

Харківський національний університет імені В. Н. Каразіна

Філософський факультет

Кафедра політології

Пояснювальна записка

до кваліфікаційної роботи бакалавра

На тему: **«Інформаційна політика України в умовах російсько-української війни»**

Виконала:

здобувачка вищої освіти 4-го курсу, групи ОП-42

денного відділення

напряму підготовки 05 - «Соціальні та поведінкові науки»

спеціальності 052 «Політологія»

ОПП «Політичні технології та аналіз політики»

Читова Віолетта Олександрівна

Керівник:

старший викладач кафедри політології,

кандидат політичних наук

Авксентьев Антон Олександрович

Рецензент:

кандидат юридичних наук,

доцент кафедри правоохоронної діяльності

Говоров Валерій Станіславович

Харків – 2025 року

Харківський національний університет ім. В.Н. Каразіна

Філософський факультет

Кафедра політології

Спеціальність 052 Політологія

Освітньо-професійна програма «Політичні технології та аналіз політик»

Рівень вищої освіти: перший (бакалаврський)

ЗАТВЕРДЖУЮ:
Завідувач кафедри

О.А. ФІСУН

(ініціали, прізвище)

(підпис)

« ____ » _____ 20__ року

ЗАВДАННЯ

На кваліфікаційну роботу бакалавра

Читової Віолетти Олександрівни

(прізвище, ім'я та по батькові)

1. Тема роботи: «Інформаційна політика України в умовах російсько-української війни» керівник роботи: Авксентьев Антон Александрович, старший викладач кафедри політології, кандидат політичних наук

(прізвище, ім'я, по батькові, науковий ступінь, вчене звання)

затверджені наказом по університету від «22» березня 2024 року. № 3801-5/795

2. Строк подання студентом роботи 30 травня 2025 р.

3. Перелік питань, які потрібно розробити:

1. Розкрити теоретичні засади поняття «інформаційна політика» та визначити її значення у внутрішньому і міжнародному контекстах.

2. Проаналізувати основні загрози інформаційній безпеці України та оцінити ефективність державної політики у відповідь на ці виклики.


3. Дослідити напрями інформаційної політики України у протидії російській дезінформації та визначити перспективи її подальшого розвитку в умовах війни.

4. План роботи

№ з/п	Назва етапу роботи	Термін виконання етапу
1	Консультація з керівником щодо обрання теми роботи	30.09.2024
2	Затвердження теми роботи	12.10.2024
3	Аналіз та підбір літературних джерел для написання роботи	30.11.2024
4	Написання змісту до кваліфікаційної роботи	30.12.2024
5	Написання першого розділу та висновків до нього	30.01.2025
6	Написання другого розділу та висновків до нього	28.02.2025
7	Написання третього розділу та висновків до нього	10.03.2025
8	Написання вступу до роботи	15.03.2025
9	Написання висновків до роботи	31.03.2025
10	Оформлення списку використаних джерел	15.04.2025
11	Написання анотації	30.04.2025
12	Фінальні коригування та доопрацювання	12.05.2025
13	Переддипломна практика	19.05.2025-06.06.2025
14	Підготовка доповіді до виступу на захисті кваліфікаційної роботи	20.05.2025
15	Підготовка презентації до виступу на захисті кваліфікаційної роботи	21.05.2025
16	Підготовка до виступу на захисті кваліфікаційної роботи	22.05.2025
17	Передзахист кваліфікаційної роботи	27.05.2025
18	Фінальні коригування та доопрацювання після зауважень на передзахисті	28-29.05.2025
19	Перевірка кваліфікаційної роботи через систему антиплагіат	30.05.2025
20	Захист кваліфікаційної роботи	13.06.2025

5. Дата видачі завдання: 30.09.2024

Здобувачка вищої освіти _____  В. О. Читова

Керівник роботи _____  А. О. Авксентьев
(підпис) (ініціали, прізвище)

ХАРКІВСЬКИЙ НАЦІОНАЛЬНИЙ УНІВЕРСИТЕТ ІМЕНІ В. Н. КАРАЗІНА
ПОДАННЯ
ГОЛОВІ ЕКЗАМЕНАЦІЙНОЇ КОМІСІЇ
ЩОДО ЗАХИСТУ БАКАЛАВРСЬКОЇ РОБОТИ

Направляється студентка *Читова В.О.* до захисту бакалаврської роботи за спеціальністю 052 – політологія на тему: «Інформаційна політика України в умовах російсько-української війни»

Бакалаврська робота і рецензія додаються.

Декан філософського факультету _____ Карпенко І. В.

Довідка про успішність

Студентка *Читова В.О.* за період навчання на філософському факультеті з 2021 року по 2025 рік повністю виконала навчальний план за спеціальністю з таким розподілом оцінок за національною шкалою:

відмінно – _____%, добре – _____%, задовільно – _____%.

Фахівець 1 категорії

навчального центру організації

освітнього процесу філософського факультету _____ Рєвкова Н. Є.

Висновок керівника бакалаврської роботи

Студентка *Читова В.О.* виконала бакалаврську роботу на тему «Інформаційна політика України в умовах російсько-української війни» яка присвячена аналізу особливостей інформаційної політики держави під час війни, зокрема стратегій протидії дезінформації та інформаційним впливам РФ.

Керівник бакалаврської роботи:
старший викладач кафедри політології,

Харківського національного
університету імені В. Н. Каразіна,
кандидат політичних наук

Авкс _____ Авксентьєв А. О.
_____20__ року

Висновок кафедри про бакалаврську роботу

Бакалаврська робота розглянута. Студентка *Читова В.О.* допускається до захисту роботи в Екзаменаційній комісії.

Зав. кафедри політології _____ Фісун О.А.
_____20__ року

ЗМІСТ

ЗМІСТ	2
ВСТУП	3
РОЗДІЛ 1 ТЕОРЕТИЧНІ ОСНОВИ ІНФОРМАЦІЙНОЇ ПОЛІТИКИ	6
1.1 Поняття «інформаційна політика»: визначення, сутність, функції	6
1.2 Роль інформаційної політики в сучасних міжнародних відносинах	12
РОЗДІЛ 2 ІНФОРМАЦІЙНА БЕЗПЕКА УКРАЇНИ: ЗАГРОЗИ ТА ВІДПОВІДІ	22
2.1 Методи та інструменти інформаційних атак	22
2.2 Державна політика в сфері інформаційної безпеки	28
РОЗДІЛ 3 ІНФОРМАЦІЙНА ПОЛІТИКА УКРАЇНИ У ПРОТИДІЇ РОСІЙСЬКІЙ АГРЕСІЇ	35
3.1 Основні напрями інформаційної політики України у сфері протидії дезінформації та російській пропаганді	35
3.2 Виклики та перспективи розвитку інформаційної політики в Україні	40
ВИСНОВКИ	46
СПИСОК ВИКОРИСТАНИХ ДЖЕРЕЛ	50
ДОДАТКИ	56

ВСТУП

У 2014 році російська федерація здійснила анексію Автономної Республіки Крим і розв'язала військові дії на сході України, що стало початком масштабної гібридної агресії проти України. Відтоді війна вийшла за межі лише збройного протистояння – поряд із фізичним наступом почалася безпрецедентна інформаційна війна. Особливого розмаху вона набула після повномасштабного вторгнення у лютому 2022 року, коли інформаційний простір України і світу став ареною системної боротьби між правдою та пропагандою.

Інформаційна політика України в умовах війни є критично важливою сферою державного управління, яка включає боротьбу з дезінформацією, забезпечення громадян достовірною інформацією, захист національного інформаційного простору, а також формування міжнародної підтримки. В умовах військового протистояння держава стикається з необхідністю не лише оборонятися на фронті, а й оперативно реагувати на інформаційні загрози – від фейкових повідомлень до кібератак на критичну інфраструктуру. Водночас сучасна інформаційна політика має бути не лише оборонною, а й стратегічною – вона повинна формувати наративи, здатні об'єднати суспільство, зміцнити довіру до влади, забезпечити стабільність демократичних інституцій та посилити позиції України на міжнародній арені. Саме тому ефективність інформаційної політики стає ключовим чинником виживання та стійкості держави в умовах гібридної війни.

Актуальність теми дослідження зумовлена безпрецедентною масштабністю та складністю інформаційної агресії з боку росії, що вимагає системного аналізу методів, засобів і результатів інформаційної політики України у відповідь на виклики. Від інформаційної стійкості держави та її громадян залежить не лише моральний дух суспільства, а й міжнародна репутація, підтримка союзників і майбутнє національної безпеки. Окрім цього, новизна ситуації полягає в тому, що ніколи раніше Україна не стикалася з такою концентрацією та інтенсивністю

інформаційного тиску ззовні, поєднаного з викликами внутрішнього інформаційного ландшафту: зниженням довіри до медіа, зростанням ролі соцмереж, а також фрагментацією суспільного дискурсу, що вимагає не просто реактивної політики, а продуманої стратегії інформаційного розвитку.

Мета роботи – проаналізувати еволюцію та сучасний стан інформаційної політики України в умовах російсько-української війни, зосередивши увагу на ключових викликах, інструментах протидії дезінформації та формуванні позитивного міжнародного іміджу країни.

Для досягнення мети визначено такі завдання:

1. Розкрити теоретичні засади поняття «інформаційна політика» та визначити її значення у внутрішньому і міжнародному контекстах.
2. Проаналізувати основні загрози інформаційній безпеці України та оцінити ефективність державної політики у відповідь на ці виклики.
3. Дослідити напрями інформаційної політики України у протидії російській дезінформації та визначити перспективи її подальшого розвитку в умовах війни.

Об'єктом дослідження виступає інформаційна політика України. Предметом – особливості реалізації інформаційної політики в умовах війни та гібридної агресії.

Методологічну основу дослідження становлять:

- системний підхід – для аналізу інформаційної політики як складової національної безпеки;
- структурно-функціональний метод – для вивчення структури та функцій державної інформаційної політики;
- контент-аналіз – для виявлення ключових тем і меседжів російської пропаганди;
- порівняльний аналіз – для зіставлення дій України з практиками інших держав у подібних ситуаціях.

Наукова новизна роботи полягає у спробі комплексно проаналізувати інформаційну політику України в умовах війни не лише з точки зору оборони, а й як інструменту дипломатії, комунікації з громадянами, міжнародного іміджу та елементу стійкості суспільства. Крім того, дослідження враховує динаміку змін в українському інформаційному середовищі у 2022-2024 роках: від високої довіри до телемарафону «Єдині новини» – до поступового зростання скепсису серед аудиторії, що створює нові виклики для державної комунікаційної політики.

Практичне значення дослідження полягає в тому, що його результати можуть бути використані для вдосконалення державної інформаційної політики, розробки програм медіа-грамотності, комунікаційних стратегій у кризових умовах, а також формування стійкого демократичного інформаційного середовища.

Структура роботи включає вступ, три розділи, кожен з яких складається з підрозділів, висновки та список використаних джерел. Робота містить 64 сторінки і ґрунтується на аналізі 53 наукових, аналітичних та офіційних джерел.

РОЗДІЛ 1

ТЕОРЕТИЧНІ ЗАСАДИ ІНФОРМАЦІЙНОЇ ПОЛІТИКИ

1.1 Поняття «інформаційна політика»: визначення, сутність, функції

У сучасному світі інформаційна політика відіграє надзвичайно важливу роль, оскільки інформація є однією з найвпливовіших складових сучасного суспільства. Зі зростанням впливу цифрових технологій, розвитком масових комунікацій та популяризацією соціальних мереж інформація стала ключовим ресурсом, що визначає поведінку суспільства, впливає на політичні процеси та формує громадську думку. У цьому контексті інформаційна політика розглядається як важливий інструмент державного управління та національної безпеки, що спрямований на формування й регулювання інформаційного простору країни.

Мета державної інформаційної політики полягає в забезпеченні якісної інформації для стратегічних та оперативних завдань соціально-економічного розвитку країни, а також у створенні інформаційно стійкого суспільства, здатного протистояти зовнішнім і внутрішнім загрозам. Завдання, які має вирішити інформаційна політика, є вкрай важливими. Це, зокрема, передбачає створення розвинутої інформаційної інфраструктури, формування та ефективного використання національних інформаційних ресурсів, стимулювання інноваційної діяльності, а також всебічний розвиток і захист національної інформаційної системи. Одним з найбільш важливих аспектів сьогодні є уникнення ризиків (особливо фінансових втрат через неузгоджене та неповне використання інформації або несанкціоноване її використання) і запобігання загрозам, які можуть зашкодити життєво важливим інтересам особи, суспільства та загальному стану в процесі інформаційної діяльності.

Сучасна інформаційна політика є інструментом забезпечення безпеки особи, суспільства, держави та світової спільноти. У багатьох країнах та міжнародних

організаціях функціонують спеціалізовані структури, які займаються інформаційною діяльністю. Окрім того, активну роль у цій сфері відіграють і вищі посадові особи держави, які реалізують найважливіші інтереси в контексті національної та міжнародної безпеки (Терещенко,2023:391). Основними напрямками державної інформаційної політики є:

- «забезпечення доступу кожного до інформації;
- забезпечення рівних можливостей щодо створення, збирання, одержання, зберігання, використання, поширення, охорони, захисту інформації;
- створення умов для формування в Україні інформаційного суспільства;
- забезпечення відкритості та прозорості діяльності суб'єктів владних повноважень;
- створення інформаційних систем і мереж інформації, розвиток електронного урядування;
- постійне оновлення, збагачення та зберігання національних інформаційних ресурсів;
- забезпечення інформаційної безпеки України;
- сприяння міжнародній співпраці в інформаційній сфері та входженню України до світового інформаційного простору» (Про інформацію, 1992).

Інформаційна політика в умовах війни являє собою систему заходів, які здійснюються державою в співпраці з інститутами громадянського суспільства для регулювання інформаційних процесів, а також для формування та розвитку інформаційного суспільства, з акцентом на національні інтереси в сфері оборони. Основна мета цієї політики полягає в захисті прав та інтересів особи, моральних цінностей, а також забезпеченні інформаційної безпеки особи, суспільства та держави (Пунда,2022:60). Державна інформаційна політика несе відповідальність за створення єдиного інформаційного простору в Україні, забезпечення інформаційної безпеки як особистості, так і суспільства та держави, а також за інтеграцію України у світовий інформаційний простір (Мирошнеченко, 2023: 41).

Термін «інформаційна політика» визначається як метод генерації, формування та використання інформаційних потоків і ресурсів різними суб'єктами, такими як організації, підприємства або установи, які мають власні інтереси в роботі з інформацією. Ю. М. Іванченко зазначає, що «інформаційна політика охоплює сукупність основних напрямів і методів діяльності держави в контексті отримання, використання, поширення та зберігання інформації» (Іванченко, 2005). Г. Почепцов підкреслює, що «інформаційна політика відповідає за організацію процесів створення, розповсюдження та зберігання інформації в соціальних системах» (Почепцов, 2015:497).

Використання терміна «інформаційна політика» зазвичай спрямоване на опис і вирішення конкретних завдань, що постають перед суб'єктами, тобто на елементи реальності, які інформаційно охоплюють різні сфери певної проблеми і не мають чітких меж, однорідних зв'язків або аналогічних характеристик. Як і будь-яка діяльність, інформаційна політика формується та реалізується з метою досягнення певних результатів. О. В. Соснін вважає, що «метою державної інформаційної політики є створення необхідних економічних, соціокультурних умов, а також правових і організаційних механізмів для формування, розвитку та ефективного використання національних інформаційних ресурсів у всіх сферах життя та діяльності громадянина, суспільства і держави» (Соснін : 23).

Продовжуючи розгляд поняття інформаційної політики, слід підкреслити, що вона охоплює широку низку функцій, які відповідають завданням формування надійної інформаційної безпеки та створення прозорого, відкритого інформаційного простору. Розглянемо детальніше основні функції інформаційної політики.

Формування інформаційного середовища є однією з основних функцій інформаційної політики держави, яка має вирішальне значення для соціального розвитку, демократії та забезпечення національної безпеки (Резнікова, 2022:532). Інформаційне середовище об'єднує різні платформи, канали комунікації та

інформаційні ресурси, що функціонують у межах певної країни або регіону і слугують як для внутрішніх, так і зовнішніх інформаційних потреб. Основні аспекти формування інформаційного середовища включають такі напрямки, як:

- розбудова національних медіа-ресурсів. Для створення якісного та незалежного інформаційного середовища держава заохочує розвиток національних медіа, що орієнтовані на суспільні інтереси і працюють відповідно до професійних стандартів журналістики, що забезпечує громадянам доступ до об'єктивної інформації та сприяє уникненню домінування іноземного контенту, який може мати зовнішньополітичні впливи;

- стимулювання прозорості та достовірності інформації. Для формування довіри громадян до медіа важливо впроваджувати та підтримувати механізми контролю якості інформації, що поширюється через державні та приватні канали, наприклад, розробка стандартів фактчекінгу, санкції за поширення дезінформації (Міненко, 2024: 253);

- розширення доступу до інформації. У демократичному українському суспільстві важливо забезпечити рівноправний доступ до інформаційних ресурсів для всіх громадян, що можливо реалізувати шляхом цифровізації державних послуг, підтримкою громадських інформаційних центрів, а також через запровадження програм, спрямованих на підвищення медійної грамотності серед населення;

- забезпечення інформаційної безпеки та захисту від інформаційних загроз. У сучасних умовах повномасштабного вторгнення Україна зіштовхується з численними викликами у сфері інформаційної безпеки, зокрема з кіберзагрозами, спробами втручання у внутрішні справи через медіа, а також з впливом дезінформації на громадську думку. Формування інформаційного середовища включає захист від подібних загроз через систему кібербезпеки, регулювання діяльності соціальних мереж та контроль за поширенням шкідливого контенту.

Регулювання інформаційних потоків та підтримка національних інтересів є

важливою частиною державної інформаційної політики, оскільки інформаційні ресурси можуть безпосередньо впливати на стабільність суспільства, політичні процеси та економічну ситуацію, адже цей напрямок охоплює різноманітні заходи та механізми, які забезпечують контроль над інформаційними потоками, формують стійке інформаційне середовище та захищають національні інтереси.

Для забезпечення національних інтересів держава повинна здійснювати постійний моніторинг внутрішніх та зовнішніх інформаційних потоків, що може включати відстеження інформації в медіа, соціальних мережах та інших комунікаційних каналах з метою виявлення потенційних загроз, таких як пропаганда, дезінформація, заклики до порушення громадського порядку чи посягання на національну безпеку (Лавченко, 2021:117).

Інформаційний суверенітет передбачає контроль держави над власним інформаційним простором і стійкість до зовнішніх інформаційних впливів. Це означає забезпечення умов, за яких національний інформаційний простір захищений від іноземних маніпуляцій та пропаганди. Важливими засобами захисту є встановлення вимог до іноземних медіа, що працюють на території країни, захист національної інформаційної інфраструктури, а також розвиток локальних медіа, які можуть конкурувати із зарубіжними за якістю контенту та довірою аудиторії.

Варто зазначити, що задля стійкості населення до дезінформації та маніпуляцій, важливо підвищувати його рівень інформаційної культури та медіа-грамотності. Держава може ініціювати програми, які спрямовані на навчання критичному мисленню, навчанню розпізнаванню фейкових новин і маніпуляцій, а також на пояснення принципів роботи медіа, що знижує ризик впливу на громадську думку ворожих інформаційних кампаній та сприяє формуванню суспільства, здатного протистояти інформаційним атакам.

Стратегія інформаційної безпеки у контексті функцій інформаційної політики повинна враховувати потреби національної безпеки та спрямовуватися на забезпечення стабільності та розвитку суспільства. Вона визначає пріоритети,

принципи, основні завдання та інструменти, необхідні для захисту інформаційного простору. Така стратегія окреслює механізми моніторингу, попередження та реагування на інформаційні загрози, а також заходи з розвитку національної інформаційної інфраструктури (Детектор медіа, 25).

Важливою функцією інформаційної політики є підтримка інформаційної відкритості та прозорості державної діяльності, що сприяє формуванню довіри громадян до уряду та державних інститутів, що досягається шляхом запровадження політики прозорого доступу до інформації про діяльність державних органів, публікації урядових звітів, проведення публічних обговорень та консультацій з громадськістю. Інформаційна відкритість підвищує підзвітність органів влади, зменшує рівень корупції та зміцнює демократичні принципи в суспільстві (Громадянське суспільство, 2019:215).

Крім того, інформаційна політика охоплює таку функцію, як підтримка інновацій у сфері інформаційних технологій (Ржевська, 2024:7). В умовах стрімкого технологічного розвитку ця функція є критично важливою для забезпечення конкурентоспроможності країни. Інноваційна складова інформаційної політики передбачає сприяння розробці новітніх технологій обробки даних, підтримку стартапів у сфері ІТ, розвиток дослідницьких центрів та співпрацю з приватним сектором для впровадження сучасних технологічних рішень. Ще одна функція інформаційної політики – це інформаційне забезпечення міжнародної комунікації. Зовнішньополітичний аспект інформаційної політики має на меті формування позитивного міжнародного іміджу країни, поширення правдивої інформації про внутрішні процеси, а також контрпропаганду та протидію дезінформації на світовій арені. Така політика включає комунікації з міжнародними медіа, просування культурних та економічних здобутків держави та підтримку діаспори у поширенні достовірної інформації про ситуацію в країні. Загалом, функції інформаційної політики є багатогранними та охоплюють різні аспекти державного управління, комунікаційних процесів та національної безпеки.

Вони спрямовані на підтримку стабільності та розвитку суспільства, забезпечення прав громадян на інформацію та збереження національних інтересів у сучасному глобалізованому світі.

Таким чином, сучасна інформаційна політика має важливе значення для національної безпеки, розвитку суспільства, підтримки інновацій та зміцнення демократичних принципів. Вона є комплексною системою заходів, які охоплюють широкий спектр напрямів і завдань, зокрема формування національної інформаційної інфраструктури, забезпечення інформаційного суверенітету, підтримку інновацій та підвищення рівня інформаційної культури.

1.2 Інформаційна політика України під час війни: вплив на міжнародні відносини

Інформаційна політика на сучасному етапі глобалізації є одним із ключових інструментів, що впливають на розвиток міжнародних відносин. Цей вплив обумовлений не лише зростанням обсягів інформаційних потоків, але й активним використанням інформаційних технологій для формування громадської думки, управління суспільними настроями, а також сприяння або перешкоджання зовнішній політиці держав. Сучасний контекст також вимагає уваги до електорального аспекту інформаційної політики в умовах війни, що створює нові виклики для демократичних процесів та формування довіри до урядів.

Інформаційна політика в міжнародних відносинах відіграє важливу роль як інструмент «м'якої сили», що дає змогу країнам досягати своїх цілей без застосування військових засобів. Використання інформації для впливу на громадську думку, формування іміджу держави за кордоном та управління репутаційними ризиками є складовими сучасної інформаційної політики, що особливо актуально в умовах глобалізації, коли інформація може швидко поширюватися та впливати на національні політики. Дж. Най визначає «м'яку

силу» як здатність спонукати інших прагнути до результатів, які вони бажають отримати, шляхом кооперації, а не примусу (Савон, 2019:183). Однак, вчений зазначає, що це «не те саме, що вплив. ... «м'яка сила» – це більше, ніж просто переконання або здатність аргументовано переконувати, хоча ці аспекти є важливими елементами цієї концепції. «М'яка сила» також включає в себе здатність приваблювати, що часто призводить до взаєморозуміння. Отже, «м'яка сила» – це приваблива сила» (Nye, 2004:321).

На сьогоднішній день основні завдання інформаційної політики на міжнародному рівні включають:

- формування позитивного іміджу держави. Країни активно працюють над створенням позитивного образу через культурну дипломатію, пропагування національних цінностей, досягнень у науці та культурі, що сприяє підвищенню привабливості держави для інвестицій та створенню сприятливих умов для дипломатичної співпраці;

- протидія дезінформації та пропаганді. В умовах сучасних гібридних конфліктів важливим напрямком є виявлення та нейтралізація дезінформаційних кампаній, що використовують недостовірну інформацію для впливу на громадську думку або дестабілізації суспільства;

- підтримка національних інтересів. Інформаційна політика сприяє відстоюванню національних позицій у міжнародних справах, включаючи дипломатичні зусилля та медіа-кампанії.

У сучасних умовах, коли країни ведуть боротьбу за міжнародну підтримку, інформаційна політика дозволяє формувати довгостроковий позитивний імідж держави. Наприклад, інформаційна стратегія, яка зосереджена на висвітленні інноваційних досягнень чи екологічних ініціатив, сприяє побудові образу держави як прогресивної, сучасної та надійної на світовій арені (Савон, 2019:193). Розвиток соціальних мереж та цифрових медіа дає змогу країнам впливати на громадську думку в реальному часі, що підвищує швидкість і точність комунікації, а також

дозволяє залучити аудиторію до важливих міжнародних подій. Інформаційна політика також допомагає забезпечити відчутну підтримку серед населення інших держав, що може сприяти формуванню сприятливих умов для укладення торговельних або дипломатичних угод.

У випадку України інформаційна політика на міжнародній арені є важливим елементом стратегії протидії російській агресії. Вона зосереджується на висвітленні реальних подій на фронті, демонстрації актів порушення міжнародного права з боку Росії та залученні міжнародної підтримки через правдиве інформування про події в країні. Завдяки активній інформаційній політиці Україні вдалося досягти вагомої підтримки від провідних міжнародних організацій та держав, а також об'єднати громадську думку демократичних країн навколо ідеї допомоги Україні.

Електоральний аспект інформаційної політики України в умовах російсько-української війни є надзвичайно важливим для збереження демократичних процесів і національної єдності. Війна, яку росія веде проти України, включає не лише збройну агресію, але й потужну інформаційну кампанію, що спрямована на дестабілізацію українського суспільства, створення недовіри до української влади та вплив на політичні процеси, зокрема, вибори. Найголовнішим викликом для електоральної інформаційної політики в умовах війни є протидія дезінформації та фальсифікаціям. Росія активно використовує інформаційні атаки та пропаганду, щоб дискредитувати політичне керівництво. До поширених методів належать фейкові новини, підроблені відео та повідомлення, що створюють відчуття нестабільності або корумпованості української влади.

Згідно з даними аналітичного центру Debunk Disinformation, «кремль витратив 1,9 мільярда доларів на російську пропаганду у 2023 році. Центр громадянської стійкості Res Publica виявив, що витрати на російські державні ЗМІ зросли втричі порівняно з 2021 роком» (Детектор медіа, 23). І більшість зусиль росії спрямовані на російську та, безумовно, українську аудиторію. Через

повномасштабне вторгнення росії в Україні наразі не проводяться вибори, і цей факт вимагає особливого підходу до електоральної інформаційної політики. Відсутність виборів через війну створює додаткові виклики для державної інформаційної політики, адже зростає ризик дестабілізації, спричинений розповсюдженням пропаганди та дезінформації, що може вплинути на громадську думку та довіру до влади.

В умовах, коли проведення виборів є неможливим через бойові дії та ризики для безпеки, інформаційна політика має особливу роль у формуванні та підтримці довіри до демократичних інститутів. Українська влада регулярно інформує населення про причини відтермінування виборів, підкреслюючи, що основною метою є забезпечення національної безпеки та цілісності держави. Проте, відсутність виборчого процесу потенційно може розколувати суспільство або викликати почуття безсилля у громадян. Тому держава через засоби масової інформації зосереджує увагу на об'єднанні громадян довкола ідеї захисту національного суверенітету, протидії агресору та відновленні територіальної цілісності. російська пропаганда використовує факт відсутності виборів як інструмент для поширення меседжів про нібито недемократичний характер української влади та спроби «узурпації влади».

Інформаційна політика України на міжнародній арені стала важливим компонентом стратегії забезпечення підтримки з боку міжнародної спільноти в умовах російсько-української війни. Міжнародний аспект політики зосереджується на зміцненні міжнародної коаліції проти агресії, підтримці міжнародного іміджу України як держави, яка бореться за демократичні цінності, і на розвінчуванні російської пропаганди на глобальному рівні.

Україна активно використовує інформаційну політику для консолідації міжнародної спільноти проти російської агресії. Поширюючи правдиву інформацію про військові злочини, що здійснюються на її території, Україна стимулює глобальне осудження дій Росії. Співпраця з ООН, Європейським

Союзом, НАТО та іншими міжнародними організаціями дозволяє Україні знаходити нових партнерів та зміцнювати підтримку існуючих. Завдяки цьому формуються міжнародні коаліції, що надають Україні фінансову, військову та гуманітарну допомогу (Укрінформ, 27).

Інформаційна політика України зосереджена на демонстрації світу своїх прагнень до свободи, незалежності та демократичних цінностей. Через комунікаційні канали, дипломатичні місії, культурні програми, міжнародні заходи та ЗМІ Україна формує у світової спільноти образ країни, що бореться за право на існування як незалежна демократична держава. Цей позитивний імідж сприяє збільшенню підтримки з боку громадян інших країн та тиску на уряди, що змушує їх займати активнішу позицію у підтримці України.

Важливим напрямом міжнародного аспекту інформаційної політики України є боротьба з російською дезінформацією, яка націлена як на міжнародну аудиторію, так і на саму Україну. Росія використовує маніпулятивні наративи для зображення України як «загрози», дискредитації українського керівництва, а також для поширення фейкової інформації про ситуацію на фронті. Міжнародні компанії Google та Jigsaw запустили в Україні новаторську ініціативу з медіа грамотності, спрямовану на протидію онлайн-дезінформації та зміцнення захисту від поширених методів цифрових маніпуляцій. Ключовою складовою цієї програми є використання методології, відомої як «пребанкінг», яка передбачає своєчасне попередження та розвінчування маніпулятивних технік. Проєкт реалізується у співпраці з Moonshot, а також за активного залучення провідних українських організацій і фахівців: Центру протидії дезінформації, Vox Ukraine, StopFake, Детектор Медіа, Суспільного мовлення і BBC Media Action. Пребанкінг орієнтований на розвиток здатності аудиторії критично оцінювати інформацію, розпізнавати маніпуляції та загалом формувати імунітет до поширення дезінформації у майбутньому (Рубрика, 28, 31).

Також, Україна активно використовує міжнародні ЗМІ, а також соціальні

мережі для поширення своєї позиції та донесення правди про російську агресію. Соціальні мережі стали потужним інструментом комунікації, оскільки вони дозволяють охоплювати широку аудиторію, зокрема молодь, та швидко реагувати на події. Найпоширенішою соціальною мережею серед українців є Telegram, соціальна мережа X використовується для демонстрації іноземним партнерам та журналістам наслідків військових злочинів.

Українські медіа активно інтегрують інформацію, оприлюднену провідними західними джерелами, що пояснюється низкою факторів, серед яких ключовою є тенденція українських високопосадовців ділитися важливою фактологічною інформацією переважно із західними засобами масової інформації. Водночас внутрішня комунікація інколи залишається більш формалізованою й одноманітною. Унаслідок цього західні медіа значною мірою впливають на формування громадської думки в Україні, зокрема на сприйняття подій війни серед населення. Одним з основних наративів, що простежуються в публікаціях таких медіа ресурсів, як The Wall Street Journal, Bloomberg та The Washington Post, є акцент на залежності оборони України від зовнішньої економічної й військової допомоги (Інститут масової інформації, 15). На рис. 1.1 наведено довіру населення до телемарафону «Єдині новини».

За даними рис. 1.1 можемо зробити наступні висновки: спостерігається зниження рівня довіри – у травні 2022 року 69% респондентів довіряли телемарафону «Єдині новини», але з часом цей показник суттєво зменшився – до 48% у жовтні 2023 року, 43% у грудні 2023 року та 36% у лютому 2024 року. Зростає недовіра – частка респондентів, які не довіряють марафону, поступово збільшувалася – з 12% у травні 2022 року до 39% у жовтні 2023 року, 38% у грудні 2023 року та 47% у лютому 2024 року. Частка тих, кому важко відповісти залишалася відносно стабільною, коливаючись у межах 14-19% протягом аналізованого періоду. Загалом спостерігається стійка тенденція до зниження довіри населення до телемарафону та зростання частки тих, хто йому не довіряє.

Індекс медіа грамотності є важливим показником, що відображає рівень здатності населення критично оцінювати медіа інформацію, розпізнавати фейки, маніпуляції та ефективно використовувати медіа ресурси у повсякденному житті. Польовий етап дослідження – з 15 січня по 29 січня 2024 року. Результати опитування наведені на рис. 1.2.

На основі даних рис. 1.2 можемо зробити висновок, що частка аудиторії, яка має рівень вище середнього, зменшилася з 81% у 2022 році до 76% у 2023 році, що свідчить про погіршення загального рівня медіа грамотності серед населення. Показники субіндексу «Розуміння ролі медіа в суспільстві» у 2023 році майже не змінилися порівняно з 2022 роком. Частка людей, які мають високий або вище середнього рівень чутливості до спотвореного контенту, зросла з 65% у 2022 році до 70% у 2023 році, що є позитивним трендом, та свідчить про більшу обізнаність українців щодо маніпуляцій у медіа. Частка аудиторії з високим і вище середнього рівнем цифрової компетентності зменшилася з 64% у 2022 році до 55% у 2023 році, що може свідчити про недостатню увагу до розвитку цифрових навичок серед населення. Хоча українці стали більш чутливими до спотвореного контенту, загальний рівень медіа грамотності знизився, особливо через погіршення цифрової компетентності, що вказує на необхідність подальшої роботи у сфері медіа освіти.

Сучасні міжнародні відносини все більше залежать від ефективної інформаційної політики, яка стає важливим інструментом держав для досягнення зовнішньополітичних цілей, забезпечення національної безпеки та формування міжнародного іміджу. Особливу увагу заслуговує досвід України у протидії інформаційним загрозам під час російсько-української війни та просування власної позиції у глобальному медіапросторі. В контексті інформаційної політики варто відзначити реалізацію державою ключових медіа проєктів, які мають стратегічне значення для комунікації з українською та міжнародною аудиторією. Зокрема, «Єдиний марафон», програми для іноземної аудиторії «FreeDOM» та «The Gaze» стали інструментами для протидії російській дезінформації та висвітлення подій в

Україні для глобального суспільства.

У 2024 році фінансування державних інформаційних проєктів залишилося на рівні попереднього року, що свідчить про стабільність державної підтримки у сфері медіа. Загальна сума витрат на виробництво та трансляцію телемарафонів «Єдині новини» та «FreeДом» склала 843 мільйони гривень, що майже дорівнює показнику 2023 року, коли фінансування цих ініціатив досягло 842 мільйонів гривень, що вказує на незмінність державного підходу до забезпечення інформаційної політики. Значна частина коштів була спрямована на підтримку телемарафону «Єдині новини», який відіграє важливу роль у висвітленні актуальних подій для внутрішньої аудиторії – на його створення у 2024 році було виділено 699 мільйонів гривень. Водночас телемарафон «FreeДом», орієнтований на російськомовну аудиторію за кордоном, отримав фінансування в розмірі 144 мільйони гривень, що підтверджує стратегічний підхід держави до поширення офіційної інформації як всередині країни, так і за її межами.

Контракти на виробництво цих телемарафонів були укладені з тими ж компаніями, що й у попередньому році. Зокрема, їх продовжили отримувати провідні українські медіа групи: телеканали «Інтер», ICTV, «1+1», «Ми – Україна», а також виробнича компанія «Кінокіт», що свідчить про сталість партнерських відносин у сфері державного фінансування інформаційних ініціатив і підтверджує вибір на користь досвідчених медіа виробників, які вже мають практику створення подібного контенту. Збереження рівня фінансування державних інформаційних ресурсів у 2024 році підкреслює їхню важливу роль у формуванні суспільної думки, протидії дезінформації та підтримці національної безпеки в інформаційному просторі. На рис. 1.3 наведено найбільших отримувачів державного фінансування телемарафонів.

Аналіз даних відображених на рис. 1.3, підтверджує тенденцію до стабільного фінансування державних інформаційних проєктів у 2024 році. Незважаючи на мінімальне зменшення загальної суми витрат у порівнянні з 2023 роком, розподіл

коштів між телемарафонами «Єдині новини» та «FreeДом» зберігся майже без змін, що свідчить про пріоритетність внутрішнього інформаційного простору, адже найбільша частина фінансування була спрямована саме на «Єдині новини». Стабільність у розподілі бюджетних ресурсів і збереження тих самих підрядників свідчить про сталість державної стратегії у сфері інформаційної політики. Держава продовжує інвестувати в інструменти поширення офіційної інформації та боротьби з дезінформацією, що залишається критично важливим в умовах військового конфлікту та інформаційного протистояння.

Інформаційна політика України спрямована також на збір доказів військових злочинів та доведення фактів порушення міжнародного права з боку росії. У цьому контексті Україна активно взаємодіє з міжнародними організаціями, включаючи Міжнародний кримінальний суд і правозахисні структури, такі як Amnesty International та Human Rights Watch, задля документування й розповсюдження свідчень щодо злочинних дій російської федерації. Глибокий аналіз протиправної діяльності Росії та її підконтрольних агентів, який охоплює період від лютого-березня 2014 року, свідчить про те, що ці дії аж ніяк не є випадковими чи спонтанними «побічними наслідками» збройного конфлікту. Натомість вони демонструють системний характер і відображають стратегічну поведінку держави-агресора в умовах війни. Так, у підсумковому звіті за 2020 рік в межах попереднього розслідування ситуації в Україні Офіс Прокурора Міжнародного кримінального суду чітко зазначив, що «дії російських агентів на окупованих українських територіях містять ознаки воєнних злочинів і злочинів проти людяності. Ці злочини можуть підпадати під різні юридичні кваліфікації та часто мають кумулятивний характер. До них належать умисні вбивства, напади на цивільне населення й цивільні об'єкти, катування, незаконне позбавлення волі, насильницькі зникнення, примусова мобілізація, позбавлення права на справедливий суд, сексуальне насильство, депортація та примусове переміщення осіб, а також знищення або привласнення майна, включно з об'єктами культурної

спадщини» (Ukrainer, 53).

Після повномасштабного вторгнення Росії 24 лютого 2022 року розслідування міжнародних злочинів на території України здійснювали не лише Міжнародний кримінальний суд, але й Спільна слідча група, Незалежна міжнародна комісія ООН з питань розслідування порушень в Україні та Московські механізми ОБСЄ. Узагальнений аналіз результатів їхньої роботи підтверджує системне скоєння російськими військовими низки міжнародних злочинів, серед яких ключовою є агресія – першопричина збройного конфлікту. Крім того, військові підрозділи РФ регулярно порушують фундаментальні принципи ведення війни: розрізнення між цивільними особами та комбатантами; пропорційність, яка передбачає переважання військової вигоди над завданою шкодою; обережність у виборі цілей; а також гуманність, що виключає застосування методів чи зброї, які спричиняють надмірні страждання. Окрім вже задокументованих до 2022 року випадків воєнних злочинів, особливу увагу приділяють жорсткому поведженню російських військових із полоненими (Ukrainer, 67).

Отже, інформаційна політика є надзвичайно важливим інструментом у сучасних міжнародних відносинах, що дозволяє державам реалізовувати свої інтереси та формувати позитивний імідж на міжнародній арені. Для України, у контексті російсько-української війни, інформаційна політика виступає критично важливим засобом захисту національних інтересів і забезпечення міжнародної підтримки. В умовах глобалізації та розвитку інформаційних технологій, країни повинні активізувати свої зусилля у боротьбі з дезінформацією, формуючи конструктивні наративи, які допоможуть зберегти довіру до державних інститутів та підвищити рівень міжнародної коаліції проти агресії.

РОЗДІЛ 2

ІНФОРМАЦІЙНА БЕЗПЕКА УКРАЇНИ: ЗАГРОЗИ ТА ВІДПОВІДІ

2.1 Методи та інструменти інформаційних атак

З початком повномасштабного вторгнення росії в Україну в лютому 2022 року інформаційна війна набула безпрецедентної інтенсивності. Росія активно задіяла різноманітні медіа-платформи, соціальні мережі та інші канали комунікації для досягнення своїх стратегічних цілей: посіяти хаос, викликати невпевненість та змусити українців піддатися проросійським наративам. Серед поширених дезінформаційних прийомів були фейкові новини про обстріли з боку Збройних сил України, брехливі повідомлення про масові замінування шкіл і торговельних центрів, а також неправдиві заяви про широкомасштабне вторгнення. Усе це мало на меті створення атмосфери страху й дестабілізації. Інформаційно-психологічні операції (ІПСО) були націлені на деморалізацію українського суспільства, послаблення довіри до влади та віри у майбутнє країни (Свідерська, 2022:60).

Дослідження Центру стратегічних комунікацій та інформаційної безпеки й Центру демократії та верховенства права (Інформаційні атаки, 57) виявило, що одним із головних інструментів інформаційної війни росії є використання рекламних кампаній у соціальних мережах, таких як Facebook. Основними цілями цих кампаній були створення паніки, дискредитація української влади та підірив довіри до Збройних сил України. російська пропаганда активно використовувала таргетинг реклами, націлюючись на різні групи населення, зокрема мешканців прифронтових регіонів та українців за кордоном. Для цього використовувалися фінансові схеми через псевдо компанії, а також «фабрики тролів», які розміщували тисячі рекламних оголошень із маніпулятивним змістом. Наслідки таких кампаній виявлялися у створенні «інформаційних бульбашок», де користувачі отримували виключно дезінформацію, що підсилювала їхні упередження, що суттєво впливало

на рівень довіри до офіційних джерел інформації та підривало моральний стан суспільства. Для протидії дезінформаційним кампаніям дослідження підкреслює важливість розвитку фактчекінгу, співпраці з платформами соціальних мереж та впровадження освітніх програм із медіа грамотності. В табл. 2.1 виокремлено ключові теми, які протягом досліджуваного періоду відпрацьовували автори повідомлень. Особливістю таких кампаній було поєднання декількох тематичних акцентів у рамках одного повідомлення. Для зручності аналізу такі повідомлення класифікувалися за їх основною темою. В представленій аналітиці демонструється розподіл цих наративів за ключовими напрямками (рис. 2.1).

Особливо активною стала кампанія дезінформації, спрямована на підрив авторитету української влади та Збройних Сил України. Через контрольовані медіа-ресурси росія поширювала хибну інформацію про буцімто масові капітуляції українських військових. На перших етапах вторгнення ці наративи домінували в російських медіа: повідомлялося про те, що військові в Україні нібито здаються в полон або переходять на російський бік. Основним завданням таких дезінформаційних атак було зниження бойового духу не лише серед військових, але й серед цивільного населення. Одночасно через телеграм-канали активно поширювалася недостовірна інформація, що уряд України начебто втратив контроль над ситуацією, виїхав із країни або прийняв капітуляцію. Інші фейки включали заяви про теплий прийом окупантів у захоплених регіонах та звинувачення у начебто незаконному прослуховуванні громадян спецслужбами під час воєнного стану (Укрінформ, 35)

Після початку вторгнення різко збільшилася кількість кібератак на державні ресурси й ключові галузі України: транспортну інфраструктуру, енергетику та фінансовий сектор. Щомісячно реєструвалося близько 25 мільйонів хакерських атак, що становило серйозну загрозу для цифрових прав, таких як конфіденційність листування, право на приватність і безпеку особистих даних. Хакери переслідували різні цілі – від виманювання коштів до крадіжки стратегічної інформації та

саботажу роботи критичних систем (Детектор-медіа, 25). У 2024 році команда CERT-UA опрацювала 4315 кіберінцидентів, що на 69,8% більше, ніж у 2023 році. Найбільш поширеними загрозами стали фішингові кампанії, використання шкідливого програмного забезпечення та атаки на веб ресурси органів влади. Особливу увагу приділяли атакам із використанням програми-шифрувальника «Cobalt Strike» та розповсюдженню вірусів сімейства «SmokeLoader». Основними цілями залишалися урядові установи, військовий сектор та критична інфраструктура, зокрема енергетика та телекомунікації. Загалом спостерігалася еволюція методів атак: зловмисники вдосконалювали тактики соціальної інженерії, а також використовували нові шляхи проникнення в державні та комерційні системи. Водночас українські кібер-фахівці та міжнародні партнери посилили заходи кіберзахисту, що дозволило мінімізувати масштаб деяких атак та запобігти витоку критично важливої інформації.

З початком повномасштабного вторгнення росії Україна стала головною мішенню для кібератак у світі. Вже 14 січня 2022 року Україна посіла перше місце у світі за кількістю атак, спрямованих проти неї. У перші місяці вторгнення кількість кібератак зросла втричі порівняно з 2021 роком. Особливий акцент було зроблено на критичну інфраструктуру, включно з енергетичним сектором. Наприклад, у квітні 2022 року вдалося запобігти атаці на енергетичну компанію, яка могла спричинити масштабні перебої з електропостачанням. Окупанти поєднували ракетні удари з кібератаками. Восени 2022 року, паралельно з фізичними обстрілами енергетичної інфраструктури, активізувалися дії хакерів. Завдяки оперативній роботі українських фахівців із кіберзахисту, ці атаки вдалося нейтралізувати, запобігши значним пошкодженням. Цей досвід демонструє не лише вразливість цифрових систем до атак під час війни, але й важливість підготовки та модернізації інструментів кібербезпеки, які стають ключовим елементом захисту сучасної держави.

На рис. 2.2 наведено злочини, які росія вчиняє проти медіа та журналістів в

Україні в період з 24 лютого 2022 року до серпня 2024 року. Зокрема, він відображає статистику нападів, кібератак, викрадень та вбивств журналістів, що є частиною широкомасштабної інформаційної агресії з боку рф. Згідно з даними Інституту масової інформації, ці порушення включають не тільки фізичне насильство, а й інші методи, спрямовані на блокування доступу до інформації та обмеження свободи слова. Використання таких методів є важливим елементом стратегії інформаційної війни, мета якої – дезорганізувати медіа-простір України та обмежити доступ до правдивої інформації.

Інформаційно-психологічні спеціальні операції (ІПСО) стали ключовим засобом впливу російської федерації, спрямованим на підірив репутації України в очах міжнародної спільноти та її громадян. Основна мета цих операцій полягає у маніпуляції емоціями, настроями та поведінкою населення через створення атмосфери хаосу, паніки та недовіри. Їхній вплив можемо поділити на декілька категорій, залежно від тривалості й завдань, які вони переслідують. Короткострокові ІПСО зазвичай орієнтовані на негайне дестабілізування ситуації через породження паніки або дезорієнтації. Наприклад, у перші дні повномасштабного вторгнення українське населення активно замальовувало позначки на будівлях, вважаючи їх інструментами ворога для коригування ракетних ударів. Поширення фейкових повідомлень про заплановані масовані обстріли на символічні дати, такі як День Незалежності чи новорічні свята, також стимулювало страх і занепокоєння. Хоча існує ймовірність, що атаки можуть відбутися будь-якого дня, саме потік таких прогнозів ускладнює розрізнення правдивих загроз від неправдивих.

Довгострокові ІПСО мають більш системний характер і спрямовані на формування постійного емоційного тиску, деморалізацію населення і посилення зневіри. Аналіз, здійснений Центром з питань захисту цивільного населення в умовах конфлікту, свідчить про те, що поширення дезінформації призводить до почуття розгубленості, емоційного виснаження та зростання тривожності.

Наприклад, фейкові повідомлення про примусову евакуацію з прифронтових територій або про уявні атаки українських військових проти цивільного населення можуть стимулювати прийняття рішень, що шкодять індивідуальному добробуту громадян. Таким чином, ІПСО є надзвичайно ефективним інструментом впливу, який спирається на емоційні реакції та інформаційну вразливість людей. Важливість критичного мислення та перевірки фактів стає першочерговою умовою для протидії таким формам психологічного та інформаційного тиску

З початку повномасштабної агресії російської федерації задокументовано понад 2000 випадків кібератак на українські державні та комерційні структури. Окрім того, було проведено численні інформаційно-психологічні операції (ІПСО) через соціальні мережі, що супроводжувалися систематичним поширенням пропагандистських наративів, використовуючи всі доступні засоби для впливу на інформаційне середовище. Зміни у довірі українців до різних джерел інформації за останні роки є важливим показником впливу інформаційного середовища та медіа на суспільну думку. Згідно з даними соціологічного дослідження «Медіа споживання українців: третій рік повномасштабної війни», проведеного у 2024 році, рівень довіри до основних джерел інформації, таких як телебачення, соцмережі, інтернет та друковані ЗМІ, зазнав значного зниження. У табл. 2.2 наведено порівняння рівня довіри до різних джерел.

Приклад окупації українських населених пунктів демонструє надзвичайну роль інформаційної боротьби в умовах конфлікту. російські окупаційні сили активно блокують діяльність українських мобільних операторів, захоплюють місцеві офіси інтернет-провайдерів та викрадають їхню інфраструктуру, замінюючи її так званими «сірими» операторами, що дозволяє окупантам обмежувати доступ до невігідних платформ, зокрема соціальних мереж та українських веб-сайтів. Станом на березень 2023 року на тимчасово окупованих територіях було заблоковано 979 українських ресурсів, зокрема 10 офіційних сайтів органів державної влади України. Робота як мінімум 46 українських інтернет-

провайдерів була припинена, що зробило недоступними платформи Viber, Instagram, Twitter, Google та YouTube.

Влітку 2022 року громадська організація «ОПОРА», яка спеціалізується на аналізі соціальних мереж, здійснила перше комплексне дослідження російської пропаганди на окупованих територіях. Було ідентифіковано базу з 118 Telegram-каналів, підконтрольних окупантам. Додатковий аналіз репостів дозволив розширити цю базу до 640 каналів, які класифіковані на п'ять основних категорій: місцеві ЗМІ, адміністративні канали, представники громадських організацій, сторінки публічних осіб та канали, що займаються обміном і продажем товарів. Місцеві медіа виконують функцію створення ілюзії нормального життя в окупованих районах, водночас дискредитуючи українську владу та Збройні Сили України. Вони також поширюють дезінформацію про війну й формують позитивний імідж армії РФ. Адміністративні канали подають інформацію від окупаційних адміністрацій, місцевої поліції та російських державних установ. Благодійні й волонтерські організації застосовуються для просування проросійської риторики. Сторінки публічних осіб здебільшого належать представникам окупаційної влади або проросійським медійникам.

Зміст, представлених у таких інформаційних каналах, можна структурно розподілити на кілька тематичних напрямів. Перший блок зосереджується на висвітленні соціальної підтримки мешканців окупованих територій, включаючи надання матеріальної допомоги вразливим категоріям населення відповідно до норм російського законодавства. Другий напрям спрямований на популяризацію російської та радянської культури, зокрема через демонстрацію творчості російських письменників і митців, а також організацію культурно-історичних заходів. Окремо прослідковується акцент на ностальгії за радянською епохою, що виявляється у святкуванні радянських пам'ятних дат та публікаціях, присвячених історії населених пунктів у часи СРСР. Додатково виділяються зусилля, спрямовані на інтеграцію з іншими регіонами російської федерації, через висвітлення

активностей, пов'язаних із професійною допомогою, благодійністю та відбудовою зруйнованих населених пунктів. Значну частину контенту становлять матеріали, спрямовані на дискредитацію України та її державної влади. Цей напрям включає поширення дезінформації про обстріли цивільного населення Збройними силами України, звинувачення у провокаціях та інші негативні наративи. Крім того, окремий блок стосується повідомлень про боротьбу з алкоголізмом, наркоманією, торгівлею контрафактною продукцією та вилученням української зброї з незаконного обігу. Такі теми додатково слугують інструментом дискредитації населення з проукраїнськими поглядами (ОПОРА, 32).

Після рішення України у 2021 році заборонити діяльність проросійських політичних партій та медіа, російська пропаганда трактувала ці кроки як прояви агресивної цензури та боротьби з політичними опонентами. Такі інтерпретації активно підтримувалися консервативними медіа, такими як Fox News, які навіть характеризували президента Володимира Зеленського як диктатора. Подібне спотворення фактів потенційно загрожує міжнародною підтримкою України. Зокрема, під час масованого обстрілу у листопаді 2022 року інцидент із падінням ракети у польському селі Пшеводув набув широкого розголосу. У подальших версіях зазначалося, що ракета могла належати українській системі протиповітряної оборони. російські медіа активно використовували цю подію для провокування напруженості у відносинах між Україною та Польщею, прагнучи таким чином підірвати підтримку з боку одного із ключових союзників України (Ukrainer, 75).

2.2 Державна політика в сфері інформаційної безпеки

Інформаційна безпека є невід'ємною та стратегічною складовою національної безпеки будь-якої держави, особливо в умовах глобальної цифровізації та інтенсивного розвитку інформаційних технологій. Сучасний

інформаційний простір стає ареною не лише для обміну даними, а й для протистояння різних суб'єктів, що використовують кіберпростір у своїх інтересах. Посилення кібератак та дезінформаційних кампаній робить необхідним чітке формування та реалізацію державної політики у сфері інформаційної безпеки. Звіт Державного центру кіберзахисту Державної служби спеціального зв'язку та захисту України (далі – ДЦКЗ Держспецзв'язку) є важливим джерелом інформації для оцінки та аналізу державної політики у цій сфері – у ньому висвітлюються ключові загрози, виклики та методи протидії у сфері кіберзахисту, а також наводяться пріоритетні напрями діяльності державних органів. Основними завданнями ДЦКЗ Держспецзв'язку є створення єдиної та ефективної інтегрованої моделі кібербезпеки, що забезпечує комплексний захист державної та критичної інформаційної інфраструктури. Ця система має працювати не лише в умовах стабільності, а й у ситуаціях кризового реагування. До ключових напрямків діяльності у сфері інформаційної безпеки належать:

- забезпечення стійкого та захищеного доступу державних органів до мережі Інтернет через створення високотехнологічних систем безпеки;
- впровадження національної системи антивірусного захисту та механізмів запобігання кіберзагрозам для захисту державних інформаційних ресурсів;
- проведення комплексних аудитів інформаційної безпеки, а також детальна оцінка стану кіберзахисту об'єктів критичної інфраструктури;
- розробка та впровадження інноваційних систем виявлення вразливостей, а також швидкого та ефективного реагування на кіберінциденти й атаки;
- налагодження міжнародної та міжвідомчої взаємодії між командами реагування на комп'ютерні надзвичайні події, що є важливим фактором у боротьбі з глобальними кіберзагрозами.

Наведені заходи спрямовані на посилення національної кібербезпеки, створення ефективних механізмів захисту державних ресурсів та адаптацію державної політики до нових викликів у цій сфері (Оперативний центр). Рис. 2.3

відображає ключові статистичні дані щодо динаміки змін у кількості зареєстрованих кіберінцидентів, оброблених підозрілих подій та критичних інцидентів у 2023 році.

Унаслідок активних бойових дій та зростання рівня кіберзагроз доступ до детальних та актуальних статистичних даних щодо частоти атак, їхніх наслідків і засобів протидії залишається обмеженим. Проте історичні аналітичні джерела свідчать про тенденцію до зростання вразливості українських компаній та державних установ до кіберзагроз. Так, ще у 2018 році близько 31% підприємств зазнали впливу кіберзлочинів, що вказує на збільшення цього показника порівняно з 24% у 2016 році. Дані опитувань свідчать про те, що українські компанії частіше, ніж їхні міжнародні аналоги, стикалися з такими явищами, як зрив бізнес-процесів, вимагання викупу, порушення прав інтелектуальної власності, крадіжки даних, маніпуляції з банківськими транзакціями, а також із політично мотивованими чи державними спонсорованими атаками (Forbes, 2023). Ці дані підтверджують, що інформаційна безпека є не лише технологічним викликом, а й стратегічним питанням, яке потребує комплексного підходу, міжнародної співпраці та постійного вдосконалення систем кіберзахисту.

Зважаючи на масштаби та складність цих загроз, Україна ще до початку бойових дій розпочала впровадження структурних заходів для посилення кіберзахисту. Ключовим кроком стало ухвалення першої Національної стратегії кібербезпеки на період 2016-2020 років, яку продовжила реалізація нинішньої Стратегії кібербезпеки України на 2021-2025 роки. Ця стратегія передбачає низку положень, спрямованих на боротьбу з кібертероризмом та кібершпигунством, одночасно акцентуючи увагу на питаннях цифрової безпеки із врахуванням економічних і соціальних аспектів. Концепція побудована на трьох ключових засадах: стримування, кіберстійкість і взаємодія. У документі враховано окремі положення з Рекомендацій Ради ОЕСР щодо національних стратегій цифрової безпеки, зокрема підвищення обізнаності про кіберризики, управління

уразливостями та міжнародну співпрацю. Водночас реалізація цих принципів залишається нерівномірною і часто обмеженою (National Security, 2021-2025). Зважаючи на складність і масштабність кіберзагроз, вкрай важливо, щоб в органах влади активно розвивалися спеціалізовані підрозділи, здатні реагувати на новітні загрози. Включення кіберспеціалізованих фахівців до складу антикорупційних, правоохоронних та розвідувальних структур дозволить швидше і ефективніше реагувати на кіберінциденти.

Інтеграція державних і приватних механізмів протидії кіберзагрозам є важливим аспектом стратегії інформаційної безпеки України. Важливою є політична відповідальність держави за створення нормативно-правових механізмів, які регулюють співпрацю між державними та приватними суб'єктами у сфері кібербезпеки. Приватний сектор, зокрема компанії, що керують критичною інфраструктурою (енергетика, транспорт, фінанси), часто є головними цілями кіберзлочинців, що зумовлює необхідність не лише технічної взаємодії, але й політичної координації, спрямованої на забезпечення чіткої регламентації обміну інформацією, стандартів безпеки та проведення спільних навчань. Ефективні нормативно-правові механізми дозволяють формувати довіру між приватним сектором і державою, сприяючи зміцненню національної кібербезпеки та ефективному реагуванню на виклики сучасного цифрового світу. Обмін інформацією, впровадження стандартів безпеки та проведення спільних кібернавчань допомагають зменшити вразливість критичних об'єктів інфраструктури.

Важливими інструментами для раннього виявлення загроз є кіберрозвідка і кібермоніторинг, що дозволяють швидко реагувати на потенційні інциденти. Міжнародне співробітництво в сфері кібербезпеки також є важливим елементом, оскільки кібератаки часто не мають кордонів. Водночас, воно відіграє ключову роль у зміцненні позицій України на геополітичній арені. Україна активно співпрацює з міжнародними організаціями, такими як НАТО, ЄС та ООН, не лише

для обміну інформацією про нові загрози чи узгодження стратегій реагування, але й для посилення свого авторитету як активного учасника глобальної безпеки. Така взаємодія сприяє формуванню міжнародного порядку денного, спрямованого на встановлення загальноприйнятих стандартів поведінки в кіберпросторі. Крім того, участь у міжнародних ініціативах дозволяє Україні інтегруватися у світову спільноту кібербезпеки, що зміцнює її зовнішню політику, спрямовану на стримування агресії, розвиток партнерських відносин та сприяння глобальній Стабільності (Завгородня, 2024, 20).

У 2022 році Україна зайняла 24 місце в індексі Кібербезпеки поряд з такими країнами як Італія та Малайзія, і входить до 25-ти країн з високим рівнем інформаційного захисту (Hawdon, 2021: 837-842), що є наслідком, того, що саме збройна агресія РФ стимулювала збільшити рівень кібербезпеки України та захищати країну в інформаційному просторі. Щодо інституційної складової забезпечення інформаційної безпеки, то сьогодні забезпечення її належного рівня має стати пріоритетом Міністерства цифрової трансформації України, оскільки на нього покладається завдання щодо участі у «формуванні державної політики у сферах криптографічного та технічного захисту інформації, кіберзахисту, ..., захисту державних інформаційних ресурсів та інформації, вимога щодо захисту якої встановлена законом, в інформаційних, електронних комунікаційних та інформаційно-комунікаційних системах і на об'єктах інформаційної діяльності, а також у сферах використання державних інформаційних ресурсів в частині захисту інформації, протидії технічним розвідкам, функціонування, безпеки та розвитку державної системи урядового зв'язку, Національної системи конфіденційного зв'язку».

Стратегія наголошує на необхідності покращення координації між різними суб'єктами національної системи кібербезпеки. Особлива увага приділяється налагодженню оперативного обміну інформацією про кіберзагрози, створенню ефективної системи підготовки кадрів і розробці моделей державно-приватного

партнерства – напрямку, передбаченого попередньою стратегією, але значною мірою нерозвиненого. Інституційна основа реалізації політики у сфері інформаційної та цифрової безпеки здебільшого покладається на Міністерство культури та інформаційної політики України. Цей орган виконавчої влади визначено відповідальним за формування та реалізацію державної політики в галузі інформаційної безпеки (Остроухов, 2021:15).

Серед принципів діяльності Міністерства виділяються такі ключові положення: «дотримання Конституції та законодавства України; впровадження міжнародно визнаних принципів і норм права; забезпечення рівноправності для всіх учасників інформаційної взаємодії незалежно від їхнього політичного, соціального чи економічного статусу; і пріоритетний розвиток сучасних вітчизняних інформаційних і телекомунікаційних технологій. Саме на неї покладено обов'язки щодо «координації діяльності суб'єктів забезпечення кібербезпеки щодо кіберзахисту; та забезпечення впровадження системи аудиту інформаційної безпеки на об'єктах критичної інфраструктури...» (Закон України, 2006).

Державним органом, який відповідає за інформаційну безпеку, є й Департамент кіберполіції Національної поліції України – «міжрегіональний територіальний орган Національної поліції України, який входить до складу кримінальної поліції та відповідно до законодавства України забезпечує реалізацію державної політики у боротьбі з кіберзлочинністю» (Про Департамент, 2006). Крім того, в Україні створено систему спеціалізованих органів з кібербезпеки, а до боротьби з кіберзлочинністю залучені звичайні слідчі, які проводять розслідування кіберзлочинів під процесуальним контролем прокуратури. Водночас існує низка проблем щодо забезпечення інформаційної та кібернетичної безпеки в Україні, які негативно впливають на функціонування держави та її міжнародний імідж. Зокрема, брак висококваліфікованих кадрів та відсутність кіберспеціалізації серед слідчих і прокурорів ускладнюють ефективне

реагування на кіберзагрози, що ставить під загрозу національну безпеку. Невідповідність законодавства сучасним реаліям, а також складність у взаємодії між різними державними суб'єктами, створюють прогалини у захисті від зовнішніх та внутрішніх кіберзагроз, що може погіршити здатність держави протидіяти викликам у сфері безпеки.

Одним з напрямів вирішення цих проблем ми пропонуємо створити спеціалізовані слідчі підрозділи та відповідні підрозділи прокуратури з розслідування кіберзлочинів та запровадити відповідну спеціалізацію суддів. Крім того, для координації наукових розробок на базі Українського науково-дослідного інституту спеціальної техніки та судово-медичної експертизи СБУ створити майданчик для постійного обміну досвідом та досягненнями у галузі кібербезпеки. Результати аналізу заходів щодо забезпечення інформаційної безпеки України вказують на значні недоліки в реалізації політики. Зокрема, відсутність впровадження ефективних попередніх стратегій, а також недостатня координація між органами державної влади, призводять до зниження рівня інформаційної безпеки, що, в свою чергу, ставить під загрозу здатність держави захищати важливі національні інтереси та реагувати на сучасні кіберзагрози, що виникають в умовах глобалізації та цифрових трансформацій. Тому захист інформаційного суверенітету, формування більш ефективної системи інформаційної безпеки, розробка та реалізація ефективних стратегій та тактик протидії інформаційним та кібернетичним загрозам мають стати пріоритетними завданнями органів державної влади, спеціальних служб та правоохоронних органів та недержавних інституцій.

РОЗДІЛ 3

ІНФОРМАЦІЙНА ПОЛІТИКА УКРАЇНИ У ПРОТИДІЇ РОСІЙСЬКІЙ АГРЕСІЇ

3.1 Основні напрями інформаційної політики України у сфері протидії дезінформації та російській пропаганді

Інформаційна політика в умовах сучасних викликів відіграє важливу роль у забезпеченні національної безпеки України. Особливо це стосується протидії дезінформації та російській пропаганді, які є одним з основних інструментів гібридної війни росії проти нашої держави. Ворог активно використовує інформацію для маніпулювання свідомістю громадян, створення хаосу та підриву морального духу суспільства. З початком військової агресії рф Україна стала перед обличчям численних інформаційних атак, мета яких – посіяти розбіжності серед населення, послабити підтримку уряду та створити сприятливе середовище для дестабілізації ситуації в країні. Тому боротьба з дезінформацією та пропагандою стала однією з найважливіших складових державної політики.

Для протидії цим загрозам Україна розробила низку стратегій та заходів. Одним із ключових напрямів є підвищення рівня медіа грамотності серед громадян, що дає можливість людям критично оцінювати інформацію, яку вони отримують з різних джерел. Крім того, важливим аспектом є розвиток національних медіа, які можуть стати реальними конкурентами російським інформаційним каналам. Водночас Україна активно співпрацює з міжнародними партнерами, щоб спільними зусиллями протистояти інформаційним маніпуляціям, що здійснюються на глобальному рівні. Процес протидії інформаційним загрозам є складним і багатограним, адже він вимагає постійної адаптації до нових реалій та методів, які використовує агресор. В умовах гібридної війни держави відіграють критично важливу роль у захисті інформаційного простору. Вони здатні впроваджувати законодавчі

ініціативи для регулювання поширення інформації, застосовувати санкції проти платформ, що сприяють розповсюдженню фейкових новин, та засновувати спеціалізовані установи для моніторингу і протидії інформаційним загрозам(Лабенко,2023:331-345). Так, в Україні була запущена платформа StopFake, яка ефективно виконує завдання з виявлення та спростування дезінформації, пов'язаної із ситуаціями в країні.

Одним з важливих напрямів боротьби з дезінформацією та російською пропагандою в Україні є розвиток медіа грамотності серед ключових гравців інформаційного простору. Наприклад, у червні 2023 року для працівників Національної ради України з питань телебачення і радіомовлення було проведено тренінг, організований платформою StopFake, що є частиною співпраці між медіа регулятором та громадською організацією. Заступниця головного редактора StopFake, Вікторія Романюк, провела вебінар, на якому учасники ознайомилися з основними поняттями, такими як дезінформація, фейки та маніпуляції, а також розглянули різні методи їх поширення. Особлива увага на вебінарі була приділена методам перевірки дезінформації. Учасники розглянули алгоритми та інструменти для виявлення маніпуляцій, зокрема такі механізми, які використовують емоційний вплив для швидкого маніпулювання громадською думкою. Також було акцентовано на тому, як важливо бути критичним навіть до авторитетних джерел, адже неправильно інтерпретовані дані можуть стати основою для маніпуляцій. Завдяки такій освітній діяльності, як цей тренінг, українські фахівці можуть покращити свої навички з медіа грамотності та ефективніше протидіяти інформаційним атакам, включаючи пропагандистські наративи, що використовуються росією. Цей тренінг став частиною стратегії державної інформаційної політики, спрямованої на боротьбу з фальшивими новинами та підвищення загальної медіа грамотності в країні. Одним із ключових інструментів поширення дезінформації та російської пропаганди в Україні є телеграм-канали. Завдяки анонімності, відсутності жорсткої модерації та можливості швидкого

розповсюдження контенту, вони стали ефективним засобом маніпуляції громадською думкою.

Дослідження, проведене Texty.org.ua (Texty.org.ua,) виявило низку впливових телеграм-каналів, які поширюють маніпулятивні наративи, часто використовуючи методи емоційного впливу та інформаційних вкидів. Зокрема, такі ресурси експлуатують страх, недовіру до офіційних джерел інформації та соціальні конфлікти, щоб дестабілізувати суспільні настрої. На рис. 3.1 представлено рівень маніпулятивності за 10 показниками.

Аналіз рис. 3.1 свідчить про значний рівень маніпулятивності в різних групах телеграм-каналів. Найвищі показники характерні для проросійських каналів, що підтверджує їхню цілеспрямовану роботу з дезінформаційними наративами. Блогери також демонструють високий рівень маніпулятивності, що може бути пов'язано як із суб'єктивним підходом до подачі інформації, так і з можливим поширенням неперевірених даних. Державні джерела та новинні агрегатори займають проміжну позицію, що може свідчити про присутність маніпулятивних технік, але з меншим ухилом у дезінформацію. Найнижчий рівень маніпулятивності спостерігається в офіційних редакціях, що вказує на порівняно вищі стандарти журналістики та фактчекінгу в традиційних медіа. Результати дослідження підтверджують важливість критичного мислення при споживанні контенту з телеграм-каналів, а також необхідність систематичного моніторингу інформаційного простору для протидії дезінформаційним кампаніям.

На рис. 3.2 наведено частку маніпулятивних повідомлень у трьох популярних українських телеграм-каналах, серед яких «Суспільне», «Труха» та «Резидент». Візуалізація демонструє загальну кількість дописів, а також використання різних маніпулятивних прийомів, таких як емоційно навантажена мова, узагальнення, апеляція до страху та сумнівів.

Дані свідчать про значні відмінності в рівні маніпулятивності між каналами. «Суспільне», яке позиціонується як державне медіа, має найнижчий відсоток маніпулятивних матеріалів. «Труха» демонструє помірний рівень маніпулятивності, використовуючи емоційно забарвлену мову та узагальнення. Натомість «Резидент» виділяється надзвичайно високим рівнем маніпуляцій, що свідчить про систематичне використання пропагандистських технік для впливу на громадську думку.

Україна активно використовує законодавчі механізми для боротьби з дезінформацією та пропагандою, які є складовою частиною інформаційної агресії рф. Одним із ключових викликів у цій сфері є відсутність чіткого визначення поняття «дезінформація» в українському законодавстві, що ускладнює правозастосування та боротьбу з маніпулятивним контентом. У 2019 році Міністерство культури, молоді та спорту України ініціювало законопроект «Про протидію дезінформації», який передбачав введення юридичної відповідальності за поширення фейкової інформації, створення уповноваженого органу з протидії дезінформації та запровадження стандартів журналістської етики. Проте законопроект викликав значний суспільний резонанс, оскільки його положення могли обмежити свободу слова, і врешті-решт він не був ухвалений.

Водночас Україна застосовує інші правові інструменти для захисту інформаційного простору. Зокрема, з 2021 року активно використовуються санкції Ради національної безпеки і оборони України (РНБО), спрямовані на блокування проросійських медіа та ресурсів, що поширюють ворожу пропаганду. Важливим кроком стало припинення діяльності телеканалів «112 Україна», NewsOne та ZIK, які належали проросійському олігарху Віктору Медведчуку та систематично транслювали маніпулятивні наративи. Також у 2022 році, після повномасштабного вторгнення рф, Україна активізувала боротьбу з ворожою дезінформацією шляхом блокування сотень веб-ресурсів, телеграм-каналів та пропагандистських платформ. Такі заходи спрямовані на обмеження впливу інформаційної зброї, яку

використовує росія для дестабілізації суспільства, зниження довіри до державних інституцій та провокування панічних настроїв серед населення.

Таким чином, законодавче регулювання є важливою складовою інформаційної політики України у сфері протидії дезінформації та російській пропаганді. Попри виклики, держава продовжує шукати ефективні механізми контролю за інформаційним простором, зберігаючи баланс між безпекою та свободою слова.

Окрім законодавчих механізмів і санкційних заходів, Україна активно розвиває освітні проєкти, спрямовані на підвищення рівня медіа грамотності населення. Одним із таких проєктів став міні серіал про протидію дезінформації, створений за підтримки українських медійних організацій. Його мета – навчити громадян розпізнавати фейки, розуміти механізми маніпуляції та критично оцінювати інформацію. Серіал пояснює ключові принципи роботи пропагандистських технологій, а також демонструє реальні приклади інформаційних атак, спрямованих на українське суспільство. Особливий акцент зроблено на методах, які використовує російська пропаганда для створення недовіри до державних інституцій, розпалювання паніки та формування спотвореного сприйняття подій. Подібні ініціативи є важливою складовою інформаційної політики України, адже вони не лише інформують громадян, а й формують стійкість суспільства до маніпуляцій. Отже, чим вищий рівень медіа грамотності серед населення, тим складніше дезінформаційним кампаніям впливати на громадську думку та послаблювати єдність українців (Укрінформ).

Таким чином, інформаційна політика України в умовах російсько-української війни спрямована на ефективну протидію дезінформації та пропаганді, які є важливими елементами гібридної війни. У відповідь на ці загрози держава реалізує комплексні стратегії, включаючи розвиток медіа грамотності серед громадян, створення спеціалізованих платформ для спростування фейкових новин, та застосування правових механізмів для блокування пропагандистських ресурсів.

Роль законодавчого регулювання, а також міжнародна співпраця, є важливими складовими цієї стратегії. Підвищення медіа грамотності та критичного мислення серед населення є запорукою стійкості суспільства до маніпуляцій і допомагає зберігати єдність нації в умовах інформаційної агресії.

3.2 Виклики та перспективи розвитку інформаційної політики в Україні

Інформаційна політика держави відіграє ключову роль у формуванні суспільної свідомості, забезпеченні національної безпеки та протидії зовнішнім загрозам. В умовах гібридної війни її значення зростає, адже боротьба ведеться не лише на полі бою, а й в інформаційному просторі. Внутрішні бар'єри, зокрема нестача фінансування, фахівців та корупційні ризики, ускладнюють ефективну реалізацію цієї політики. Повномасштабне вторгнення Росії загострило проблему, оскільки інформаційний простір став одним із головних напрямів протистояння, де використовуються маніпуляції, дезінформація та кібернетичні атаки.

Російська дезінформаційна кампанія активно використовує соціальні мережі, анонімні Telegram-канали та псевдоаналітичні ресурси для поширення фейків. Як зазначено у звіті «Детектор медіа», у період з 13 по 19 січня 2025 року зафіксовано активну хвилю дезінформації (рис. 3.3). Основні наративи включали твердження про «колоніальний статус» України, провал мобілізації та нібито втрату територій. Головна мета таких фейків – посіяти паніку в суспільстві, підірвати довіру до влади та міжнародних союзників.

У той же час, саме інформаційна політика держави повинна стати основою для ефективної боротьби з такими загрозами. В Україні існує потреба в системному підході до розробки та реалізації стратегій, що сприятимуть формуванню національної інформаційної політики, спрямованої на захист від зовнішніх і внутрішніх викликів. Тому розвиток політичних механізмів у цій сфері потребує належної уваги, зокрема в частині розробки та оновлення законодавчих ініціатив,

створення структур для ефективного управління інформаційними потоками та підвищення рівня медіа грамотності населення.

Однак на шляху до ефективної реалізації інформаційної політики в Україні є кілька внутрішніх бар'єрів, які суттєво ускладнюють цей процес. Одним з основних викликів є відсутність достатнього фінансування. Багато програм у сфері інформаційної безпеки та стратегічних комунікацій не отримують належного бюджету, що перешкоджає розвитку критичної інфраструктури, оновленню технологій та проведенню освітніх кампаній. Україна досі значною мірою залежить від зовнішнього фінансування для покриття витрат на боротьбу з інформаційними атаками, що робить країну вразливою до змін на міжнародному рівні.

Корупція, яка проникає в різні сфери управління, також негативно впливає на ефективність інформаційної політики. Проблеми з розподілом фінансових ресурсів, які мають йти на забезпечення безпеки інформаційного простору, часто призводять до неефективного використання коштів та зниження якості інформаційних кампаній. Такі корупційні схеми ускладнюють реалізацію важливих державних ініціатив, роблячи систему більш вразливою до маніпуляцій. Окрім цього, високий рівень корупції створює недовіру громадян до державних органів та офіційних інформаційних джерел. В умовах інформаційної війни це стає критичним викликом, оскільки суспільство схильне шукати альтернативні, часто неперевірені або навіть ворожі наративи. Недостатня прозорість влади та відсутність ефективних антикорупційних механізмів лише поглиблюють цю проблему. Рівень корупції в Україні залишається одним із визначальних чинників, що впливають на можливості держави в інформаційній сфері. Для кращого розуміння ситуації розглянемо індекс сприйняття корупції в Україні у порівнянні з іншими країнами-кандидатами на вступ до ЄС.

Аналіз рис. 3.5 демонструє, що Україна залишається серед країн із високим рівнем корупційних ризиків, що суттєво ускладнює реалізацію ефективної інформаційної політики. У порівнянні з іншими країнами-кандидатами на вступ до

ЄС, показник України є нижчим за середній рівень, що вказує на необхідність посилення антикорупційних заходів та підвищення прозорості державного управління. Високий рівень корупції підриває реалізацію державної інформаційної політики, оскільки обмежує фінансування стратегічних комунікацій, знижує ефективність інформаційних кампаній та посилює вплив маніпулятивного контенту, що загрожує інформаційній безпеці країни.

Політична нестабільність також грає свою роль: суперечності між політичними силами та інтереси окремих груп часто заважають формуванню єдиної стратегії інформаційної політики. Часто це призводить до фрагментарності рішень, відсутності послідовності у впровадженні реформ і нерідко – до використання інформаційної політики як інструменту політичної боротьби. Водночас недостатня координація між державними органами ускладнює реагування на інформаційні виклики та загрози. І, зрештою, технічні проблеми, такі як застаріле програмне забезпечення, відсутність сучасних інструментів для моніторингу кіберзагроз та недостатній рівень кібер-грамотності державних службовців, залишають країну вразливою до зовнішніх атак, сприяючи поширенню дезінформації та втраті контролю над інформаційним простором.

Додатковим фактором, що посилює ці проблеми, є низький рівень довіри громадян до державних інституцій. За даними Київського міжнародного інституту соціології, станом на грудень 2024 року Верховній Раді України довіряють лише 35% громадян, а Кабінету Міністрів – 41%. Високий рівень недовіри до ключових органів влади ускладнює комунікацію держави з суспільством, створюючи сприятливий ґрунт для маніпуляцій і поширення фейкової інформації. У таких умовах навіть стратегічно важливі інформаційні ініціативи можуть не знаходити відгуку серед населення або ж викликати спротив. Водночас, значна частина громадян висловлює довіру до волонтерських організацій (88%) та Збройних сил України (96%), що свідчить про те, що в умовах слабкості державних комунікацій саме громадянське суспільство та військові структури відіграють ключову роль у

формуванні довіри та мобілізації суспільства. Проте відсутність ефективної координації між державними органами та громадськими ініціативами може знижувати ефективність інформаційної політики, що критично важливо в умовах сучасних гібридних загроз. На рис. 3.6 наведено результати соціологічного дослідження Київського міжнародного інституту соціології щодо рівня довіри до основних органів державної влади, Збройних сил України, Служби безпеки України та Національної поліції у грудні 2024 року порівняно з попередніми роками.

Аналіз представлених даних на рис. 3.6 свідчить про значні коливання рівня довіри громадян до органів державної влади, що безпосередньо впливає на ефективність інформаційної політики. Спостерігається суттєве зниження довіри до президента, уряду та Верховної Ради у 2024 році порівняно з попередніми роками, що може свідчити про зростання суспільного розчарування та невдоволення політичними процесами. Водночас високий рівень довіри до ЗСУ та збереження порівняно стабільного рівня довіри до СБУ підкреслює ключову роль силових структур у забезпеченні національної безпеки. Зниження довіри до Національної поліції може вказувати на проблеми у сфері правопорядку та необхідність покращення комунікації між громадянами та правоохоронними органами. Загалом, результати дослідження демонструють, що довіра до державних інституцій є нестабільною та потребує комплексних заходів для її відновлення, зокрема через ефективну та прозору інформаційну політику.

Щоб розвинути перспективи інформаційної політики в Україні, важливо звернути увагу на кілька ключових напрямів. Один із них – це підвищення співпраці з міжнародними партнерами, зокрема з країнами НАТО та ЄС. Таке партнерство дасть змогу не лише зміцнити інформаційну безпеку країни, а й взяти участь у спільних проектах, що стосуються кібербезпеки та протидії дезінформації. Спільні навчання та обмін досвідом між експертами з різних країн дозволять Україні значно поліпшити власні механізми реагування на інформаційні загрози.

Також важливим є розвиток законодавчої та нормативної бази, яка дозволить чітко регулювати інформаційні процеси та забезпечить захист прав громадян у цифровому середовищі. Оновлення законів, зокрема щодо боротьби з фейковими новинами, буде критичним кроком у боротьбі з маніпуляціями в медіа та соціальних мережах. Законодавство має бути адаптоване до швидко змінюваного інформаційного середовища.

Не менш важливим є створення ефективних інструментів для моніторингу інформаційного простору. Використання новітніх технологій, зокрема штучного інтелекту для автоматичного виявлення фейків і маніпуляцій, допоможе у реальному часі реагувати на загрози. Така технологічна база сприятиме розвитку ефективних стратегій протистояння інформаційним атакам. Прозорість інформаційних кампаній також стане важливим кроком на шляху до зміцнення довіри громадян до державних інститутів. Створення відкритих платформ, де громадськість зможе стежити за інформаційною діяльністю держави, допоможе знизити рівень недовіри і підтримати інформованість населення. Громадянське суспільство, волонтерські ініціативи та незалежні медіа можуть стати потужними союзниками в цій боротьбі, оскільки вони можуть виступати як альтернативні канали комунікації, зменшуючи вплив маніпуляцій і пропаганди. І, звісно, не можна обійти питання створення єдиної національної стратегії інформаційної безпеки. Тільки за умови координації зусиль усіх рівнів влади, громадських організацій та бізнесу можна досягти ефективної протидії інформаційним загрозам – ця стратегія має бути не тільки про захист від зовнішніх загроз, але й про боротьбу з внутрішніми маніпуляціями та політичними спекуляціями. Всі ці аспекти в сукупності можуть допомогти Україні ефективно розвивати свою інформаційну політику в умовах сучасних викликів.

Зокрема, недосконалість інформаційної політики та стратегії управління інформаційними ресурсами є одним із факторів, що ускладнюють боротьбу з інформаційними загрозами. У межах цієї теми важливим є формування ефективної

системи стратегічних комунікацій. Інформаційна політика має стати ключовим інструментом не тільки для захисту від агресії, але й для формування довіри серед громадян до державних інституцій та міжнародних партнерів. Стратегічні комунікації допоможуть в інтеграції різних рівнів влади та громадянського суспільства в процес прийняття рішень та протидії дезінформації. Також важливою складовою є підвищення рівня медіа грамотності населення, оскільки тільки освічене суспільство здатне протистояти маніпуляціям і пропаганді. Як зазначає портал «SPRAVDI» (SPRAVDI), основна проблема полягає в тому, що громадяни часто не мають достатніх навичок критичного мислення, що робить їх вразливими до фейків. Інформаційна політика має передбачати освітні ініціативи, спрямовані на розвиток критичного мислення, яке стане запорукою ефективного реагування на інформаційні атаки. Крім того, для ефективної реалізації інформаційної політики важливо оновлення законодавчої бази, що дозволить створити умови для більш ефективної взаємодії між державними органами та громадянським суспільством. Встановлення чітких норм та правил управління інформаційним середовищем сприятиме забезпеченню стабільності й безпеки в умовах гібридних загроз.

Таким чином, забезпечення інформаційної безпеки України в нинішніх умовах є надзвичайно важливим завданням, але для цього необхідно не лише покращити технічні засоби захисту, але й розвивати інформаційну політику, створюючи правову базу для протидії інформаційним атакам, пропаганді та кіберзагрозам. Важливим аспектом є розробка стратегій для протидії дезінформації, підвищення рівня медіа грамотності серед населення, модернізація законодавчої бази та створення умов для більш ефективної співпраці з міжнародними партнерами в сфері кібербезпеки та стратегічних комунікацій. Тільки за умови скоординованих дій держави, громадянського суспільства та міжнародних партнерів можна забезпечити стійкість та захист інформаційного простору України, що є фундаментом для збереження національної безпеки та суверенітету в умовах сучасних викликів.

ВИСНОВКИ

У результаті проведеного дослідження встановлено, що інформаційна політика України в умовах російсько-української війни набула особливого стратегічного значення, перетворившись із другорядного напрямку державної політики на один із ключових інструментів забезпечення національної безпеки, соціальної єдності та міжнародної підтримки. З урахуванням характеру сучасної гібридної війни, в якій інформаційний компонент має не менше значення, ніж збройний, інформаційна політика стала засобом не лише оборони, але й активної наступальної комунікації. Водночас інформаційна політика поступово трансформується в системну державну стратегію, що охоплює як оборонні заходи, так і довгострокове формування комунікаційної культури, стійкої до зовнішніх впливів, що означає перехід від ситуативного реагування до прогнозування, планування і стратегічного управління наративами.

По-перше, у межах першого розділу було розкрито сутність поняття «інформаційна політика», її основні функції, принципи та інструменти реалізації. У сучасному інформаційному суспільстві вона виконує не лише роль регулятора інформаційного простору, а й механізму формування громадської думки, легітимізації влади та просування зовнішньополітичного курсу держави. Особливої актуальності інформаційна політика набуває в період воєнного конфлікту, коли країна перебуває під інформаційним тиском як ззовні, так і зсередини. Дослідження довело, що ефективна інформаційна політика повинна бути міжгалузєвою, охоплювати державні й недержавні комунікаційні канали, а також базуватися на принципах відкритості, достовірності та стратегічної цілеспрямованості. Важливою умовою її ефективності є також залучення громадянського суспільства, експертного середовища, незалежних медіа та освітніх установ до спільного вироблення комунікаційних рішень, що формують довіру до держави в умовах війни.

По-друге, у другому розділі було здійснено аналіз ключових інформаційних загроз для України в умовах війни, зокрема інструментів дезінформації, кібератак, інформаційних «вкидів» та психологічних операцій, які активно використовує російська федерація. З'ясовано, що ці загрози мають системний характер і спрямовані на дискредитацію українських державних інституцій, деморалізацію населення, послаблення бойового духу військових, а також розкол у міжнародній коаліції на підтримку України. У відповідь держава розробила цілу низку стратегічних документів і практичних механізмів, серед яких – Доктрина інформаційної безпеки України, створення Центру протидії дезінформації, запуск інформаційної платформи «Єдиний марафон» та інші ініціативи. Водночас виявлено низку викликів: недостатній рівень координації між органами влади, обмеженість ресурсів, потреба в підвищенні цифрової та медіа-грамотності населення. Разом з тим, актуальною залишається потреба у впровадженні ефективного механізму моніторингу результативності цих заходів, а також у забезпеченні незалежної зовнішньої оцінки державної інформаційної політики.

По-третє, у третьому розділі було охарактеризовано конкретні напрями реалізації інформаційної політики України в умовах повномасштабного вторгнення. Зокрема, визначено, що держава перейшла від переважно оборонної позиції до активної інформаційної протидії: організовано інтенсивну міжнародну комунікацію через МЗС, започатковано проєкти англомовного мовлення («FreeДОМ», «The Gaze»), створено офіційні Telegram-канали для поширення перевіреної інформації та спростування фейків. Окрему роль відіграє стратегічна комунікація Президента України та Офісу Президента, які стали джерелами авторитетної інформації як всередині країни, так і для зовнішньої аудиторії. Ефективна персоніфікація лідерства в інформаційному просторі дозволила Україні сформувати виразний міжнародний образ – країни, що чинить опір тиранії, захищаючи не лише власну незалежність, а й європейські цінності. Цей фактор сприяв посиленню підтримки України з боку іноземної аудиторії та міжнародних

медіа.

Одним із ключових досягнень України у сфері інформаційної політики є підтримка високого рівня довіри до офіційних джерел у перші місяці повномасштабного вторгнення, що дозволило уникнути паніки, посприяти мобілізації громадян і сформувати широку міжнародну коаліцію. Водночас упродовж 2023-2024 років спостерігається тенденція до зниження довіри до державних комунікаційних каналів, зокрема до телемарафону «Єдині новини», що вимагає оновлення форм і методів інформаційної політики, з урахуванням зміни очікувань громадян, зростання впливу соціальних мереж і посилення інформаційної конкуренції, що створює потребу в сегментації комунікацій для різних груп населення – за віком, рівнем цифрової грамотності, регіоном проживання, соціальним статусом. Застарілі формати комунікацій не здатні втримати увагу аудиторії в умовах надлишку контенту й розмитості джерел.

Інформаційна політика України також стикається з внутрішніми бар'єрами: кадровим голодом, недостатнім фінансуванням, нерозвиненістю стратегічних комунікацій на рівні місцевого самоврядування, а також відсутністю сталої координації між органами державної влади, медіа та громадським сектором. Особливої уваги потребує розвиток цифрових навичок і критичного мислення серед населення. Як показують дані соціологічних опитувань, зниження цифрової компетентності з 64% у 2022 році до 55% у 2023 році свідчить про необхідність інвестування в медіа-освіту. Особливо це стосується молоді, яка є найбільш вразливою до впливу соціальних мереж, де значна частина контенту поширюється без перевірки фактів або має маніпулятивний характер. Саме освітні ініціативи у сфері медіа-грамотності можуть стати запобіжником від масштабних інформаційних криз у майбутньому.

Таким чином, основні висновки дослідження полягають у наступному:

- інформаційна політика України є ключовим елементом національної безпеки в умовах гібридної війни, що охоплює як внутрішню комунікацію з

громадянами, так і зовнішню дипломатію на міжнародній арені;

- інформаційна агресія з боку рф має багатовекторний характер, включаючи фейки, психологічні операції, кібератаки та пропаганду, на які Україна відповідає через інтеграцію зусиль державних і громадських інституцій;

- Україна сформувала базові інституції та інструменти протидії дезінформації, однак їх ефективність залежить від подальшого розвитку нормативно-правової бази, координації та інституційної спроможності;

- внутрішня довіра до державних інформаційних каналів є непостійною, що вимагає постійного вдосконалення комунікаційних стратегій та адаптації до нових форматів подачі інформації;

- міжнародна інформаційна політика України є прикладом успішної комунікації в умовах війни, що сприяє мобілізації підтримки союзників, проте потребує подальшого зміцнення шляхом налагодження співпраці зі світовими медіа та платформами;

- довгостроковий виклик полягає в тому, щоб перетворити інформаційну політику з реактивного інструменту на стратегічну галузь, яка формує бачення майбутнього України як демократичної, відкритої та інноваційної держави.

У підсумку, інформаційна політика України в умовах війни є не просто сферою державного управління, а полем щоденного бою за свідомість, підтримку, стабільність і майбутнє. Її ефективність визначає здатність держави протистояти агресії не лише зброєю, а й словом, правдою, наративом. Подальше вдосконалення інформаційної політики – це інвестиція в безпечне майбутнє країни.

СПИСОК ВИКОРИСТАНИХ ДЖЕРЕЛ

1. Іванченко Ю.М. Сутність, головні напрями та способи державної інформаційної політики в Україні. *Державне управління: теорія та практика*. 2005. № 2. URL: <http://www.academy.gov.ua/ej/ej2/>.
2. Інститут масової інформації. Західні наративи. Що з іноземних медіа потрапляє в інфопростір України. URL: <https://imi.org.ua/monitorings/zahidni-narytyvy-shho-z-inozemnyh-media-potraplyaye-v-infoprostir-ukrayiny-i61744>
3. Інститут масової інформації. 620 злочинів скоїла рф проти медіа та журналістів за два з половиною роки повномасштабної війни. URL: <https://imi.org.ua/monitorings/617-zlochyniv-vchynyla-rf-proty-media-ta-zhurnalistiv-za-dva-z-polovynoyu-roky-povnomasshtabnoyi-i63178>
4. Інформаційна безпека. Підручник В. В. Остроухов, М. М. Присяжнюк, О. І. Фармагей, М. М. Чеховська та ін.; під ред. В. В. Остроухова. К.: Видавництво Ліра-К, 2021. 412 с. 15.
5. Інформаційні атаки в соціальних мережах: дослідження впливу російської дезінформації через рекламу в Facebook. URL: <https://cedem.org.ua/wp-content/uploads/2024/05/informacijni-ataky-v-soczialnyh-merezhah.-doslidzhennya-vplyvu-rosijskoyi-dezinformaciyi-cherez-reklamu-v-facebook.pdf>
6. Київський міжнародний інститут соціології. Динаміка довіри соціальним інституціям у 2021-2024 роках. URL: <https://www.kiis.com.ua/?lang=ukr&cat=reports&id=1467&page=1>
7. Київський міжнародний інститут соціології. Довіра телемарафону «Єдині новини». URL: <https://kiis.com.ua/?lang=ukr&cat=reports&id=1369>
8. Кіберзагрози в сучасному політичному просторі: метод. вказівки для підготовки до практичних занять та самостійної роботи здобувачів вищої освіти другого (магістерського) рівня галузі знань – 05 «Соціальні та поведінкові науки», спеціальності – 052 «Політологія» / Ю. В. Завгородня; Нац. ун-т «Одеська юрид. академія». Одеса, 2024. 30 с. URL: <https://hdl.handle.net/11300/28400>

9. Лабенко О. В., Шакун Н. В., Заїка Т. П. Критичне мислення та медіаграмотність у цифрову епоху: виклики та можливості для української освіти. *Перспективи та інновації науки (Серія “Педагогіка”, Серія “Психологія”, Серія “Медицина”)*. 2023. Вип. № 12 (30). с. 331-345.

10. Левченко О. В. Система забезпечення інформаційної безпеки держави у війсьній сфері: основи побудови та функціонування: монографія/О. В. Левченко. - Житомир: Видавець ПП “Євро-Волинь”, 2021. 172 с.

11. Мирошніченко А. І. Інформаційна політика в умовах воєнного стану. *Вчені записки ТНУ імені В. І. Вернадського. Серія: Публічне управління та управління*. 2023. Т. 34 (73). № 4. с. 41-45.

12. Міненко Є. С. Розвиток інститутів інформаційної безпеки сучасної України як чинник суспільно-політичної стабільності: дис. ... канд. філос. наук: 052. Київ, 2024. 257 с.

13. Національна рада України з питань телебачення і радіомовлення. Для працівників Національної ради освіти платформа StopFake провела тренінг із медіа грамотності. URL: <https://webportal.nrada.gov.ua/dlya-pratsivnykiv-natsionalnoyi-rady-osvitnya-platforma-stopfake-provela-trening-iz-mediagramotnosti/>

14. Оперативний центр реагування на кіберінциденти державного центру кіберзахисту державної служби спеціального зв'язку та захисту інформації України. Звіт про роботу системи виявлення вразливостей і реагування на кіберінциденти та кібератаки. URL: <https://scpc.gov.ua/api/files/9c21855d-74da-45d1-90f9-5d4f6795996a>

15. ОПОРА. Як працює російська пропаганда в телеграмі на тимчасово окупованих територіях. URL: https://www.oporaua.org/polit_ad/iak-pratsiuie-rosiiska-propaganda-v-telegrami-na-timchasovo-okupovanikh-teritoriiakh-24743

16. Питання Міністерства цифрової трансформації : постанова Кабінету Міністрів України від 18.09.2019 р. № 856. URL: <https://zakon.rada.gov.ua/laws/show/856-2019-%D0%BF#Text>

17. Портал SPRAVDI. Медіаграмотність як ключ до боротьби з російською пропагандою: виклики та рішення для України. URL: <https://spravdi.gov.ua/mediagramotnist-yak-klyuch-do-borotby-z-rosijskoju-propagandoyu-vyklyky-ta-rishennya-dlya-ukrayiny/>

18. Про Державну службу спеціального зв'язку та захисту інформації України: Закон України від 23.02.2006 р. № 3475-IV. URL: <https://zakon.rada.gov.ua/laws/show/3475-15#Text>

19. Про інформацію: Закон України від 02.10.1992 № 2657-XII. URL: <https://zakon.rada.gov.ua/laws/show/2657-12#Text>

20. Почепцов Г.Г. Сучасні інформаційні війни. Київ : Києво-Могилянська академія, 2015. 497 с.

21. Пунда О. О., Добрянська О. Д., Новицька Н. Б. Принципи інформаційної політики в умовах війни та їх нормативно-правове закріплення. *Екологічне право*. 2022. № 1–2. с. 60–65.

22. Резнікова О. О. Національна стійкість в умовах мінливого безпекового середовища: монографія. Київ: НІСД, 2022. 532 с.

23. Ржевська Н. Сучасна інформаційна політика: досвід США для України. *Політичні дослідження/Political Studies*, 2024. Вип. № 1 (7).

24. Савон К. В. Міжнародний імідж України: сучасний стан та перспективи розвитку/К. В. Савон // Актуальні проблеми політики: зб. наук. пр./редкол.: С. В. Ківалов (голов. редкол.), Л. І. Кормич (голов. ред.), І. М. Милосердна (відп. ред.) [та ін.]; НУ «ОЮА», Південноукр. центр гендер. проблем. Одеса: Фенікс. 2019. Вип. № 64. с. 180-193.

25. Сайт міста Слов'янська. Як в Україні на законодавчому рівні борються з фейками та дезінформацією. URL: <https://www.6262.com.ua/news/3871436/ak-v-ukraini-na-zakonodavcomu-rivni-borutsa-z-fejkami-ta-dezinformacieu>

26. Свідерська О. І. Цифрова пропаганда та ризики інформаційної безпеки у контексті російсько-української війни. *Політикус*. 2022. Вип. № 2. с. 60-65.

27. Соснін О.В. Державна інформаційна політика і національні інформаційні ресурси. URL: http://old.niss.gov.ua/book/D_p2.html.

28. Суспільне новини. Новинам із яких джерел українці найбільше довіряють – дослідження ОПОРИ. URL: <https://suspilne.media/792121-novinam-iz-akih-dzerel-ukrainci-najbilshe-doviraut-doslidzenna-opori/>

29. Терещенко В. В. Особливості державної інформаційної політики в умовах війни. *Юридичний науковий електронний журнал*. 2023. № 2. с. 391–395.

30. Укрінформ. Комісія ООН представила новий звіт про воєнні злочини військ РФ в Україні. URL: <https://www.ukrinform.ua/rubric-ato/3840125-komisia-oon-predstavila-novij-zvit-pro-voenni-zlocini-vijsk-rf-v-ukraini.html>

31. Укрінформ. СБУ попереджає: Ворожі фейки з'являються щодня. URL: <https://www.ukrinform.ua/rubric-ato/3420585-sbu-vorozi-fejki-zavlautsa-sodna.html>

32. Укрінформ. В Україні створили міні серіал про протидію дезінформації. URL: <https://www.ukrinform.ua/rubric-society/3909981-v-ukraini-stvorili-miniserial-pro-protidiu-dezinformacii.html>

33. Громадянське суспільство vs. корупція в Україні. Київ: ДУХ І ЛІТЕРА, 2019. 240 с.

34. Департамент кіберполіції України. Про Департамент. 2024. URL: <https://cyberpolice.gov.ua/contacts/>

35. Державна служба спеціального зв'язку та захисту інформації України. CERT-UA минулого року опрацювала 4315 кіберінцидентів. URL: <https://cip.gov.ua/ua/news/cert-ua-minulogo-roku-opracyovala-4315-kiberincidentiv>

36. Детектор медіа. Аналіз стратегії інформаційної безпеки в порівнянні з чинною доктриною інформаційної безпеки. URL: <https://detector.media/infospace/article/187663/2021-05-03-analiz-strategii-informatsiynoi-bezpeky-v-porivnyanni-z-chynnoyu-doktrynoyu-informatsiynoi-bezpeky/>

37. Детектор медіа. Російська пропаганда та медіаграмотність: як Україна

протистоїть дезінформації. URL: <https://go.detector.media/rosijska-propaganda-ta-mediagramotnist-yak-ukrayina-protistoyit-dezinformatsiyi/>

38. Детектор медіа. Індекс медіа грамотності українців 2020–2023 (четверта хвиля). URL: <https://detector.media/infospace/article/225738/2024-04-22-indeks-mediagramotnosti-ukraintsiv-20202023-chetverta-khvylya/>

39. Детектор-медіа. 25 мільйонів кібератак щомісяця. Як росія намагається зашкодити Україні в цифровому просторі. URL: <https://detector.media/infospace/article/204308/2022-10-29-25-milyoniv-kiberatak-shchomisyatsya-yak-rosiya-namagaietsya-zashkodyty-ukraini-v-tsyfrovomu-prostori/>

40. Детектор-медіа. «Україна стала британською колонією» та інші фейки. Огляд російської дезінформації за 13-19 січня 2025 року. URL: <https://detector.media/monitorynh-internetu/article/237362/2025-01-22-ukraina-stala-brytanskoyu-koloniieyu-ta-inshi-feyky-oglyad-rosiyskoi-dezinformatsii-za-1319-sichnya-2025-roku/>

41. Деякі питання діяльності Міністерства культури та інформаційної політики: постанова Кабінету Міністрів України від 16.10.2019 р. № 885. URL: <https://zakon.rada.gov.ua/laws/show/885-2019-%D0%BF#Text14>.

42. Міні серіал протидії пропаганді. URL: <https://youtu.be/Ml5AHZrWGDY>

43. Рубрика. Google та Jigsaw запустили в Україні ініціативу з медіа грамотності для підвищення стійкості до дезінформації. URL: <https://rubryka.com/2024/09/11/google-ta-jigsaw/>

44. Dozorro TI Ukraine: Фінансування телемарафонів у 2024 році майже не змінилося порівняно з попереднім роком. URL: <https://vz.ua/news/83484-dozorro-ti-ukraine-finansuvannya-telemarafoniv-u-2024-rotsi-mayzhe-ne-zminilosya-porivnyano-z-poperednim-rokom>

45. Forbes Ukraine. Збитки українців від кіберзлочинності торік зросли до 1 млрд грн – дослідження ЄМА [The losses of Ukrainians from cybercrime increased to UAH 1 billion last year - EMA research]. 2023.

URL:<https://forbes.ua/news/zbitki-ukraintsiv-vid-kiberzlochinnosti-torik-zroslido-1-mlrd-grn-doslidzhennya-ema-21022023-11884>

46. Interfax-Україна. Україна з 14 січня 2022 року залишається на першому місці у світі за кількістю кібератак проти неї - заступник голови Держспецзв'язку.

URL: <https://interfax.com.ua/news/interview/911979.html>

47. National Security and Defense Council of Ukraine. Стратегія кібербезпеки України (2021 – 2025 роки). URL:

https://www.rnbo.gov.ua/files/2021/STRATEGIYA%20KYBERBEZPEKI/proekt%20strategii_kyberbezpeki_Ukr.pdf.

48. Texty.org.ua. Рівень маніпулятивності українських телеграм-каналів. URL: <https://texty.org.ua/projects/113607/karusel-emocij-riven-manipulyatyvnosti-movy-ukrayinskyh-telehram-kanaliv/>

49. Transparency International Ukraine. Україна в Індексі сприйняття корупції – 2024. URL: <https://cpi.ti-ukraine.org/>

50. Ukraïner. Види міжнародних злочинів і які вже вчинила РФ. URL: <https://www.ukraïner.net/mizhnarodni-zlochyny/>

51. Ukraïner. Як ворожі ІПСО дискредитують Україну. URL: <https://www.ukraïner.net/ipsa/>

52. Hawdon J. Cybercrime: Victimization, perpetration, and techniques. American Journal of Criminal Justice. 2021. № 46 (6). p. 837-842.

53. Nye, J. S. (2004). Soft Power. The Means to Success in World Politics. New York: Public Affairs, 328 p. (in English).

ДОДАТКИ

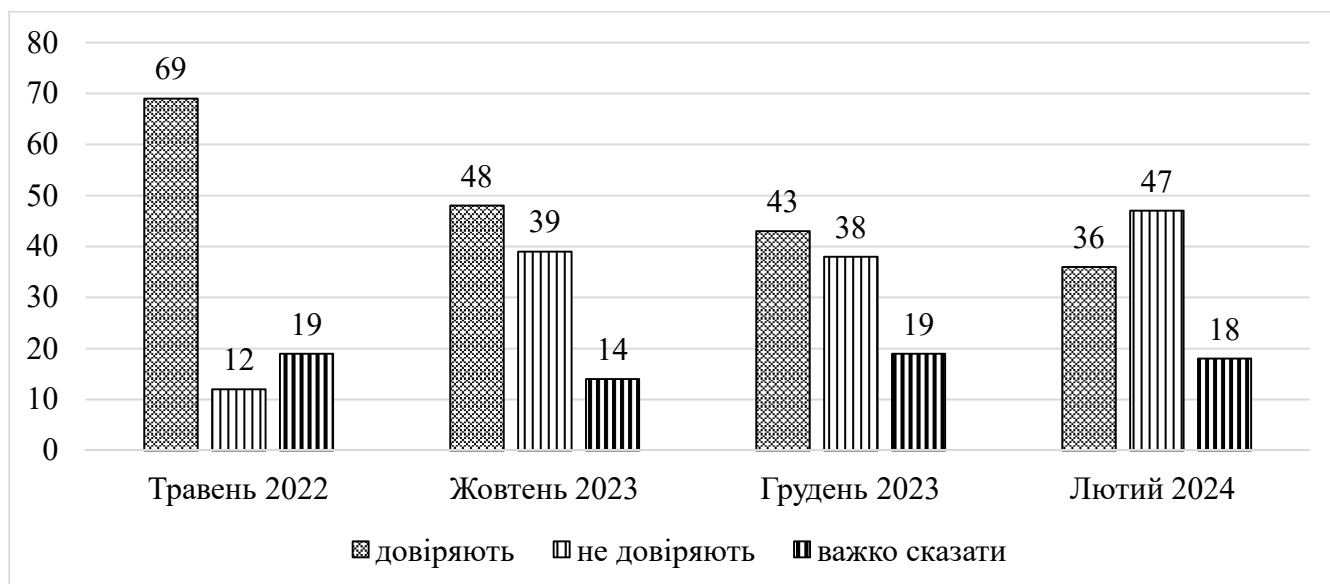


Рис. 1.1 Довіра населення до телемарафону «Єдині новини», %

Джерело: побудовано за даними (Київський міжнародний інститут соц., 27)



Рис. 1.2 Порівняння значень субіндексів медіа грамотності за період 2020-2023 рр., % Джерело: побудовано за даними (Детектор медіа, 56)



Рис. 1.3 Найбільші отримувачі державного фінансування телемарафонів у 2024 році

Джерело: (Dozorro, 2024)

Таблиця 2.1

Ключові теми, які протягом березня-листопада 2023 року відпрацьовували автори

повідомлень

Тема	Характеристика повідомлень
Фронт	«ситуація в зоні бойових дій, битва за Бахмут, наступ ЗСУ на півдні України»
Мобілізація	«несправедливість мобілізації, спекуляції на пов'язаних з нею страхах»
Захід	«недовіра західних партнерів до української влади, наратив про зовнішнє управління, втручання західних країн у внутрішньополітичні справи та військове планування, затримка військової допомоги, зацікавленість Заходу у війні, наявність територіальних претензій у сусідів до України, погане ставлення іноземців до українців»
Зброя	«погана якість західних озброєнь, недостатня кількість зброї на фронті, неспроможність України виготовляти власну зброю»
Корупція	«тотальна корумпованість української влади, розкрадання західної допомоги»
Влада	«некомпетентність української влади, персональні атаки на президента України та його сім'ю, інших представників політичного керівництва, звинувачення у згортанні демократії, конфлікти всередині влади»
Енергетика	«відключення електроенергії та опалення»
Демографія	«людські втрати України через війну, небажання біженців повертатися з-за кордону»
Деморалізація	«спекуляції на регіональних та мовних відмінностях, дискредитація західних цінностей, втрата ціннісних орієнтирів в українському суспільстві, низький бойовий дух ЗСУ, зростання рівня злочинності»
Бідність	«низький рівень матеріального достатку українців, зокрема, соціально незахищених верств населення»

Виплати	«фейкові повідомлення про грошову допомогу українцям від уряду, іноземних партнерів або міжнародних організацій»
Турбота про військових	«байдужість держави до військовослужбовців та їхніх сімей, відсутність належної підтримки поранених»

Джерело: побудовано за даними (Інформаційні атаки)

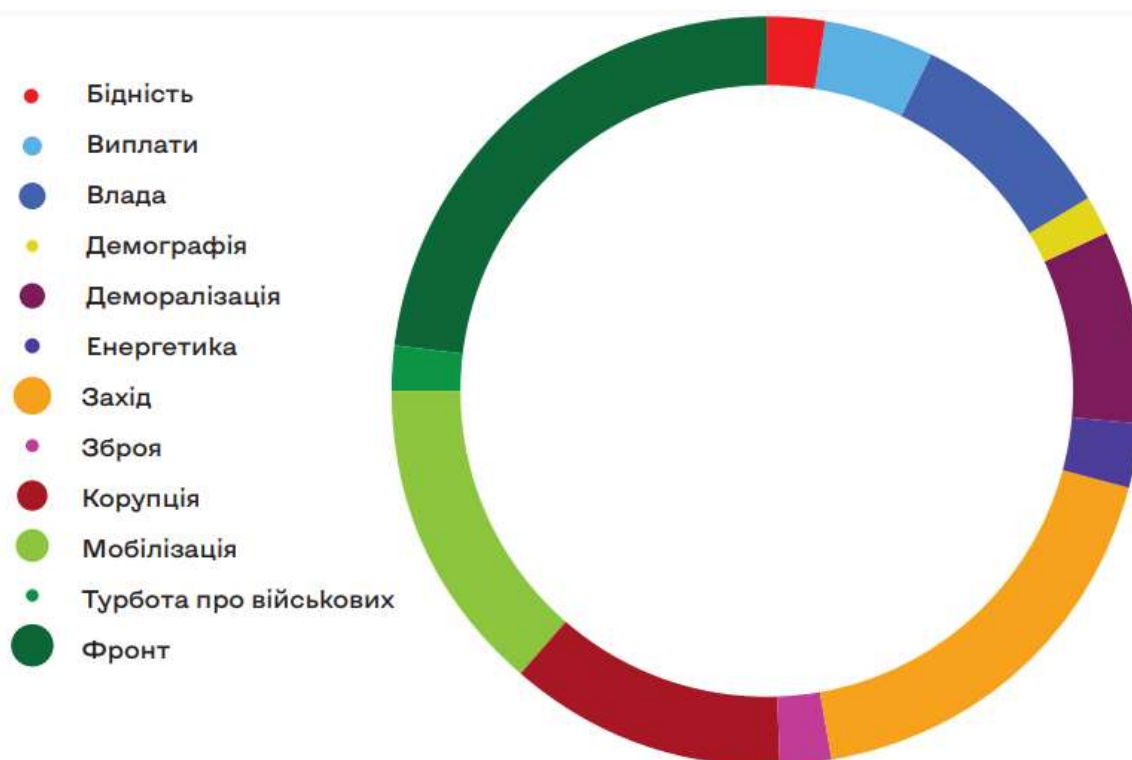


Рис. 2.1 Розподіл публікацій за основним наративом

Джерело: (Інформаційні атаки)



Рис. 2.2 Злочини росії проти медіа та журналістів в Україні, з початку повномасштабного вторгнення станом на серпень 2024 року

Джерело: побудовано за даними (Інститут масової інформації)

Таблиця 2.2

Порівняння рівня довіри населення України до різних джерел протягом 2023-2024

рр., %

Джерело інформації	2023 рік	2024 рік	Зміна з 2023 року по 2024 рік
Соцмережі	60	47,3	- 12,7
Інтернет (без соцмереж)	48,8	43	- 5,8
Телебачення	61,1	34,1	- 27
Радіо	41	24,2	- 16,8
Друковані ЗМІ	30,3	18	- 12,3
Жодне джерело	7,7	15,2	+ 7,5

Джерело: побудовано за даними (Суспільне новини, ОПОРИ)



Рис. 2.3 Кількісні показники зібраних та опрацьованих даних у 2023 році
Джерело: (Оперативний центр)

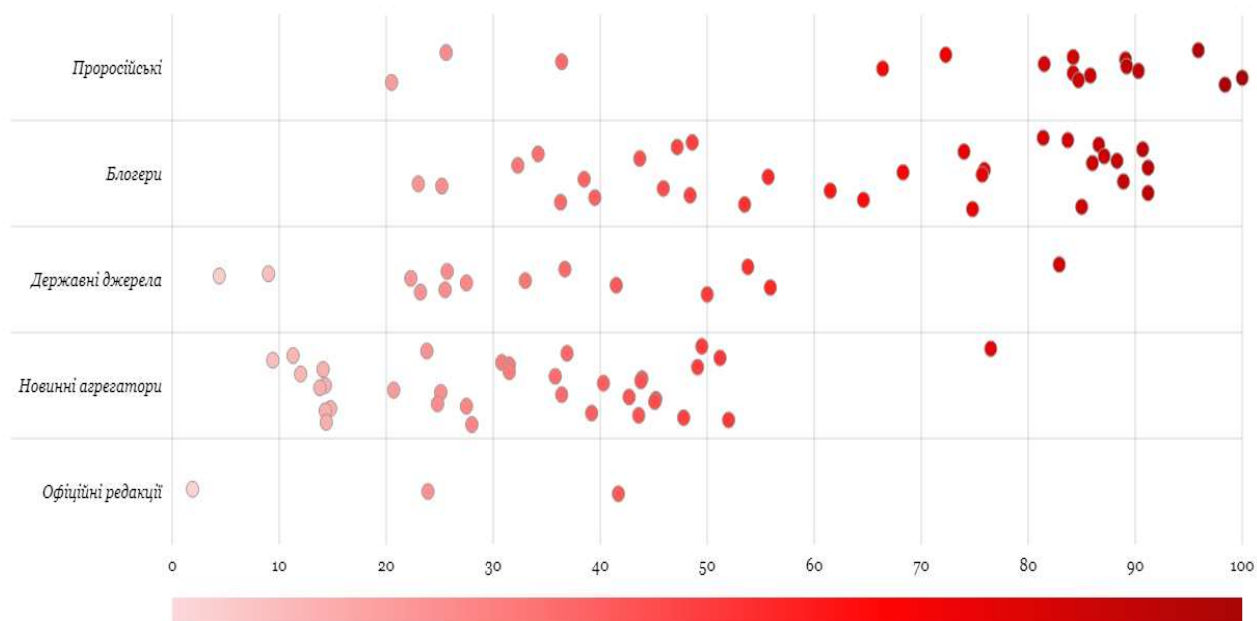


Рис. 3.1 Рівень маніпулятивності у впливових телеграм-каналах станом на жовтень 2024 року, %

Джерело: (Texty.org.ua)

111
1



Кількість дописів

Нейтральні дописи

Навантажена/емоційна мова

Блискучі узагальнення та ейфорія

Апеляція до страху та сумнівів

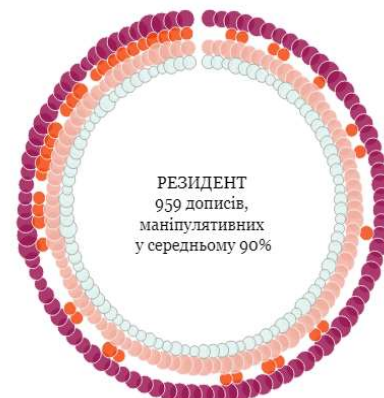
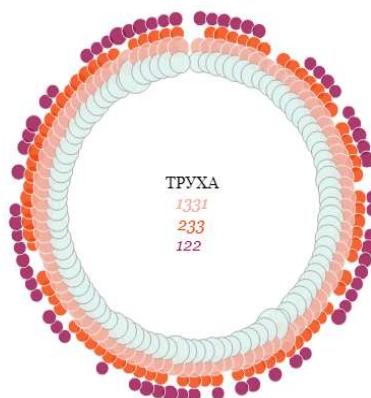
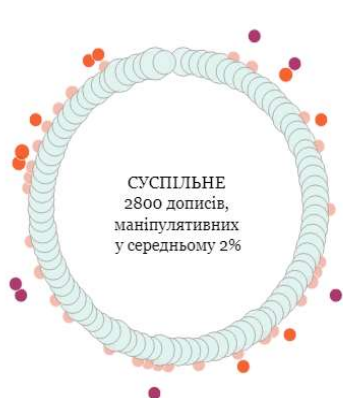


Рис. 3.2 Порівняння рівня маніпулятивності у телеграм каналах «Суспільного», «Трухи» і «Резидента» станом на жовтень 2024 року

Джерело: (Texty.org.ua)



Рис. 3.3 «Вкиди» рф щодо війни в Україні, що були зафіксовані протягом 13-19 січня 2025 року Джерело: (Детектор медіа, 2025)



Рис. 3.4 «Вкиди» рф щодо війни в Україні, що були зафіксовані від початку повномасштабного вторгнення станом на 22 січня 2025 року

Джерело: (Детектор медіа, 2025)



Рис. 3.5 Індекс сприйняття корупції в Україні і країнах-кандидатках в ЄС у 2024 році

Джерело: (Transparency International Ukraine, 2024)

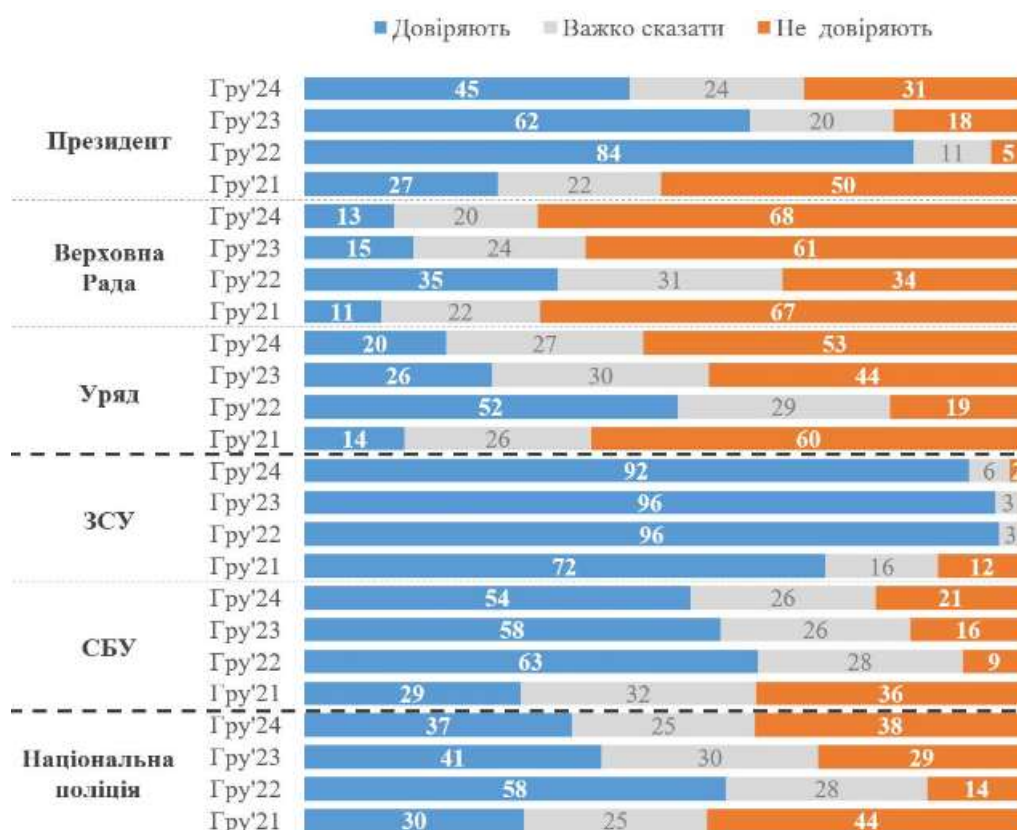


Рис. 3.6 Довіра населення України до основних органів державної влади, ЗСУ, СБУ та Національної поліції у грудні 2021-2024 року, %

Джерело: (Київський міжнародний інститут соціології, 2021-2024)

АНОТАЦІЯ

Читова В. О. Інформаційна політика України в умовах російсько-української війни (бакалаврська робота). Харків: ХНУ імені В. Н. Каразіна, 2025. 64 с. (рукопис)

Кваліфікаційна робота бакалавра присвячена дослідженню інформаційної політики України в умовах російсько-української війни. У роботі проаналізовано основні напрями інформаційної політики держави з особливим акцентом на період повномасштабного вторгнення у 2022-2024 роках. Дослідження охоплює питання протидії дезінформації, кібербезпеки, регулювання медіа та формування національного інформаційного нарративу. На прикладі діяльності державних органів, громадських ініціатив і медіа-аналізу виявлено основні виклики інформаційній безпеці України та оцінено ефективність заходів, спрямованих на посилення інформаційного суверенітету. Особливу увагу приділено впливу інформаційної політики на суспільну стійкість, міжнародну підтримку та формування іміджу України за кордоном. Висновки роботи підкреслюють ключову роль стратегічної комунікації у веденні сучасної війни та необхідність подальшого розвитку комплексної інформаційної політики.

Ключові слова: інформаційна політика, дезінформація, стратегічна комунікація, медіа, російсько-українська війна, кібербезпека.

ANNOTATION

Chytova V. O. Ukraine's information policy in the context of the russian-ukrainian war (Bachelor's Thesis). Kharkiv: V. N. Karazin Kharkiv National University, 2025. 64 p. (manuscript)

The bachelor's qualification thesis is devoted to the study of Ukraine's information policy under the conditions of the russian-ukrainian war. The paper analyzes the main directions of the state's information policy, with a particular focus on the period of the full-scale invasion from 2022 to 2024. The study covers issues of countering disinformation, cybersecurity, media regulation, and the formation of a national information narrative. Based on the activities of state institutions, civil initiatives, and media analysis, the main challenges to Ukraine's information security are identified, and the effectiveness of measures aimed at strengthening informational sovereignty is assessed. Special attention is paid to the impact of information policy on societal resilience, international support, and the formation of Ukraine's image abroad. The findings highlight the crucial role of strategic communication in modern warfare and the need for further development of a comprehensive information policy.

Keywords: information policy, disinformation, strategic communication, media, russian-ukrainian war, cybersecurity.

Відгук наукового керівника
на кваліфікаційну роботу бакалавра
здобувачки вищої освіти 4-го курсу
групи ОП-42 денної форми навчання спеціальності 052 «Політологія»
освітньо-професійної програми «Політичні технології та аналіз політики»
філософського факультету
Харківського національного університету імені В. Н. Каразіна
Читової Віолетти на тему:
«Інформаційна політика України в умовах російсько-української війни»

Кваліфікаційна робота Читової Віолетти Олександрівни присвячена надзвичайно актуальній темі, що перебуває у центрі як наукових, так і суспільно-політичних дискусій – формуванню та реалізації інформаційної політики України в умовах російсько-української війни. Актуальність обраної теми обумовлена зростанням значення інформаційної безпеки в умовах гібридних загроз, масштабних дезінформаційних кампаній, кібератак та активної боротьби за інформаційний простір не лише в межах держави, а й на міжнародному рівні.

Студентка продемонструвала глибоке розуміння предмета дослідження, виявила вміння логічно структурувати матеріал, аналізувати як теоретичні підходи, так і конкретні практичні кейси. Структура роботи є цілком логічною та відповідає вимогам до кваліфікаційних робіт: вона складається з трьох розділів, кожен з яких має чітке змістове навантаження. У першому розділі авторка розкрила поняттєво-теоретичні засади інформаційної політики, що дозволило закласти підґрунтя для подальшого аналізу. Другий розділ присвячено вивченню проблем інформаційної безпеки України та реагування на виклики, пов'язані з російською агресією. У третьому розділі досліджено конкретні аспекти протидії дезінформації, роль державних інституцій та громадянського суспільства у забезпеченні інформаційного суверенітету.

Особливої уваги заслуговує аналітичний підхід, який здобувачка застосувала під час оцінки ефективності інформаційної політики держави. Вона не лише описала актуальні механізми та інструменти, а й критично осмислила їхню результативність, виокремивши як успішні практики, так і проблемні зони. Здобувачка відповідально працювала над кваліфікаційною роботою протягом усього навчального року, своєчасно надавала проміжні результати, ініціювала обговорення проблемних моментів, була відкритою до конструктивної критики й рекомендацій. Вона продемонструвала здатність до самостійного пошуку та опрацювання значної кількості джерел – як наукових, так і публіцистичних, аналітичних, нормативних. Список використаних джерел є різноманітним, актуальним і вказує на добросовісне академічне ставлення до процесу дослідження. Мовне оформлення роботи відповідає нормам наукового стилю, текст відзначається ясністю викладу та логічністю побудови аргументації. Висновки роботи є обґрунтованими та логічно витікають із дослідженого матеріалу.

Загалом, кваліфікаційна робота Читової Віолетти Олександрівни є самостійним, збалансованим дослідженням, що поєднує теоретичну глибину з практичним спрямуванням. Вона відповідає всім вимогам до бакалаврських кваліфікаційних робіт, а її зміст свідчить про високий рівень підготовки здобувачки до подальшої наукової чи аналітичної діяльності в сфері політології. Вважаю, що дана кваліфікаційна робота заслуговує на відмінну оцінку, а її авторка – на присвоєння кваліфікації бакалавра зі спеціальності 052 «Політологія».

Науковий керівник:

Кандидат політичних наук,
Старший викладач кафедри політології
Філософського факультету
Харківського національного університету імені В.Н. Каразіна

Авксентьев Антон Александрович


(підпис)

РЕЦЕНЗІЯ

на кваліфікаційну роботу бакалавра
здобувачки вищої освіти 4-го курсу групи ОП-42 денної форми навчання
спеціальності 052 «Політологія» освітньо-професійної програми
«Політичні технології та аналіз політики» філософського факультету
Харківського національного університету імені В. Н. Каразіна
Читової Віолетти Олександрівни
«Інформаційна політика України в умовах російсько-української війни»

Кваліфікаційна робота здобувачки є змістовним і своєчасним дослідженням проблематики інформаційної політики України в умовах російсько-української війни. Обрана тема вирізняється високим ступенем актуальності, адже з початком повномасштабної агресії російської федерації у 2022 році інформаційний простір став одним із ключових полів гібридного протистояння. Робота демонструє глибоке розуміння ролі інформаційної політики у забезпеченні національної безпеки, формуванні міжнародного іміджу держави, зміцненні суспільної стійкості та збереження довіри до державних інституцій. Структура кваліфікаційної роботи є логічною та збалансованою. Вона складається з трьох розділів, які послідовно розкривають обрану тематику.

У першому розділі подано теоретичні засади інформаційної політики. Авторка детально аналізує поняття, функції та роль інформаційної політики в системі міжнародних відносин, що створює міцне методологічне підґрунтя для подальшого дослідження та засвідчує належний рівень теоретичної підготовки.

Другий розділ присвячений аналізу загроз інформаційній безпеці України та інституційним відповідям з боку держави. У підрозділі 2.1 розглянуто методи та інструменти інформаційних атак, які застосовує Росія в контексті гібридної війни. У підрозділі 2.2 проаналізовано механізми державної політики у сфері протидії цим загрозам, зокрема роль Служби

безпеки України, Центру стратегічних комунікацій, Міністерства цифрової трансформації тощо. Оцінка ефективності державних заходів є виваженою та аргументованою.

У третьому розділі основна увага приділяється інформаційній політиці України в умовах російської агресії. Авторка розглядає стратегічні напрями протидії дезінформації та пропаганді, окреслює виклики, з якими стикається держава, а також перспективи розвитку інформаційної політики. Висновки відображають системний підхід до аналізу, обґрунтовані посиланнями на нормативно-правові акти, аналітичні звіти та приклади з медіа-практики.

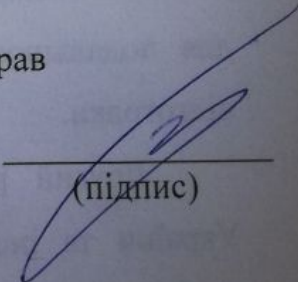
Робота вирізняється чіткою структурованістю, використанням широкого кола джерел – наукових, емпіричних, нормативно-правових. Авторка демонструє здатність до критичного мислення, аналітичної роботи та формулювання практичних рекомендацій щодо вдосконалення інформаційної політики України.

Кваліфікаційна робота Читової Віолетти Олександрівни на тему «Інформаційна політика України в умовах російсько-української війни» є цілісним і комплексним дослідженням, що відповідає вимогам до робіт бакалаврського рівня. Робота заслуговує на високу оцінку, а її авторка – на присвоєння кваліфікації бакалавра за спеціальністю 052 «Політологія».

Рецензент:

Кандидат юридичних наук,
доцент кафедри правоохоронної діяльності
Навчально-наукового інституту №5
Харківського національного університету внутрішніх справ

Говоров Валерій Станіславович


(підпис)