL: https://repository.mu.edu.ua/jspui/bitstream/123456789/121/1/Tend_rozv_such_systemy_MV_2016.pdf#page=69.

84. Недодай М. Використання можливостей штучного інтелекту у створенні інформаційно-психологічних операцій URL: https://tit.duikt.edu.ua/index.php/telecommunication/article/view/2526/2407.
85. Dixit P. OpenAI shuts down tool to detect AI-written text due to low accuracy URL: https://www.businesstoday.in/technology/news/story/openai-shuts-down-tool-to-detect-ai-written-text-due-to-low-accuracy-391269-2023-07-26.
86. Осмоловська А. Чинники формування образу країни на міжнародній арені URL: https://jpl.donnu.edu.ua/article/view/5957.
87. Бондаренко І. Іміджологія у системі гуманітарних знань: культурно-освітні стратегії URL: https://files.znu.edu.ua/files/Bibliobooks/Inshi81/0060761.pdf.
88. Помаранцев П. Nothing is True and Everything is Possible: Adventures in Modern Russia / П. Помаранцев, L: Faber & Faber, 2022. С. 254.
89. Racz A. Russia's Hybrid War in Ukraine URL: https://fiia.fi/en/publication/russias-hybrid-war-in-ukraine.
90. Tsyfra Y. The role of diplomatic services in shaping international image: Ukrainian diplomacy before and after 24 February 2022 URL: https://uaforeignaffairs.com/en/journal-article/192.
91. Otlan Y. Essays on State Communication: Diplomatic Signals, Media Narratives, and Propaganda URL: https://escholarship.org/uc/item/30m0f563.
92. Stent A. How the war in Ukraine changed Russia's global standing URL: https://www.brookings.edu/articles/how-the-war-in-ukraine-changed-russias-global-standing/.
93. Darczewska J. The anatomy of Russian information warfare. The Crimean operation, a case study URL: https://www.osw.waw.pl/en/publikacje/point-view/2014-05-22/anatomy-russian-information-warfare-crimean-operation-a-case-study.
94. Russia Today. Ukrainian promises on African grain not being kept – NYT URL: https://www.rt.com/russia/560560-ukraine-grain-africa-problems/.
95. Інтернет Свобода. Як упізнати тролів та знайти їх мережу URL: https://netfreedom.org.ua/article/yak-upiznati-troliv-ta-znajti-yih-merezhu.

96. Starbird K. Disinformation as Collaborative Work: Surfacing the Participatory Nature of Strategic Information Operations URL: https://dl.acm.org/doi/10.1145/3359229.
97. Нагорняк Т. Публічний імідж України в умовах невизначеності URL: https://jpl.donnu.edu.ua/article/view/12038.
98. Гуцал С. Публічна дипломатія та стратегічні комунікації: визначення концептуальних основ URL: http://clouds.iir.edu.ua/index.php/pol_n/article/view/2769.
99. Barghoorn F. C. The Soviet Cultural Offensive. The role of Cultural Diplomacy in Soviet Foreign Policy. Princeton, 1960. 353 p.
100. Cummings M. Cultural diplomacy and the United States Government: a Survey URL: https://www.americansforthearts.org/by-program/reports-and-data/legislation-policy/naappd/cultural-diplomacy-and-the-united-states-government-a-survey.
101. 2020: The Year of Digital Resurgence URL: https://digdipblog.com/2020/12/24/2020-the-year-of-digital-resurgence/.
102. Дубовик Н. Культурна дипломатія як інструмент міжнародної комунікації України URL: https://molodyivchenyi.ua/index.php/journal/article/view/5813/5684.
103. Українські книжкові полички в межах проєкту Олени Зеленської поповнилися «Історією України-Руси» Михайла Грушевського URL: https://www.president.gov.ua/news/ukrayinski-knizhkovi-polichki-v-mezhah-proyektu-oleni-zelens-89153.
104. Стратегія публічної дипломатії МЗС URL: https://mfa.gov.ua/pro-ministerstvo/strategiyi-mzs.
105. Кубко В. Культурна дипломатія в системі стратегічних комунікацій України URL: http://fps-visnyk.lnu.lviv.ua/archive/45_2022/15.pdf.
106. Стратегія Українського інституту на 2020-2024 рік URL: https://ui.org.ua/wp-content/uploads/2022/01/strategy-ukrainian-institute-3.pdf.

107. За літо «Океан Ельзи» зібрав понад 19 млн гривень для України URL: https://tsn.ua/glamur/za-lito-okean-elzi-zibrav-ponad-19-mln-griven-dlya-ukrayini-na-scho-muzikanti-vitratyat-groshi-2148673.html.

108. Гриненко В. «Курган і Агрегат» зібрали 14 мільйонів гривень на ЗСУ в благодійному турі Європою URL: https://www.village.com.ua/village/culture/culture-news/356757-laquo-kurgan-i-agregat-raquo-zibrali-14-milyoniv-griven-na-zsu-u-blagodiynomu-turi-evropoyu.

109. Центр протидії дезінформації. На що спрямована культурна спецоперація росії в Європі URL: https://cpd.gov.ua/articles/na-shho-spryamovana-kulturna-speczoperacziya-rosiyi-v-yevropi/.