

**МІНІСТЕРСТВО ОСВІТИ І НАУКИ УКРАЇНИ ЧЕРНІВЕЦЬКИЙ  
НАЦІОНАЛЬНИЙ УНІВЕРСИТЕТ ІМЕНІ ЮРІЯ ФЕДЬКОВИЧА**

**Факультет історії, політології та міжнародних відносин  
кафедра міжнародних відносин та суспільних комунікацій**

**ПРОТИДІЯ ДЕЗІНФОРМАЦІЇ ТА ПРОПАГАНДИ В  
ІНФОРМАЦІЙНОМУ ПРОСТОРІ УКРАЇНИ: ПРАВОВИЙ ТА  
ІНСТИТУЦІЙНИЙ АСПЕКТИ**

**Кваліфікаційна робота**

**Рівень вищої освіти – другий (магістерський)**

***Виконав:***

студент 6 курсу, 604 групи

**Мансоур Амер**

***Керівник:***

кандидат історичних наук,

доцент Звоздецька О.Я.

**Рецензент:**

кандидат політичних наук,

доцент

*До захисту допущено*

*на засіданні кафедри*

*протокол № \_\_\_\_\_ від \_\_\_\_\_ 2024 р.*

*Зав. кафедрою \_\_\_\_\_ проф. Макар В.Ю.*

**Чернівці – 2024**

**Анотація:**

Магістерська робота присвячена аналізу правових та інституційних механізмів протидії дезінформації і пропаганді в інформаційному просторі України. У дослідженні розглянуто ключові поняття "дезінформація" та "пропаганда", їхній вплив на суспільство та засоби маніпуляції громадською думкою. Окрему увагу приділено нормативно-правовій базі та інституційним заходам України у боротьбі з деструктивними інформаційними впливами, а також порівнянню з міжнародним досвідом. Практична частина роботи пропонує рекомендації щодо вдосконалення медіаосвіти, фактчекінгу та підвищення ефективності державних інституцій у боротьбі з інформаційними загрозами.

**Ключові слова:** дезінформація, пропаганда, гібридна війна, медіаосвіта, фактчекінг, інформаційна безпека, законодавство України.

**Summary:**

The master's thesis focuses on the analysis of legal and institutional mechanisms to counter disinformation and propaganda in Ukraine's information space. The research examines the key concepts of "disinformation" and "propaganda," their societal impact, and tools for manipulating public opinion. Special attention is paid to Ukraine's regulatory framework and institutional measures against destructive information influences, alongside a comparison with international practices. The practical part of the study offers recommendations for improving media literacy, fact-checking, and enhancing the effectiveness of state institutions in combating information threats.

**Keywords:** disinformation, propaganda, hybrid warfare, media literacy, fact-checking, information security, Ukrainian legislation.

Кваліфікаційна робота містить результати власних досліджень. Використання ідей, результатів і текстів наукових досліджень інших авторів мають посилання на відповідне джерело.

\_\_\_\_\_ А. Мансоур

## ЗМІСТ

|                                                                                                                                         |    |
|-----------------------------------------------------------------------------------------------------------------------------------------|----|
| ВСТУП .....                                                                                                                             | 5  |
| РОЗДІЛ 1. ТЕОРЕТИКО-МЕТОДОЛОГІЧНІ АСПЕКТИ ДОСЛІДЖЕННЯ<br>ПРОТИДІЇ ДЕЗІНФОРМАЦІЇ ТА ПРОПАГАНДИ В ІНФОРМАЦІЙНОМУ<br>ПРОСТОРІ УКРАЇНИ..... | 8  |
| 1.1. Концептуальні та методологічні засади дослідження понять<br>«дезінформації» та «пропаганди».....                                   | 8  |
| 1.2. Стан наукової розробки проблеми.....                                                                                               | 18 |
| Висновки до 1 розділу .....                                                                                                             | 31 |
| РОЗДІЛ 2 ПРАВОВІ ТА ІНСТИТУЦІЙНІ МЕХАНІЗМИ ПРОТИДІЇ<br>ДЕЗІНФОРМАЦІЇ ТА ПРОПАГАНДИ РОСІЇ .....                                          | 33 |
| 2.1. Виклики та загрози в інформаційному просторі України в умовах війни<br>.....                                                       | 33 |
| 2.2. Нормативно-правове регулювання захисту національного<br>інформаційного простору .....                                              | 45 |
| 2.3. Діяльність державних інститутів у протидії деструктивним<br>інформаційним впливам .....                                            | 51 |
| Висновки до 2 розділу .....                                                                                                             | 61 |
| РОЗДІЛ 3 ПРАКТИЧНИЙ АНАЛІЗ ТА РЕКОМЕНДАЦІЇ ЗАХИСТУ<br>СУЧАСНОГО ІНФОРМАЦІЙНОГО ПРОСТОРУ УКРАЇНИ .....                                   | 63 |
| 3.1. Медіаосвіта як інструмент протидії дезінформації та пропаганди в<br>суспільстві.....                                               | 63 |
| 3.2. Роль, функції та завдання фактчекінгових організацій у протидії<br>дезінформації.....                                              | 69 |
| 3.3. Рекомендації щодо подальших заходів у виявленні та протидії<br>дезінформації.....                                                  | 73 |
| Висновки до 3 розділу .....                                                                                                             | 82 |
| ВИСНОВКИ .....                                                                                                                          | 84 |
| СПИСОК ВИКОРИСТАНИХ ДЖЕРЕЛ.....                                                                                                         | 88 |

## ВСТУП

**Актуальність** обраної теми є беззаперечною в умовах розвитку цифрового суспільства і зростаючого впливу медіа на формування громадського світогляду. Проблема дезінформації та інформаційних загроз є однією з ключових у сучасному світі, а особливо в умовах гібридної війни, яку веде російська федерація проти України. З 2014 року, після анексії Криму і початку бойових дій на Донбасі, росія застосовує комплексну стратегію гібридної війни, в якій інформаційний компонент має не менш важливе значення, ніж військовий. Повномасштабне вторгнення у 2022 році ще більше загострило необхідність захисту інформаційного простору України, адже інформаційна агресія стала невід'ємною складовою зусиль агресора щодо підризу національної єдності, деморалізації населення та створення хаосу у громадській думці. Інформаційні атаки росії мають багатовекторний характер. Їхні основні цілі включають створення недовіри до державних інституцій, дискредитацію збройних сил України, формування розколу в українському суспільстві та маніпуляцію міжнародною думкою. Вони поширюються через соціальні мережі, онлайн-видання, пропагандистські медіа та навіть традиційні канали комунікації. В умовах, коли інформаційний простір стає головним полем бою, боротьба з дезінформацією є критично важливою для забезпечення національної безпеки. Дезінформація, що цілеспрямовано поширюється росією, спрямована на послаблення обороноздатності країни шляхом впливу на психологічний стан громадян та маніпулювання суспільною думкою. Використовуючи гібридну тактику, ворог створює ситуації, які одночасно вражають економіку, моральний стан суспільства і міжнародний імідж України.

Правові й інституційні аспекти боротьби із дезінформацією набувають особливої значущості у контексті загострення геополітичної ситуації, де поширення фейків може впливати на стабільність країни й суспільно-політичні процеси у ній. Зростання медіаграмотності й активна участь громадян у

формуванні інформаційного простору є необхідністю для гарантування демократичного суспільства і захисту національної безпеки.

Наша магістерська робота, яка зосереджується на правових аспектах регулювання й інституційних принципах протидії дезінформації в українському інформаційному просторі, має велике значення для визначення ефективних інструментарію і стратегій. Вивчення цієї теми дозволить виробити рекомендації стосовно вдосконалення законодавства й створення інституцій, здатних відповідати на сучасні виклики і забезпечувати стабільність та стійкість українського інформаційного простору.

**Метою** даної магістерської роботи є аналіз правових та інституційних механізмів протидії дезінформації та пропаганди в інформаційному просторі України.

Досягнення поставленої мети у магістерській роботі вимагає вирішення *наступних завдань*:

- розкрити підходи визначення понять «дезінформація» та «пропаганда»;
- охарактеризувати впливу соціальних мереж на поширення неправдивої інформації;
- проаналізувати нормативно-правову базу протидії дезінформації та пропаганди;
- висвітлити діяльність державних та громадських структур у протидії дезінформації;
- описати розвиток медіаосвіти як інструменту протидії дезінформації та пропаганди в суспільстві;
- виокремити роль, функції та завдання фактчекінгових організацій у протидії дезінформації.

**Об'єктом** дослідження є поширення та вплив дезінформації й пропаганди в українському інформаційному просторі.

**Предметом** дослідження є правові та інституційні механізми протидії дезінформації і пропаганди в інформаційному просторі України.

**Хронологічні рамки** нашого дослідження становлять 2014-2024 рр., що пов'язано з початком гібридної та повномасштабної війни росії з Україною.

**Практична значимість дослідження.** Отримані результати і висновки наукового дослідження можуть бути використані у процесі викладання навчальних дисциплін, спецкурсів у вишах та факультативних предметів в школах.

**Методи дослідження.** На різних етапах роботи, відповідно до поставлених завдань були використані спеціальні та загальнонаукові методи, а саме метод аналізу використано при опрацюванні нормативно-правової бази України, що стосується поширенню дезінформації та боротьби з нею; історичний метод дав змогу простежити основні етапи розповсюдження дезінформації та формування інституційних механізмів для ефективної протидії цій загрозі на теренах України; метод узагальнення використано для виявлення головних загроз та викликів в умовах розквіту сучасних технологій.

Також нами було застосовано методологічний прийом кейс-стаді, який передбачає вивчення певних випадків і подій, пов'язаних із дезінформацією і пропагандою в інформаційному просторі України, з метою отримання глибшого розуміння конкретних ситуацій.

**Структура роботи.** Магістерська робота складається зі вступу, трьох розділів, восьми підрозділів, висновків до розділів, загальних висновків та списку використаної літератури (71 позиція). Загальний обсяг роботи становить 77 сторінок.

## РОЗДІЛ 1

### ТЕОРЕТИКО-МЕТОДОЛОГІЧНІ АСПЕКТИ ДОСЛІДЖЕННЯ ПРОТИДІЇ ДЕЗІНФОРМАЦІЇ ТА ПРОПАГАНДИ В ІНФОРМАЦІЙНОМУ ПРОСТОРІ УКРАЇНИ

#### 1.1. Концептуальні та методологічні засади дослідження понять «дезінформації» та «пропаганди»

В українському інформаційному просторі боротьба з дезінформацією та пропагандою є дуже важливим завданням у сучасних реаліях. У нинішніх українських реаліях, через масштабну військову агресію Росії, що супроводжується потужною інформаційною війною, боротьба з дезінформацією та пропагандою набула надзвичайно важливого значення. Російська Федерація використовує витончені інформаційно-психологічні технології для підриву морального духу українського суспільства, дискредитації влади, маніпулювання громадською думкою, послаблення бойового духу населення та військовослужбовців. Український інформаційний простір став важливою ареною геополітичного протистояння, і на цій арені дезінформація поступово перетворюється на потужну зброю стратегічного впливу. Російська пропаганда є системною, багаторівневою та охоплює широкий спектр каналів комунікації - від традиційних ЗМІ до соціальних мереж та месенджерів. Її основний наратив спрямований на створення альтернативної реальності, применшення героїзму українського народу та заперечення права України на національний суверенітет і незалежність. У цьому контексті розробка ефективних механізмів протидії інформаційним загрозам має не лише наукову цінність, а й унікальне практичне значення для забезпечення національної безпеки України. Дослідження концептуально-методологічних засад протидії дезінформації має особливе значення як для теоретичного осмислення, так і для розробки ефективних стратегій захисту національного інформаційного суверенітету.



Це завдання потребує багатоаспектного та комплексного дослідження з метою ефективної протидії цим загрозам та забезпечення інформаційної безпеки суспільства.

Неправдива інформація та пропаганда відіграють важливу роль у ході війни і впливають на національне та міжнародне сприйняття ситуації на лінії фронту. Дезінформація (пропаганда, фейкові новини) не є новим явищем, з яким світ зіткнувся вперше - вона супроводжувала мирні внутрішньополітичні рухи та військово-політичні протистояння між різними країнами з часів утворення першої держави. Водночас сучасні інформаційні технології, зміна способів сприйняття інформації та криза «класичних» медіа трансформували світовий інформаційний ландшафт [61, с. 9].

Інформаційна війна є одним з ключових напрямків війни проти Росії. Щодня українські державні інституції, приватні компанії та пересічні українські громадяни стикаються з великою кількістю інформаційних загроз. У сучасній війні неправильне використання інформації може призвести до значних втрат, а інформація є справжньою зброєю [28, с. 119].

24 лютого 2022 року Росія розпочала відкриту збройну агресію проти України. Однак гібридна війна триває ще з 2014 року. Неправдива інформація є одним з основних інструментів російської агресії проти нашої країни. Російське керівництво використовує дезінформацію для досягнення кількох цілей. Перш за все дестабілізувати ситуацію в Україні та підірвати довіру до української влади; сприяння захопленню та окупації українських територій; ізолювати українське суспільство [23, с. 332-333].

Неправдива інформація є окремим явищем від суміжних понять «брехня», «дезінформація», «обман» та «маніпуляція». Для того, щоб проаналізувати це явище, визначити засоби боротьби з дезінформацією на державному рівні у воєнний час та сформулювати ефективні рекомендації, необхідно концептуалізувати термін «дезінформація», визначивши низку характеристик дезінформації.

У загальному розумінні дезінформація - це навмисне поширення неправдивої та оманливої інформації для досягнення певної мети. Роман Михайленко є автором дослідження «Феномен дезінформації в умовах російської агресії», яке було представлено на міжнародній науково-практичній конференції «Дезінформація в контексті протидії російській агресії в Україні: виклики та перспективи» (Анн-Арбор - Харків, 2023 р.). У своїй роботі він проаналізував природу дезінформації та її вплив на українське суспільство, наголосивши, що вона спрямована проти незалежності, суверенітету та територіальної цілісності України. У дослідженні зазначається, що дезінформація є інструментом гібридної війни, який допомагає поширювати агресивну пропаганду, розпалювати ненависть та маніпулювати громадською думкою. Автори також вказують на шляхи протидії дезінформації, зокрема шляхом посилення регуляторних механізмів та підвищення інформаційної грамотності населення, Р.В. Михайленко стверджує, що дезінформація спрямована на ліквідацію незалежності України, повалення чинної влади України, порушення суверенітету і територіальної цілісності України, пропаганду війни, жорстокості та насильства, розпалювання міжетнічної, релігійної та расової ворожнечі, тощо [28, С. 119].

Дезінформація — це цілеспрямована стратегія маніпуляції інформацією, що має на меті досягнення конкретних політичних, економічних або соціальних цілей шляхом обману суспільства чи певних його груп. Згідно з Оксфордським словником, це «усвідомлене розповсюдження хибної інформації». Ключовими ознаками тут є свідомий характер обману і поширення інформації, яка суперечить істині [39, с. 45].

У звіті «Багатовимірний підхід до дезінформації» Європейської комісії поняття дезінформації охоплює всі форми неправдивої, неточної або оманливої інформації, яка створюється, розповсюджується та пропагується з метою завдання шкоди суспільству чи отримання вигоди. Основними характеристиками є її спрямованість, умисність та інструменталізація для досягнення визначених цілей [13, с. 19].

Українська освітня платформа EdEra у співпраці з IREX розглядає дезінформацію як маніпулятивний контент, спеціально створений для обману громадськості. Це визначення підкреслює маніпулятивний аспект інформації та її спрямованість на викривлення реальності у свідомості споживачів [58, с. 32]. Інститут масової інформації додає важливий аспект телеологічності дезінформації: це завжди цілеспрямоване поширення неправдивої інформації з метою послаблення довіри до джерел чи створення хаосу в суспільстві [59, с. 12].

Аналітики організації «TEXTY.ORG.UA» вважають, що поняття «дезінформація» передбачає акцент на певному світогляді, позиції. Тобто вони під дезінформацією мають на увазі просування або формування певного дискурсу у медіа, до того ж він може бути неочевидним для кінцевого споживача інформації [59].

Визначення дезінформації зі звіту HLEG застосовується у документації Європейської Комісії і Ради Європи, на нього опираються різні дослідники явища дезінформації. В колективній аналітичній доповіді 2019 р. українські експерти підтримують концепцію використання поняття «дезінформація» замість поняття «фейкові новини», водночас пропонують дещо інший погляд на його розуміння. Це зумовлено, зокрема, несерйозним ставленням до проблеми обмеження поширення дезінформації в Україні, включенням до цілей дезінформації економічного компоненту (отримання вигоди), а також використанням розмитих понять «неточна» та «оманлива» інформація. Також нечіткою є різниця між такими цілями дезінформації, як «обдурення» та «введення в оману» [61, с. 23].

Автори доповіді «Фейки, пропаганда, дезінформація та виборчий процес: як нам захистити демократичні практики?» виокремлюють такі ознаками дезінформації:

1. Вплив на певну (цільову або масову) аудиторію через її оприлюднення.
2. Спрямованість (наявність організатора та певний намір).
3. Негативні наслідки.

4. Наявність в основі дезінформації «неправдивості», яку можна перевірити.

5. Імітаційність (представляється як правдивий матеріал).

6. Відповідність певним переконанням, системам поглядів, оскільки дезінформація на випадкові теми не досягає мети.

7. Відношення до соціально значущих подій, що є чутливими для населення або мають символічну цінність [61, с. 24].

У сучасних академічних та лексикографічних джерелах дезінформація постає багатогранним феноменом, який виходить за межі простого викривлення фактів. Кембриджський та Оксфордський словники трактують це поняття переважно через призму навмисного обману, підкреслюючи інтенційність поширення неправдивої інформації.

Особливо цікавим є історичний контекст, що його наголошує Оксфордський словник: поняття дезінформації з'явилося в європейському науковому дискурсі у 50-х роках минулого століття, маючи виразне російське термінологічне походження. Радянська лексикографічна традиція пропонувала дещо відмінну концептуалізацію, акцентуючи не стільки на неправдивості, скільки на цілеспрямованій маніпуляції уявленнями про реальність.

Сучасне розуміння дезінформації виходить за класичні рамки простого спотворення інформації. Нині це складний комунікативний феномен, який може включати не лише відверто хибні відомості, але й частково правдиві дані, навмисно препаровані або контекстуально викривлені з метою досягнення певних маніпулятивних цілей. Ключовим елементом залишається саме інтенційність та приховане прагматичне навантаження такої інформації.

Таким чином, дезінформація постає не просто як технічний засіб викривлення реальності, а як складний соціально-комунікативний інструмент впливу на масову свідомість, що має глибокий маніпулятивний потенціал [32, С. 36].

- Дезінформація («dis-information»). Інформація, яка є неправдивою та навмисно створена для заподіяння шкоди людині, соціальній групі, організації чи країні.
- Невірна, хибна інформація («mis-information»). Інформація, яка є неправдивою, але не створена з метою заподіяння шкоди.
- Шкідлива, зловмисна інформація («mal-information»). Інформація, яка базується на реальних подіях та використовується для заподіяння шкоди людині, організації чи країні» [13].

Згідно із дослідженням Лундського університету, одним із різновидів дезінформації є також пропаганда, тобто «інформація, створена із метою впливати на свідомість громадськості або громадську думку для того, щоб здобути вигоду певному політику, організації або уряду» [5, с. 201].

У якості різновидів дезінформації також розглядаються пародія сатира і реклама, які «мають суттєвий потенціал і можуть бути легко застосовані для передачі конкретних або суперечливих ідей цільовій аудиторії». Окрім цього, такі класифікації також визначають інтерпретацію реальних фактів як різновид дезінформації [67, с. 56].

Інтерпретація, тобто тлумачення на основі певного розуміння, яке базується на таких категоріях як думка, судження й погляд і не може бути обмеженим чи стати об'єктом регулювання й відповідальності. Водночас визначення поняття «погляд» має бути конкретизоване на законодавчому рівні [5, с. 201].

Наступної проблеми стосуються канали поширення дезінформації. Дезінформація втілюється через новини (теле- та радіоповідомлення, статті, онлайн-публікації, соціальні медіа), діяльність ботоферм, тролів чи здійснення інформаційних витоків. Найчастіше дезінформація закладається саме в новини, оскільки вони є найбільш оперативними та найбільш популярними, а, отже, їхнє розповсюдження може бути найшвидшим та наймасовішим. Саме тому такі новини потрібно називати фейковими новинами, які постають як один із найпоширеніших механізмів дезінформації.

Дезінформація, як конкретне викривлення реальності, порушує нормальне протікання демократичних процесів у суспільстві (вибори, громадські заходи), впливає на політичні погляди і волевиявлення, розколює суспільство й розпалює конфлікти, підриває довіру до політичного і військового керівництва держави. Особливу небезпеку для нашої країни дезінформація становить у часи збройної агресії росії у формі повномасштабного вторгнення в Україну, поєднаного з гібридними формами ведення війни [27, С. 246].

Саме через цей чинник виникає необхідність постійного моніторингу дезінформаційних спробросії, націлених проти українського суспільства й демократичного світу загалом, а також систематичного відстеження змін у характері діяльності російського пропагандистського апарату.

Різновиди дезінформації - це різновиди неправдивої інформації скоріше, а не дезінформації. Virізняють наступні види:

- fakefact («фейк-факт») – імітація ситуації (дія у фізичному середовищі або організована подія), яка виправдано дає змогу робити певні інтерпретації; вчені стверджують, що це є найбільш потужний різновид дезінформації;
- fakesource («фейк-сурс») – неправдиве джерело або приписування хибної інформації відомому джерелу;
- fakecontext («фейк-контекст») – неправдивий контекст;
- click-beit («клік-бейт») – невідповідність заголовка змісту. .

Водночас дезінформація часто є лише частиною масштабнішого явища – пропаганди. Ще одним важливим інструментом просування своїх інтересів в інформаційному просторі є російська пропаганда, яка активно використовується для посилення впливу дезінформаційних кампаній. Пропаганда – це потужний інструмент маніпулювання суспільною думкою. Світові війни минулого століття, економічні й соціальні кризи, домінування тоталітарних режимів і, разом з цим, утвердження пропаганди як інструменту впливу на свідомість населення, призвели до формування хибного деформованого відображення суспільством правової реальності. Деформація правової свідомості – це феномен,

який відображає викривлене розуміння цінності права та втілює негативне ставлення до правопорядку та законності.

Визначення терміну «пропаганда» подається фактично в усіх енциклопедичних виданнях, які повною мірою розкривають значення цього явища. В цілому, це є система засобів і прийомів впливу на свідомість і поведінку людей для досягнення певних соціальних, політичних й економічних цілей.

У політологічному словнику під редакцією Головатого М. Ф. та Антонюка О. В. пропаганда постає як діяльність, що передбачає системне розповсюдження, глибинне роз'яснення економічних, соціально-політичних, правових ідей, поглядів, теорій та забезпечує формування у суспільстві конкретних настроїв, утвердження у громадській свідомості певних цінностей, уявлень та орієнтацій із метою максимального розширення кола прихильників певної ціннісної системи [62, с. 145].

В основному пропаганда реалізується переважно через засоби масової інформації, допомагаючи набуті форми мотивації, але на практиці зводиться переважно до психологічного навіювання, тобто безпосереднього подання певної інформації; це слова, сказані однією людиною іншій, і відбувається це без волі сприймаючої особи, часто навіть без її явного усвідомлення. Основними складовими процесу публік релейшнз є суб'єкт (соціальна група, яка виражає свої інтереси через публісіті), зміст, форма і метод, засоби або канали публісіті (телебачення, радіо, система лекційного публісіті, газети) і об'єкт (публісіті по відношенню до цільової аудиторії або соціальної групи). Для кращого розуміння процесу зв'язків з громадськістю дуже важливими є соціальні інтереси об'єкта публісіті, їх зіставлення із загальними інтересами суспільства, а також інтересами окремої групи, яка є об'єктом публісіті. Це визначає зміст пропаганди і впливає на вибір форм, методів і засобів пропаганди. Основна психологічна мета пропаганди - впливати на систему політичних, соціальних та ідеологічних відносин людей і змінювати цю систему шляхом формування нових відносин або посилення (послаблення) існуючих [19, с. 20].

Сьогодні виділяють наступні типи пропаганди:

- чорна пропаганда – приховує реальне джерело певної інформації й використовує інше як «першоджерело»;
- сіра пропаганда – поширення певної інформації без посилання на джерело чи конкретного автора;
- позитивна пропаганда – спрямована на зміцнення соціального благополуччя;
- негативна пропаганда – спрямована на розпалення соціальної ворожнечі, соціальних конфліктів, загострення протиріч у суспільстві та пробудження первинних інстинктів людей [37, с.15].

Українська дослідниця Васильєва Н.В. у своїй роботі зосереджується на пропаганді як потужному інструменті, який використовується в інформаційно-комунікативній політиці. Вона досліджує, як пропаганда може загрожувати національній безпеці. Імовірно, авторка аналізує конкретні приклади з українського та міжнародного контексту, розглядаючи різноманітні способи маніпуляції громадською думкою.

Гапій В.Е. у своїй статті досліджує більш глибокі психологічні аспекти пропаганди. Він зосереджується на тому, як пропаганда впливає на підсвідомість людини, використовуючи різноманітні прийоми і маніпулятивні техніки. Можливо, автор також аналізує, як ці механізми використовуються в сучасній Україні. Обидва автори розглядають пропаганду як серйозну загрозу, яка може мати далекосяжні наслідки для суспільства. Вони підкреслюють важливість розуміння механізмів пропаганди для того, щоб протистояти їй. Пропаганда – це не просто передача інформації, а скоріше спроба маніпулювати сприйняттям і поведінкою людей. Вона часто використовує емоції, стереотипи та спрощення для досягнення своїх цілей. Сучасні інформаційні технології значно посилюють ефективність пропаганди. Протидія пропаганді вимагає критичного мислення, медіаграмотності та освіти [19; 21].

Концептуально-методологічні засади дослідження протидії дезінформації та пропаганді в українському інформаційному просторі ґрунтуються на різних підходах і методологіях до розуміння, аналізу та протидії цим негативним



явищам. Основними концептуальними та методологічними підходами до дослідження протидії дезінформації є

Міждисциплінарний підхід - вибір методів і підходів з різних дисциплін (соціології, політології, медіазнавства, психології тощо) для більш глибокого розуміння природи і впливу дезінформації та пропаганди. Аналіз медіа-контенту - вивчення медіа-контенту, включно з новинами, соціальними мережами та веб-сайтами, з метою виявлення відповідних закономірностей, тенденцій та джерел дезінформації та пропаганди.

Опитування та соціологічні дослідження - допомагають нам зрозуміти вплив дезінформації та пропаганди на населення, сприйняття та переконання, а також визначити переваги щодо джерел інформації.

Порівняльний аналіз - зіставлення актуального досвіду зарубіжних країн у сфері протидії дезінформації та пропаганді на основі використання ефективних практик і стратегій.

Використання технологій - застосування сучасних технологічних можливостей (використання штучного інтелекту, аналіз великих масивів даних, автоматизація процесу виявлення та аналізу дезінформації та пропаганди в Інтернеті). [19, с. 34; 21, с. 636].

Такий концептуально-методологічний підхід допомагає розробити стратегії та заходи для ефективної протидії дезінформації та пропаганді в інформаційному просторі України.

Дезінформація та пропаганда є невід'ємними елементами сучасної інформаційної війни, які відіграють ключову роль у формуванні масової свідомості та маніпуляції суспільними настроями. Вони перетворилися на складний інструмент стратегічного впливу, що активно використовується Російською Федерацією в умовах гібридної війни проти України. Такі інформаційні загрози не тільки підривають національну безпеку, а й створюють викривлену реальність, спрямовану на дестабілізацію внутрішньополітичної ситуації, послаблення довіри до державних інституцій та формування вигідних агресору наративів.

Наукові концепти дезінформації ґрунтуються на її визначенні як свідомого поширення неправдивої або маніпулятивної інформації з метою досягнення політичних, соціальних чи економічних цілей. Її вплив часто реалізується через поширення фейкових новин, маніпуляцію фактами або контекстами, що викликає зміни у сприйнятті реальності як на індивідуальному, так і на колективному рівнях. Дезінформація виконує декілька основних функцій, серед яких — дискредитація влади, деморалізація суспільства, створення розколу в його структурі та маніпуляція міжнародною громадською думкою.

Пропаганда, яка діє паралельно з дезінформацією, має більш системний характер. Вона спрямована на створення довготривалого впливу на суспільні уявлення та формування стійких наративів, що відповідають стратегічним цілям її ініціаторів. У контексті російської інформаційної агресії пропаганда використовується для посилення впливу дезінформаційних кампаній, спрямованих як на внутрішню аудиторію, так і на міжнародну. Її інструментарій включає традиційні ЗМІ, соціальні мережі, онлайн-видання, а також індивідуальні інформаційно-психологічні операції.

Отже, дезінформація та пропаганда є багатофакторними феноменами, які вимагають комплексного аналізу та розробки стратегій протидії. Їхній вплив в умовах сучасної гібридної війни підкреслює важливість не лише підвищення медіаграмотності населення, але й забезпечення координації між державними інституціями, громадським сектором і міжнародними партнерами для збереження інформаційного суверенітету та стабільності суспільства.

## **1.2. Стан наукової розробки проблеми**

Наукове дослідження проблеми протидії дезінформації та пропаганді в українському інформаційному просторі залишається ключовою та важливою темою. Це питання набуло великого значення внаслідок складних суспільно-політичних подій та гібридної війни, яку веде Російська Федерація проти Української держави.

Предметом нашого дослідження є дослідження механізмів поширення дезінформації, виявлення її джерел та впливу на суспільство. Дослідники також вивчають роль соціальних мереж, ЗМІ та геополітичні аспекти цього явища. Результати їхніх досліджень можуть стати основою для розробки стратегій боротьби з дезінформацією та підвищення рівня інформаційної грамотності суспільства.

Стан наукової розробки питань протидії дезінформації та пропаганді в українському інформаційному просторі є предметом детального аналізу та обговорення в сучасних наукових колах.

Поняття «дезінформація» досліджували вітчизняні та зарубіжні дослідники комунікаційно-інформаційного простору, зокрема Самчинська О. М. [32], яка ґрунтовно проаналізувала сутність та концептуальні виміри процесів дезінформації, та зарубіжні вчені, які досліджували різні аспекти цього явища.

Згідно з її підходами, дезінформація не є статичним процесом, а має багатогранну структуру, в межах якої можна виокремити кілька ключових етапів. Перш за все, вона визначає дезінформацію як стратегічний інструмент, який активно використовується для зміни громадської думки, маніпулювання політичними процесами і навіть перекручування фактів до рівня, коли вони починають сприйматися як істина. У цьому контексті, важливо відзначити, що дезінформація не обмежується лише явищем спотворення фактів, а включає в себе цілу систему механізмів, що забезпечують її поширення, легітимізацію і сприйняття[38].

Самчинська О.М. зазначає, що дезінформація є складним соціальним і комунікаційним процесом, в межах якого інформація, що є неповною або неправдивою, спеціально виготовляється і поширюється з метою маніпулювання громадською думкою. Вона є частиною широкого спектра комунікаційних стратегій, що включають в себе обман, маніпуляцію, дисторсії та перекручення. Важливою особливістю дезінформації, яку виділяє авторка, є її здатність адаптуватися до різних соціальних і культурних контекстів, де неправдива

інформація може бути подана як факт, що відповідає певним ідеологічним чи політичним переконанням аудиторії.

Вона пропонує визначити кілька етапів дезінформаційного процесу, які є необхідними для того, щоб неправдива інформація стала частиною загального інформаційного потоку. На першому етапі формується інформація, яка буде використана для маніпуляції або введення в оману. Це може бути як свідоме створення вигаданих фактів, так і перекручення наявних даних, що є частиною більш широкої пропагандистської кампанії. Вона підкреслює, що на цьому етапі важливо враховувати мету маніпуляції: зміна політичних, соціальних чи економічних умов через виведення певних груп на вулиці, зміна політичних напрямків чи підвищення політичної впливовості. Другим етапом є поширення неправдивої інформації через різні канали комунікації[38]. Цей етап може бути особливо ефективним завдяки впливу медіа і соціальних мереж, які мають можливість досягати масової аудиторії за короткий проміжок часу. Самчинська О.М. зазначає, що на цьому етапі велике значення має саме візуальна складова — заголовки, фото, відео, що швидко привертають увагу і можуть навіть без подальшої перевірки становити основу для формування сприйняття. Третім етапом є легітимізація дезінформації. На цьому етапі неправдива інформація починає сприйматися як реальність, і її інтерпретація стає загальноприйнятою. Це може бути досягнуто через повторення інформації в різних джерелах, де вона подається як факт, або через висвітлення в рамках авторитетних джерел, що дозволяє здобути громадське визнання. Дезінформація, таким чином, набуває вигляду правдивої і перевіреної інформації, що впливає на масове сприйняття подій.

Одним із найважливіших аспектів, на який вона звертає увагу, є використання маніпулятивних технологій для поширення дезінформації. Вона підкреслює, що маніпуляція в сучасному медіапросторі є невід'ємною частиною процесу створення і розповсюдження неправдивої інформації. Серед основних технологій, які використовуються для маніпуляції, виділяються:

1. **Медіа-маніпуляція:** Це використання медіа для нав'язування певних думок або переконань. Наприклад, через вибірккову подачу фактів або інтерпретацію подій так, щоб вони відповідали заздалегідь визначеним політичним чи соціальним цілям.

2. **Фальшиві новини:** Створення новин, які не відповідають реальності, але мають сильний емоційний або політичний заряд, що сприяє їх поширенню.

3. **Вірусні кампанії:** Використання соціальних мереж для організації кампаній, які можуть швидко набути популярності завдяки механізмам поширення контенту через мережі. Це дозволяє дезінформації поширюватися експоненціально і охоплювати великі аудиторії.

4. **Фальшиві експерти:** Часто до поширення дезінформації долучаються вигадані або неперевірені «експерти», які надають авторитету неправдивим заявам. Це допомагає переконати громадськість у правдивості інформації, адже люди схильні довіряти тим, кого вважають професіоналами[38].

У контексті досліджень дезінформації важливо звернути увагу на маніпуляційні технології, що активно застосовуються в рамках російської пропаганди, зокрема щодо поширення неправдивої інформації про події в Україні. О. І. Степанюк та А. В. Сліпченко стали одними з провідних вітчизняних дослідників, які ґрунтовно аналізують механізми, через які Росія використовує дезінформацію як інструмент політичного впливу. Їхні дослідження висвітлюють основні напрямки роботи російської пропаганди, включаючи побудову фальшивих наративів, спрямованих на дискредитацію українських військових, правозахисників, а також державних інституцій України. Це дозволяє побачити, як стратегічні комунікації та маніпулятивні технології допомагають створювати образ ворога, що має вигідно змінювати сприйняття подій у світі.

Основною метою російської пропаганди є не лише дезінформація, а й створення специфічного образу, який маніпулює громадською думкою як в межах Росії, так і за її межами. Пропаганда зводиться до створення фальшивих новин і викривлення фактів, аби сформувати вигідне для Росії уявлення про

реальність. У своїх дослідженнях О. І. Степанюк та А. В. Сліпченко детально розглядають, як за допомогою сучасних медіа та соціальних мереж Росія здійснює кампанії, спрямовані на поширення дезінформації. Вони зазначають, що один із найефективніших методів — це використання соціальних мереж як основного каналу для трансляції маніпуляцій, адже ці платформи дають змогу швидко поширювати інформацію на широку аудиторію та знижують рівень перевірки фактів [19, с.30].

Важливим аспектом є і стратегічна роль соціальних медіа в процесах маніпуляції та організації кампаній з дезінформації. Дослідники підкреслюють, що соціальні мережі дозволяють здійснювати точкові маніпуляції, формуючи потрібний наратив, що може бути надзвичайно ефективним для досягнення політичних цілей. Вони особливо звертають увагу на використання «ботів» та «тролів», які активно поширюють фальшиві новини, а також на важливість алгоритмів, що дозволяють цим новинам досягати великої аудиторії, зокрема у соціальних мережах, де відсутня традиційна журналістська етика.

Крім того, дослідники аналізують механізми побудови фальшивих новин, які є складовою частиною російської пропаганди. Фальшиві новини, згідно з їхніми спостереженнями, мають дуже важливу роль у створенні так званих «перемішаних реальностей», де правда і брехня переплітаються, що ускладнює завдання для реципієнтів інформації [19]. Таким чином, неправдиві новини часто подаються у вигляді, що виглядає правдоподібно, а їхня мета полягає в тому, щоб викликати емоційну реакцію, яка змінює уявлення людей про події. Зокрема, маніпулювання фактами щодо війни в Україні спрямоване на формування уявлення про захисників як агресорів, а також на подання викривленої картини того, що відбувається на фронті.

Ще одним важливим моментом є методи використання соціальних мереж для маніпуляцій, що дозволяють активізувати інформаційні кампанії, скоординовані за допомогою різних «клієнтів» — користувачів, які поширюють певний наратив у маси. Степанюк та Сліпченко звертають увагу на важливість «клієнтської роботи» для успішного реалізування кампанії, де метою є не просто

поширення певної неправдивої інформації, а й формування належного контексту, який дозволяє впливати на масову свідомість. Це не просто фабрикація фактів, але й їхні емоційні та психологічні наслідки, які запускаються через медіаплатформи.

Одним із важливих аспектів маніпулятивної діяльності, що розглядається у роботах авторів, є створення образу ворога. Росія активно формує через медіа-канали негативний образ України та українських громадян, перекручуючи реальні факти і замінюючи їх на вигадані історії, які мають підсилити агресивні настрої як серед внутрішньої аудиторії, так і серед міжнародної спільноти. Ці наративи часто мають за мету не лише дискредитацію української державності, а й створення глибокої тривоги та неспокою серед інших країн, намагаючись викликати сумніви щодо надійності України як держави.

Нарешті, механізми маніпуляції та дезінформації, що їх застосовує Росія, показують, як складно відрізнити правду від вигадки в умовах сучасного інформаційного простору. Як зазначають дослідники, в умовах такої глобалізованої медіапростору важливо мати інструменти, які дозволяють критично ставитися до споживаної інформації. Вони наголошують на необхідності розвитку фактчекінгу та медіаграмотності серед громадян, оскільки ці інструменти стають основою для протидії маніпуляціям, що здійснюються за допомогою медіа та соціальних мереж.

Загалом, дослідження О. І. Степанюка та А. В. Сліпченка дають глибоке розуміння того, як маніпулятивні технології використовуються для досягнення політичних цілей через дезінформацію. Вони допомагають чітко окреслити механізми роботи російської пропаганди, яка активно впливає на глобальний інформаційний простір, і водночас підкреслюють важливість розуміння цих процесів для адекватної відповіді на сучасні інформаційні виклики.

Однією з основних стратегій боротьби з дезінформацією є розвиток фактчекінгу та медіаграмотності, що є важливими інструментами для подолання маніпуляцій в інформаційному просторі. М. В. Гороховський та його колеги розробили інноваційний підхід до цієї проблеми, звертаючи особливу увагу на

необхідність розвитку критичного мислення серед громадян, а також на важливість навчання вмінню перевіряти інформацію, що надходить через різноманітні медіа-канали. Вони акцентують увагу на тому, що в умовах бурхливого розвитку цифрових технологій та глобалізації інформаційних потоків, вміння правильно оцінювати та перевіряти інформацію є критично важливим для захисту суспільства від дезінформації.

О.М. Гороховський наголошує, що фактчекінг є одним із ключових інструментів у боротьбі з дезінформацією, адже цей процес передбачає не лише перевірку фактичної точності інформації, але й з'ясування контексту її поширення. Важливо зазначити, що фактчекінг включає не тільки перевірку простих фактів, а й аналіз джерел інформації, дослідження можливих мотивів поширення певної інформації, а також визначення методів її маніпулятивного використання. В умовах сучасної інформаційної війни, де інструменти пропаганди використовуються з метою перекручення фактів і створення вигаданих наративів, фактчекінг стає необхідним елементом для відновлення справжнього стану речей та протидії маніпуляціям.

З огляду на глобалізацію інформаційних потоків, коли новини та повідомлення з різних куточків світу моментально потрапляють до широкої аудиторії, О.М. Гороховський підкреслює, що важливість фактчекінгу лише зростає. Процес глобалізації дозволяє інформації поширюватися без обмежень і миттєво досягати будь-якої точки світу, однак це також створює серйозні загрози для інформаційної безпеки. У таких умовах фактчекінг не лише допомагає виявляти неправдиві або маніпулятивні повідомлення, але й сприяє формуванню відповідальної інформаційної культури серед громадян. Адже правильно організований фактчекінг дозволяє не лише виявляти помилки або фальшиві новини, а й відновлювати правду в публічному просторі.

Не менш важливим є розвиток медіаграмотності, що також є важливою частиною стратегії боротьби з дезінформацією. Медіаграмотність передбачає не лише вміння користуватися медіа-технологіями, а й критично оцінювати інформацію, що надається через різні медіа-канали. Це включає в себе здатність



аналізувати джерела інформації, розуміння того, як формуються новини, а також здатність виявляти елементи маніпуляції в текстах та відео. Розвиток медіаграмотності дозволяє громадянам не лише оцінювати правдивість інформації, але й знижувати рівень сприйняття маніпуляцій, що активно використовуються в умовах сучасних інформаційних війн.

Дослідник зазначає, що в умовах, коли громадяни мають доступ до величезної кількості інформації, важливо створювати інструменти для її критичного осмислення. Тому важливими аспектами медіаграмотності є не лише знання того, як перевіряти факти, але й здатність розуміти, як працюють інформаційні потоки, як вони формують уявлення людей про події та процеси у світі. Таким чином, розвиток медіаграмотності сприяє підвищенню рівня інформаційної безпеки, адже допомагає громадянам приймати більш усвідомлені рішення в умовах постійної інформаційної нестабільності [14, с.29].

У своїх дослідженнях, О.М. Гороховський також підкреслює, що фактчекінг та медіаграмотність є важливими інструментами не лише для окремих осіб, але й для цілого суспільства. Вони дозволяють створити середовище, в якому дезінформація не може безкарно поширюватися, а маніпуляції втрачають свою ефективність. Розвиток цих інструментів забезпечує підтримку об'єктивної інформації в медіапросторі, сприяючи формуванню здорової громадської думки, яка базується на фактах, а не на фальшивих наративах.

Проблема фактчекінгу в Україні має свою специфіку, яка обумовлена як внутрішніми, так і зовнішніми загрозами інформаційної безпеки. Українське медіаполе переживає інтенсивний вплив не тільки з боку державних структур та громадських організацій, а й від зовнішніх акторів, зокрема з боку держав, що займаються активним використанням інформаційних маніпуляцій. Дослідження С. В. Романюка та О. В. Шуби вказують на те, що незалежна перевірка фактів є важливою складовою стратегії боротьби з дезінформацією, а їхні роботи докладно розглядають особливості фактчекінгової діяльності в Україні,

аналізуючи вплив і потребу в цьому процесі для ефективної комунікації в умовах сучасної інформаційної війни.

Романюк і Шуба зазначають, що в Україні зростає потреба у розвитку інститутів, які займаються перевіркою фактів, особливо в контексті глобальних інформаційних загроз. Роль таких інститутів стає незамінною для боротьби з маніпуляціями, що можуть вплинути на громадську думку та політичну ситуацію в країні [54]. Вони підкреслюють, що цей процес є необхідним для відновлення довіри до медіа та державних інституцій, адже лише через незалежну перевірку фактів можна забезпечити прозорість і об'єктивність інформаційного простору. Важливо, що дослідники акцентують увагу на тому, що саме в Україні фактчекінг здатний стати важливим елементом стратегічних комунікацій, особливо в контексті сучасних виборчих кампаній, соціальних протестів та інших суспільно важливих подій.

Аналіз методологічних аспектів фактчекінгу, проведений Романюком та Шубою, також є важливим для розвитку цього інструменту в Україні. Вони детально розглядають процеси перевірки інформації, акцентуючи увагу на різних рівнях перевірки — від базового аналізу фактів до більш складних методів перевірки, що включають перевірку джерел інформації, вивчення контексту і встановлення достовірності наданих даних. Окрім того, дослідники також зазначають важливість технологічних інструментів у цій сфері, адже сучасні цифрові технології дозволяють швидко аналізувати великий обсяг інформації та перевіряти її достовірність в режимі реального часу.

Також важливою частиною роботи є розвиток стратегічних комунікацій в Україні, які є ключовими для забезпечення ефективного функціонування фактчекінгу в умовах інформаційної війни. Романюк і Шуба наголошують, що стратегічні комунікації повинні базуватися на принципах відкритості, прозорості та достовірності, що дозволяє забезпечити не лише боротьбу з дезінформацією, а й належну взаємодію з громадськістю. Вони підкреслюють, що саме в Україні необхідно створити нові медіа-структури та платформи, які могли б стати

основою для незалежної перевірки фактів і боротьби з інформаційними маніпуляціями.

Унікальність фактчекінгу в українському медіапросторі полягає також у тому, що цей процес не тільки допомагає зберігати інформаційну безпеку, але й сприяє формуванню критичної громадської думки, здатної протистояти дезінформації. Дослідження Романюка і Шуби демонструють, що фактчекінг в Україні є не лише інструментом для перевірки конкретних фактів, але й важливим елементом для формування здорової медіа-середовища, в якому громадяни можуть отримувати об'єктивну та точну інформацію.

Отже, розроблені підходи до фактчекінгу, пропоновані дослідниками, показують, що для України важливо не лише розвивати цей інструмент, але й інтегрувати його в загальний контекст інформаційної політики, що дозволяє значно підвищити рівень протидії дезінформації та маніпуляціям, а також сприяти розвитку відповідальної інформаційної культури серед населення.

Досягнення значного прогресу у сфері інформаційної безпеки є результатом системного підходу до аналізу сучасного стану цієї галузі, що був здійснений Виздриком І. О. та Мельником О. А. Їхні дослідження дозволяють глибше зрозуміти основні виклики, які постають перед Україною у боротьбі з маніпуляціями та пропагандою, особливо в умовах війни. На думку вчених, одним із основних завдань у боротьбі з маніпулятивним інформаційним впливом є створення ефективних механізмів захисту на всіх рівнях — від державних інституцій до окремих громадян.

Ці науковці аналізують стан інформаційної безпеки в Україні, зокрема звертають увагу на те, як зовнішні агресори, зокрема Росія, активно використовують дезінформаційні кампанії для маніпулювання громадською думкою. Це включає поширення неправдивої інформації, спотворення реальності, а також створення фальшивих наративів, що мають на меті дискредитувати українську державність, її військових та громадянське суспільство. Вчені підкреслюють, що ця боротьба є важливою не лише з огляду на захист країни від інформаційних загроз, але й як частина більш широкої

стратегії національної безпеки, що має включати інформаційну стратегію для протидії зовнішньому впливу.

На основі проведеного аналізу автори визначають низку основних викликів, з якими стикається Україна в боротьбі з інформаційними маніпуляціями. Одним із таких викликів є значний вплив соціальних мереж, які стають основним каналом для поширення фальшивих новин та маніпуляцій. Виздрик і Мельник також зазначають, що існує необхідність в активізації роботи з медіаграмотності серед населення, що дозволить знизити ефективність таких маніпуляцій та зменшити рівень їхнього впливу на громадську думку.

Дослідники звертають увагу на те, що, незважаючи на значний обсяг наукових праць, присвячених боротьбі з дезінформацією, існує певна прогалина в дослідженнях методів і принципів поширення пропаганди саме під час російсько-української війни. Оскільки інформаційна війна стала невід'ємною частиною сучасних військових конфліктів, дослідження, що аналізують особливості інформаційних операцій та методи поширення неправдивої інформації в цей період, є надзвичайно актуальними. Відтак, необхідно детальніше вивчати використання пропагандистських технологій, які Росія застосовує для дестабілізації ситуації в Україні та маніпулювання її громадською думкою, що вимагає розробки нових підходів до аналізу та протидії подібним загрозам.

Стратегія державної інформаційної політики України повинна ґрунтуватися на багаторівневому та комплексному підході, який враховує різноманітні аспекти захисту національних інтересів. Цей підхід не лише забезпечує належний захист прав і свобод громадян, але й підтримує розвиток інфраструктури інформаційної безпеки, яка є критично важливою в умовах сучасних викликів. Наприклад, під час російсько-української війни державна інформаційна політика України спрямована на боротьбу з ворожою пропагандою, що вимагає оперативного реагування та інтеграції новітніх технологій для протидії дезінформації.

Один з ключових аспектів цієї політики — захист прав громадян через удосконалення технічних та юридичних механізмів забезпечення правди в медіапросторі. В Україні для боротьби з фальшивими новинами створено численні незалежні організації фактчекінгу, такі як «StopFake», які перевіряють достовірність інформації, що поширюється в медіа. Це дозволяє громадянам отримувати точнішу інформацію та захищає їх від маніпуляцій. Проте, для ефективної боротьби з маніпуляціями важливо також розвивати інститут медіаграмотності серед населення, аби люди могли самостійно відрізнити правду від фальшування.

Важливою складовою є підтримка розвитку інформаційної інфраструктури, яка включає в себе сучасні засоби збору, обробки та поширення інформації. На прикладі інформаційної безпеки в Україні можна згадати запуск державного реєстру «Державний реєстр новин», де зберігаються перевірені новини. Цей реєстр дозволяє підвищити прозорість інформаційного простору та знизити можливості для маніпуляцій з боку як внутрішніх, так і зовнішніх акторів.

Особливу увагу також слід приділити використанню соціальних мереж для моніторингу та реагування на інформаційні загрози. Відомо, що соціальні мережі є одними з основних каналів поширення дезінформації, зокрема, в умовах військових конфліктів. Росія активно використовує ці платформи для розповсюдження неправдивої інформації про події в Україні. У відповідь на це українські органи влади та громадські організації розробили спеціальні інструменти для моніторингу контенту на соціальних платформах, що дозволяють своєчасно виявляти та спростовувати фальшиві новини.

Ще одним важливим елементом є створення ефективної політики щодо розвитку інформаційного потенціалу країни, що має прямий зв'язок із національними інтересами. Наприклад, активна робота інформаційних агентств, таких як «Укрінформ» та «Українська правда», сприяє забезпеченню об'єктивної і прозорої інформації, що в свою чергу допомагає створити позитивний імідж країни на міжнародній арені. Інформація про успіхи Збройних сил України,

гуманітарну допомогу постраждалим від війни та інші важливі ініціативи дає змогу сформувати правильну картину світу для міжнародної спільноти, зменшуючи можливості для ворожої пропаганди.

Тому стратегія державної інформаційної політики має включати не тільки технічні рішення, але й інституційні та соціальні ініціативи, які забезпечують ефективну боротьбу з дезінформацією. Це дозволить Україні зміцнити свою інформаційну безпеку, захистити права громадян, а також забезпечити належне функціонування демократичних процесів, навіть в умовах глобальних інформаційних воєн. Тільки комплексний підхід до інформаційної політики може гарантувати сталий розвиток держави в сучасному геополітичному середовищі.

## Висновки до 1 розділу

Подолання дезінформації в сучасному українському інформаційному просторі стало однією із нагальних проблем, яка вимагає детального наукового вивчення та вироблення дієвих практичних рішень. Перший розділ нашої магістерської роботи присвячений теоретико-методологічним аспектам цього питання, які включають у себе концептуальні і методологічні основи, а також аналіз стану наукової розробленості проблеми нашого дослідження. Висновки до цього розділу дають можливість визначити основні напрями подальших досліджень і практичних заходів.

Концептуальні засади дослідження протистояння дезінформації і пропаганді передбачають визначення ключових понять і їхніх характеристик. Дезінформація визначається як навмисне розповсюдження хибної інформації із метою введення в оману, у той час як пропаганда передбачає використання маніпулятивних технологій впливу на масову суспільну свідомість. Визначення цих понять і їхня класифікація є важливими для розуміння природи інформаційних небезпек і розробки дієвих стратегій протидії їм. Окрім цього, також потрібно правильно відрізняти різні типи дезінформаційних і пропагандистських впливів, зокрема політичну пропаганду, соціальну дезінформацію тощо.

Методологічні принципи нашого дослідження становить міждисциплінарний підхід, який включає соціологічні, психологічні, політичні та комунікаційні аспекти. Такий підхід дає змогу комплексно дослідити феномен дезінформації й пропаганди, а також проаналізувати їхній вплив на суспільство. Основними методами нашого дослідження виступають контент-аналіз, експеримент, експертне опитування та метод моделювання. Застосування цих методів відкриває можливість всесторонньо вивчити проблему і розробити ефективні засоби протидії. Наприклад, контент-аналіз дає змогу розглянути основні наративи і технологію маніпулювання, які застосовувалися у пропаганді,

а експертне опитування може дати нам аналітичні оцінки від фахівців стосовно ефективності певних стратегій протидії дезінформації й пропаганді.

Стан наукової розробки теми нашої магістерської роботи щодо протидії дезінформації і пропаганді в Україні демонструє, що ця тема є дуже актуальною сьогодні, проте розглянуті нами дослідження перебувають на початковому етапі розробки. Доволі багато аспектів залишаються поза увагою дослідників і потребують подальшого детального вивчення. Необхідною є також активна співпраця між науковими інституціями та державними органами управління за для вироблення комплексних стратегій протидії інформаційним загрозам. Окрім цього, важливо і розвивати інститути медіаграмотності, які могли б у кожному населеному пункті нашої країни критично оцінити здобуту інформацію і зменшувати вплив ворожої дезінформації й пропаганди.

Таким чином, розділ закладає міцну теоретичну й методологічну основу для подальшого вивчення і розробки успішних стратегій протидії дезінформації і пропаганді в українському інформаційному просторі. Окреслені нами концептуальні й методологічні принципи, а також аналіз наукової розробленості проблем, дозволяють визначити ключові напрямки майбутніх наукових досліджень, які сприятимуть зміцненню інформаційної безпеки нашої країни.



## РОЗДІЛ 2

### ПРАВОВІ ТА ІНСТИТУЦІЙНІ МЕХАНІЗМИ ПРОТИДІЇ ДЕЗІНФОРМАЦІЇ ТА ПРОПАГАНДИ РОСІЇ

#### **2.1. Виклики та загрози в інформаційному просторі України в умовах війни**

У сучасному світі інформаційна безпека відіграє одну із ключових ролей у захисті національних інтересів держави та стабільного функціонування громадянського суспільства. Таке значення інформаційної безпеки зумовлюється активним розвитком сучасних інформаційних технологій, комунікації та процесом інформатизації, а значить, зі зростанням впливу інформаційної сфери на життя населення, створенням інформаційного суспільства та технологій, які продовжують значною мірою впливати на відносини у галузі національної безпеки: інформаційні технології не тільки стали затребуваними по всьому світу, але й активно використовуються також у військовій сфері [51].

Тепер, коли світ перебуває у постійному розвитку, інформаційний простір перевантажується різними небезпеками в усіх сферах суспільного життя. На це варто звернути окрему увагу, так як події, що відбуваються в інформаційному просторі, несуть у собі потенційні загрози для нівелювання чинних засад інформаційного суспільства й виникнення нових суспільних відносин, які утворюються внаслідок певних інформаційних взаємозв'язків.

Інформаційна безпека – багатоаспектна сфера діяльності, у якій лише комплексний підхід може сприяти досягненню успіху. Проблеми, пов'язані із застосуванням інформаційних систем, можна поділити на такі категорії: забезпечення цілісності, конфіденційності й доступності ресурсів інформації та допоміжної інфраструктури. Інформаційна безпека постає як доволі обширне поняття і не обмежується тільки захистом від несанкціонованого доступу до інформації. Суб'єкт інформаційних відносин може зазнати шкоди не лише

внаслідок несанкціонованого доступу, проте і внаслідок можливої системної помилки [20, С. 196].

В умовах воєнних дій питання про потребу формування концепції єдиної інформаційної політики стало доволі актуальним. Зважаючи на таку необхідність, Президент України прийняв відповідний указ «Щодо реалізації єдиної інформаційної політики в умовах воєнного стану» (№ 152/2022) [12].

Інформаційна безпека постає як інтегрована складова національної безпеки та розглядається як пріоритетна функція будь-якої країни. Інформаційна безпека, з однієї сторони, передбачає забезпечення всебічного інформування населення і вільного доступу до різноманітних інформаційних ресурсів, а з іншої – здійснює контроль за можливим розповсюдженням дезінформації, сприяє єдності суспільства, оберігає інформаційний суверенітет, протидіє негативним інформаційно-психологічним впливам, а також захищає національний інформаційний простір від численних маніпуляцій, інформаційних кампаній та війн. Комплексної вирішення проблеми забезпечення інформаційної безпеки дозволить не лише захистити інтереси суспільства і країни, але й також забезпечити громадянське право на отримання всесторонньої, якісної та об'єктивної інформації [20].

Існують два аспекти тлумачення інформаційної безпеки в сфері національної безпеки. З однієї сторони, інформаційну безпеку розглядають як окремий компонент національної безпеки будь-якої держави, а з іншої – як інтегровану складову економічної, військової, політичної безпеки. Найґрунтовнішим є наступне визначення: інформаційна безпека – рівень захищеності критично важливих інтересів держави, суспільства та кожної особи, який мінімізує шкоду внаслідок неповноти, невчасності та недостовірності інформації, негативного інформаційного впливу, негативних наслідків використання сучасних інформаційних технологій, а також в результаті несанкціонованого поширення інформації. Це визначення є доцільним і повноцінно відображає взаємодію суб'єктів інформаційних відносин [20, 196].

Оскільки інформаційна безпека постає як складне, системне, багаторівневе явище, на розвиток якого безпосередньо впливають внутрішні й зовнішні фактори, розглянемо найбільш важливі серед них, а саме:

- 1) політична ситуація у світі (зовнішній чинник);
- 2) наявність можливих внутрішніх та зовнішніх загроз;
- 3) рівень інформаційно-комунікаційного розвитку держави (внутрішній чинник);
- 4) внутрішньополітична ситуація в країні [29].

Одночасно інформаційна безпека виступає як складна, динамічна, цілісна соціальна система, до елементів якої належать підсистеми безпеки держави, суспільства та будь-якої особи. Саме системна, взаємозалежна, інформаційна цілісність таких підсистем становить якісну визначеність, яка призначається для здійснення захисту критично важливих інтересів держави, суспільства та кожної людини, забезпечення конкурентоздатного, прогресивного розвитку.

Найсерйознішими загрозами національним інтересам і національній безпеці України у сфері інформаційної безпеки визначено:

- Здійснення російською федерацією націлених на ослаблення Української держави спеціальних інформаційних кампаній як на її території, так і за кордоном;
  - інформаційна експансія;
  - інформаційний контроль на тимчасово окупованих територіях;
  - неналежний рівень розвитку національної інформаційної інфраструктури, це обмежує українські можливості ефективно долати інформаційну агресію;
- недієвість сучасної інформаційної політики нашої країни, не розвиненість українського законодавства у сфері регулювання суспільних відносин у інформаційній сфері, невідповідний рівень розвиток суспільної медіакультури [48, с. 64–65].

Якщо посилатися на офіційну Доктрину інформаційної безпеки нашої країни, в якій під інформаційною безпекою мається на увазі рівень захищеності

українських національних інтересів у інформаційній сфері, який визначається сукупністю узгоджених інтересів держави, суспільства та кожного громадянина, то можна зробити підсумок, що ключовим напрямком політики держави щодо забезпечення інформаційної безпеки є дотримання конституційних прав та свобод будь-якої людини у інформаційній сфері [65].

Інформаційна загроза - це будь-яка подія, дія або стан, що потенційно може призвести до порушення інформаційної безпеки, тобто до втрати конфіденційності, цілісності або доступності інформації. Іншими словами, це все, що може зашкодити нашим даним, системам і послугам, які на них базуються [5].

Метою доктрини визначено конкретизацію засад розвитку й втілення державної інформаційної політики, у першу чергу, стосовно подолання деструктивного інформаційного впливу РФ в умовах гібридної війни [65].

Доктрина також визначає українські національні інтереси у інформаційній сфері, перешкоди на шляху їх реалізації, основні напрямки, пріоритети національної політики у даній сфері [665, С. 346].

Згідно із положеннями «Доктрини інформаційної безпеки» від 2017 р. нашої країни, потенційними загрозами українським інтересам і національній безпеці у інформаційній сфері є:

- здійснення спеціальних інформаційних кампаній, націлених на підрив обороноспроможності, деморалізацію у лавах ЗСУ й інших військових підрозділах, сприяння екстремістським проявам, посилення панічних настроїв серед населення, дестабілізацію соціально-політичної й соціально-економічної обстановки в країні, розпалювання міжрелігійної та міжетнічної ворожнечі;
- країна-агресор здійснює спеціальні інформаційні кампанії також на території інших країн для того, щоб створити негативний імідж Української держави у світі;
- інформаційна експансія держави-агресора і підконтрольних їй військових структур, зокрема через розвиток власної інформаційної інфраструктури на українській території і території інших держав;

- інформаційний контроль країни-агресора на тимчасово окупованих територіях;
- невідповідний розвиток державної інформаційної інфраструктури, що нівелює спроможність нашої країни дієво реагувати на інформаційні напади та правильно діяти у інформаційному полі з метою втілення українських національних інтересів;

недоцільність поточної національної інформаційної політики, недосконалість законів, що здійснюють регулювання суспільних відносин у сфері інформаційної безпеки [5].

В одній із публікацій Державного департаменту США стосовно щодо російської дезінформації розкривається механізм функціонування пропагандистської машини рф. У цій статті російську пропагандистську систему пропонується розглядати в якості певної екосистеми, тобто як складну багаторівневу структуру, здатну до відновлення, саморегуляцій і розростання[14].

Окрім п'яти стовпів російської дезінформації (глобальна інформаційна служба за кошти державного бюджету, офіційна комунікація влади рф, проксі-ресурси, кібердезінформація, соціальні мережі), значного поширення набули утворені на пострадянському просторі структури впливу на свідомість населення. Наприклад, РПЦ МП є однією із найпотужніших організацій впливу рф в Україні, поряд із афілійованими росією політичними угрупованнями (наприклад, партія ОПЗЖ), багатьма громадськими організаціями (наприклад, «Россотрудничество») й агентурою впливу, які діють на українській території. Цей вплив, спрямований насамперед на українське населення, а також на державні та недержавні структури у політичній, економічній, соціальній та інших сферах суспільного життя, розповсюджується російською стороною не тільки в Україні, але по всьому пострадянському просторі і за його межами [30, С. 270].

Згідно з дослідженням американського експерта Діаса Руїса, Карлоса «Дезінформація на платформах цифрових медіа: підхід до формування ринку»

(2023 р.), опублікованою у виданні «Нью Медіа енд Сисаєті» (NewMedia&Society), дезінформація розповсюджується у соціальних мережах через обманні кампанії, втілені декількома способами, насамперед через теорії змови, астротурфінг, культуру війни, клік-бейт, містифікації, ехокамери, пропаганду, фейкові новини, чутки та псевдонауку [37].

Також до потенційних загроз національній безпеці нашої країни у інформаційній сфері можна віднести:

- прояви обмеження свободи слова та доступу громадян до інформації;
- спотворення, викривлення, замовчування, блокування та упереджене висвітлення певної інформації;
- несанкціоноване поширення інформації;
- відверту дезінформацію й пропаганду;
- інформаційну експансію зі сторони інших країн, а також деструктивне інформаційне вторгнення в державний інформаційний простір, коли одні держави із більш потужними інформаційними можливостями розширюють через ЗМІ свій вплив на населення та громадськість менш потужної у сфері інформаційної безпеки держави;
- створення та функціонування у державному інформаційному просторі непідконтрольних інформаційних потоків;
- розповсюдження через ЗМІ культу насильства та жорстокості;
- повільне інтегрування нашої країни до світового інформаційного простору;
- необґрунтованість державної інформаційної політики, а також відсутність відповідної інформаційної інфраструктури;
- створення та поширення дезінформації в Інтернеті [24, С. 30].

Потрібно підкреслити, що проти України зі сторони російської федерації проводиться також й інформаційна війна [24, С. 30].

У 2021 р. набув чинності президентський указ «Про рішення Ради національної безпеки та оборони України від 15 жовтня 2021 р. «Про Стратегію інформаційної безпеки» [58].

Ухвалена Стратегія визначила найбільш актуальні загрози та виклики українській національній безпеці у інформаційній сфері, завдання та стратегічні цілі, зосереджені на протидію подібним загрозам, засоби захисту права громадян країни на отримання інформації й захист особистих даних [58].

Ключовими напрямками гарантування інформаційної безпеки нашої країни виступають стійкість і взаємодія, для реалізації яких доцільним є здійснення наступних стратегічних цілей:

- боротьба із дезінформацією та інформаційними операціями, спрямованими на ліквідацію української державності, повалення чинної влади, порушення суверенітету та територіальної єдності країни, воєнну пропаганду, пропаганду насильств та жорстокості, розпалювання національної, расової, міжетнічної, релігійної ненависті і ворожнечі, скоєння актів тероризму, порушення прав та свобод людини;
- сприяння всебічному розвитку національної культури й утвердження громадянської ідентичності серед українського населення;
- покращення рівня медіаграмотності і медіа-культури українського суспільства. Наше суспільство повинне бути захищеним від шкідливого впливу дезінформації і маніпуляцій, а вітчизняне медіа-середовище – повинно бути соціально відповідальним і стабільно функціонувати;
- контроль за дотриманням прав кожного громадянина на збирання, використання, зберігання й розповсюдження інформації, свободу волевиявлення і переконань, захист особистого життя, доступ до правдивої й достовірної інформації, а також гарантування захисту прав журналістів, забезпечення їх безпеки у процесі виконання службових обов’язків, боротьба із поширенням незаконного контенту;
- інформаційна реінтеграція українських громадян, які мешкають на тимчасово окупованих територіях, а також на прилеглих до них територіях, до

загальноукраїнського інформаційного простору, відновлення їхнього права на отримання інформації, що створює для них можливість підтримувати зв'язок із країною;

- вироблення дієвої системи стратегічних комунікацій;
- побудова інформаційного суспільства і покращення рівня культурного діалогу [58].

Російська інформаційна агресія проти України являє собою складну, багатошарову систему маніпулятивних впливів, спрямованих на дестабілізацію суспільно-політичної ситуації та руйнування національної безпеки [52, с. 1-2]. Зокрема, російські «ботоферми» створюють потужні інформаційні потоки, які цілеспрямовано поширюють дезінформацію про українських захисників, спотворюючи суспільну думку та намагаючись підірвати моральний дух населення [56, с. 1-3]. Особливо небезпечним інструментом впливу є поширення фейкових новин, які не лише маніпулюють емоційним станом аудиторії, але й формують викривлену картину реальності, що створює передумови для маніпулятивного впливу на підсвідомість людини [21, с. 636-641]. Російська пропаганда активно використовує технології створення так званих «інформаційних бульбашок», котрі обмежують доступ громадян до альтернативних джерел інформації та поглиблюють когнітивний дисонанс. Крім того, держава-агресор системно впроваджує наративи, спрямовані на дискредитацію України на міжнародній арені, використовуючи складні психологічні механізми впливу на масову свідомість [19, с. 34-41]. Такі інформаційні атаки становлять реальну загрозу національній безпеці, оскільки вони підривають не лише інформаційний суверенітет, але й створюють передумови для маніпулятивного конструювання суспільних настроїв.

Інформаційні платформи й соціальні мережі у сучасному світі відіграють неостанню роль у розповсюдженні як об'єктивної інформації, так і дезінформації й пропаганди. Засобами у цьому процесі виступають:

- алгоритмічна фільтрація й персоналізація контенту;
- поширення «вірусного» контенту;



- ботоферми і фейкові акаунти;
- спрямування на цільову аудиторію.

Значна кількість інформаційних платформ застосовують алгоритми, які здійснюють аналіз даних користувачів і продукують персоналізований контент. Наслідком цього може стати виникнення «інформаційних бульбашок», в яких користувачі отримують тільки інформацію, яка підтверджує їхні переконання, уникаючи альтернативних точок зору.

Інформаційні бульбашки –це наслідок персоналізованого пошуку, коли пошуковий алгоритм видає користувачу результати виходячи із його попередніх дій у мережі. Якщо користувач захоче віднайти інформацію на суперечливу тему, то алгоритм видаватиме у першу чергу ту інформацію, яка відповідатиме його колу спілкування та вподобанням.

Особам в інформаційній бульбашці стає все важче сприймати альтернативні погляди. Таким людям важко погоджуватися з тим, що не співпадає з їхньою позицією. Перша їх реакція – відстоювання своїх поглядів. Така інформаційна ізоляція посилює наше незнання щодо певних подій, речей, поглядів і процесів. Вона може спричинити суспільний розкол та, навіть, утвердження екстремістських поглядів [65].

Соціальними мережами можна доволі швидко поширювати інформацію через своїх колег та друзів, а хибний контент може за короткий час стати вірусним й розповсюдитися серед багатьох користувачів. Тому, оскільки сьогодні технології соціальних мереж активно застосовуються для обміну інформацією і вони стають основою для розповсюдження фейків, особливо важливими стають індикатори правдивості інформації, які можуть бути унікальними для певної соціальної мережі, зокрема, це відноситься до самої інформації, а також її автора [22, С. 75].

Наштовхуючись на невеликі вірусні відеоролики люди можуть подумати, що вони є реальними, а не інсценованими. Наприклад, у грудні 2023 р. у мережі розповсюдилось відео із пораненим військовим, який начебто впав та розсипав фрукти на дорогу. Далі було показано, як частину фруктів переїхало

авто, а решту підбрала собі перехожа. І тільки продавчиня, лоток якої знаходився поруч, відреагувала на ситуацію – безкоштовно підготувала для військового повний пакет нових фруктів й овочів. Описані події начебто відбувалися в Оболонському р-ні м. Києва, неподалік від ТРЦ «DreamTown». Втім, насправді це була інсценована постановка. Логотип на відеоролику підтверджує те, що його створила кіпрська компанія «Фабіуса Медіа», яка займається продукуванням аналогічного контенту у багатьох країнах світу [36, с. 58].

Питання російських ботоферм в українському інформаційному просторі досліджено у джерелі [24], яке розкриває механізми їхньої деструктивної діяльності. Зокрема, російські «ботоферми» створюють розгалужену мережу штучно зареєстрованих акаунтів у соціальних мережах Facebook, Twitter, Telegram, Instagram, які цілеспрямовано поширюють дезінформаційні меседжі про перебіг воєнних дій, соціально-політичну ситуацію в Україні та намагаються маніпулювати суспільною думкою [19, с. 34-41].

Основні стратегії таких ботоферм включають:

- Автоматизоване масове коментування та лайкання контенту.
- Поширення фейкових новин про українських військових.
- Дискредитацію України на міжнародній арені.
- Створення штучного інформаційного шуму.

Штучно зареєстровані акаунти можуть застосовуватися для автоматизованого поширення дезінформації. Такі боти можуть лайкати, ретвітити чи коментувати конкретний контент для того, щоб зробити його вірусним або донести його до більшої обширної аудиторії. Як приклад, можна навести відому російську ботоферму – «Агентство інтернет-досліджень», яке відіграло чималу роль у маніпулюванні думкою американських громадян під час проведення президентських виборів у Сполучених Штатах у 2016 р. і яке фактично допомогло Д. Трампу стати президентом. Особливістю «Агентства інтернет-досліджень» є величезний штат співробітників, які цілодобово генерують дезінформаційний контент, використовуючи складні алгоритми

таргетування та психологічного впливу [14, с. 45-47]. Їхня мета - не просто поширити неправдиву інформацію, а створити альтернативну реальність, що підриває інформаційний суверенітет України [21, с. 636-641].

Від початку повномасштабного вторгнення РФ СБУ вдалося розкрити та знешкодити понад 10 ботоферм, які діяли у різних українських містах – зокрема, у Києві, Львові, Одесі та Запоріжжі. Найбільшою виявилася ботоферма у м. Запоріжжя, яка утримувала більше 70 тис. фейкових акаунтів і понад 50 інтернет-спільнот у різних соцмережах, які розповсюджували проросійські меседжі чи дезінформацію.

Також за допомогою рекламних інструментів таких платформ як Фейсбук чи Гугл, можна навмисно розповсюджувати дезінформацію серед конкретної цільової аудиторії, враховуючи детальну інформацію щодо їхніх інтересів і поглядів.

Соціальні мережі, наприклад, Фейсбук, Телеграм, Інстаграм тощо, відіграють неостанню роль у сучасному інформаційному просторі. Вони є не тільки платформами для спілкування і розваг, але й також є потужними інструментами для поширення й обміну інформацією. Проте, поряд зі значною кількістю переваг, соціальні мережі можуть містити у собі певні ризики такі як розповсюдження фальшивої і маніпулятивної інформації.

Соціальні мережі також використовують для здійснення організованих інформаційних кампаній, де тролі (акаунти, створені реальними особами з метою здійснення маніпуляцій) та боти (штучні акаунти) активно розповсюджують конкретну інформацію чи дезінформацію.

Наступною тактикою, якою часто користуються у соціальних мережах для поширення дезінформації, постає штучне підсилення певних меседжів через системи репостів, лайків і коментарів. Це може сформувати ілюзорну популярність певних думок чи ідей [67, с.112].

У умовах постійно змінюваної глобальної ситуації інформаційна безпека набуває все більшої значущості. Це особливо актуально для України, де інформаційні загрози є частиною гібридної війни, розв'язаної Росією. Загроза

дезінформації стала основним елементом сучасного військового конфлікту, де маніпуляція інформацією має не менше значення, ніж фізичні військові операції. Сучасні технології дозволяють здійснювати інформаційні атаки на держави, спрямовані на підрив їхнього суверенітету, ослаблення внутрішньої стабільності та зниження морального духу нації.

Зокрема, національні загрози, пов'язані з інформаційною безпекою, можна розглядати через призму дезінформаційних кампаній, які активно використовуються агресором для підриву соціально-політичної ситуації в Україні. Зокрема, на основі соціальних мереж і месенджерів здійснюється масове розповсюдження неправдивої інформації, що створює ілюзію реальності, в якій не відображаються істинні події. Використання «ботоферм» і фейкових акаунтів дозволяє Росії маніпулювати суспільною думкою, створюючи інформаційні бульбашки, де кожен користувач отримує тільки ту інформацію, яка підтверджує його власні переконання. Це призводить до глибокого розколу в суспільстві, посилюючи поляризацію та виникнення екстремістських поглядів.

Не менш небезпечним є використання пропаганди для посилення інформаційного контролю на окупованих територіях, де вона сприяє дестабілізації та деморалізації населення. У цьому контексті також виникають проблеми щодо розвитку національної інформаційної інфраструктури, яка є необхідною для ефективного реагування на зовнішні інформаційні атаки. У цих умовах особливу увагу варто звернути на необхідність удосконалення законодавства, яке забезпечує інформаційну безпеку, а також на розвиток медіаграмотності серед населення, що є важливим інструментом у боротьбі з дезінформацією.

Метою стратегії інформаційної безпеки України є не лише захист національних інтересів у інформаційній сфері, але й відновлення права громадян на доступ до правдивої і об'єктивної інформації, що є основою для підтримки демократії та стабільності в країні. Водночас важливо враховувати, що ефективне протидія інформаційним загрозам потребує комплексного підходу, що включає як державні інститути, так і активну участь громадянського

суспільства. Зокрема, стратегічні комунікації, спрямовані на розвиток національної ідентичності, підвищення рівня медіаграмотності, а також реінтеграція населення з тимчасово окупованих територій в єдиний інформаційний простір України, є ключовими елементами цієї стратегії.

Отже, на тлі війни і гібридних загроз, дезінформація стає не лише інструментом психологічного впливу, але й суттєвим викликом для національної безпеки. Необхідно постійно удосконалювати механізми протидії цим загрозам, як на державному рівні, так і в межах суспільства в цілому. Важливим є також розуміння природи і механізмів дезінформації, що дозволяє ефективно ідентифікувати її прояви та запобігати маніпуляціям.

## **2.2. Нормативно-правове регулювання захисту національного інформаційного простору**

На фоні російсько-українського протистояння у 2014 р. почало формуватися нове законодавство у цій сфері. У відповідності із ст. 17 української Конституції, гарантія інформаційної безпеки є однією із найважливіших функцій країни поряд із відстоюванням територіальної цілісності та суверенності [1].

26 квітня 2014 р., із анексією росією Кримського півострова та початком її військової агресії на сході України, було прийнято розпорядження «Про деякі заходи щодо забезпечення безпеки у інформаційній сфері», згідно з яким СБУ було доручено гарантувати безпеку представникам ЗМІ, а МВС – забезпечувати безперервну трансляцію національного аудіовізуального контенту у південно-східних областях України, а також забезпечувати на цій території оборону об'єктів наземної радіотелевізійної мережі [8].

У зв'язку із посиленням російської пропаганди, спрямованої на маніпулювання свідомістю українського населення, було ухвалено Рішення РНБО України «Про заходи щодо вдосконалення формування і реалізації державної політики в сфері інформаційної безпеки України» (28.04. 2014 р.).

Як наслідок, було впроваджено зміни до певних законів стосовно протидії інформаційній агресії, вироблено механізм протидії негативному інформаційно-

психологічному впливу. Цей нормативно-правовий документ також передбачав створення стратегії кібербезпеки та сприяння розвитку інформаційного простору [10].

До цього всього, було внесено зміни у наступні законопроекти: «Про інформацію» [5], «Про основи національної безпеки України» [6], «Про Державну службу спеціального зв'язку та захисту інформації України» [4]. Відтепер вони мали відповідати міжнародним стандартам щодо питань інформаційної й кібернетичної безпеки, а також вдосконалити державну політику у сфері інформаційної безпеки.

У 2016 р. РНБО України було прийнято Доктрину інформаційної безпеки, юридичною основою якої стала Стратегія національної безпеки України, затвердженої відповідним президентським указом від 26 травня 2015 р. Метою цієї Доктрини стало вироблення основ формування і реалізації державної політики у сфері інформаційної безпеки, насамперед стосовно протидії інформаційному впливу РФ в умовах розпочатої нею гібридної війни [65].

Загрозами національним інтересам і безпеці України у доктрині визначаються дії країни-агресора (росії), зокрема проведення спеціальних інформаційних кампаній, націлених на деморалізацію у лавах ЗСУ, підлив обороноспроможності країни, сприяння екстремістським проявам, появі панічних настроїв серед українського населення, дестабілізацію внутрішньополітичної ситуації й формування негативного образу України в світі. До того ж, у якості загроз також зазначались інформаційне переважання країни-агресора на тимчасово окупованих територіях, нерозвиненість державної інформаційної інфраструктури, недоцільність національної інформаційної політики, недоліки законодавства у цій сфері, поширення пропаганди сепаратизму у українських регіонах [33, с. 26-27].

Згідно з Доктриною, до національних інтересів інформаційної політики України належать:

- формування системи реагування й оцінювання інформаційних загроз;

- конкретизація повноважень державних органів регулювання інформаційної безпеки та забезпечення захищеності населення від інформаційно-психологічних маніпуляцій;
- гарантування захисту українського суспільства від інформаційного впливу і дестабілізуючої ворожої пропаганди [33, с. 26-27].

Одним із пріоритетних напрямів діяльності української системи національної безпеки, а також важливою складовою стійкого інформаційного простору, є також зміцнення кібербезпеки.

У 2016 р. президентським указом було прийнято «Стратегію кібербезпеки України», що стало суттєвим рішенням стосовно впровадження довгострокового планування у даній сфері. За період реалізації цієї Стратегії було докладено чимало зусиль для встановлення і розвитку державної системи кібербезпеки. Важливим етапом інституалізації системи кібербезпеки в Україні стало ухвалення у 2017 р. закону «Про основні засади забезпечення кібербезпеки України», в якому було визначено її об'єкти, суб'єкти, ключові принципи. Законом також встановлено правові й організаційні основи гарантування захисту критично важливих інтересів держави, суспільства та кожного громадянина, українських національних інтересів у кіберпросторі, головні напрями, цілі й принципи державної політики у галузі кібербезпеки, повноваження державних структур, установ, підприємств, організацій, конкретних осіб і громадян у цій сфері, основні принципи організації їхньої діяльності щодо забезпечення кібербезпеки [18; 11].

Окрім Доктрини також було ухвалено й інші законодавчі акти. Зокрема, для збільшення ефективності протидії російській дезінформації та пропаганді було прийнято Президентський указ «Про рішення РНБО України від 26 січня 2018 р. «Про додаткові заходи щодо протидії інформаційній агресії російської федерації» [10]. Зміст цього документа доступний тільки для службового користування. Метою та завданням даного указує додаткові заходи, спрямовані на протидію російській дезінформації [19, с. 139;].

Нормативне регулювання інформаційної безпеки та кібербезпеки передбачають Конституція України, українські закони, президентські укази та постанови ВРУ та КМУ. У 2021 р. було вироблено оновлену стратегію інформаційної безпеки. Однією із актуальних загроз, як і раніше, визначалася інформаційна політика росії. Головними викликами визначено:

- інформаційний вплив російської пропаганди на українське населення;
- переважання російського інформаційного впливу на тимчасово окупованих українських територіях;
- обмежені можливості України у протистоянні російським дезінформаційним кампаніям [58].

Ключовою загрозою для Української держави, згідно із Стратегією кібербезпеки України, прийнятою президентським указом від 14 травня 2021 р., постає гібридна війна рф проти України в кіберпросторі.

Відповідно, основними напрямками забезпечення української кібербезпеки постають:

- створення кіберпростору для відстоювання суверенітету України й розвитку українського суспільства;
- гарантування прав та законних інтересів українських громадян у кіберпросторі;
- європейська та євроатлантична інтеграція в галузі кібербезпеки [6, с. 8-9].

Стратегія інформаційної безпеки була законодавчо зафіксована у президентському указі «Про рішення РНБО України від 15 жовтня 2021 р. «Про Стратегію інформаційної безпеки». Згідно із цим указом, інформаційна безпека України є невід'ємною частиною національної безпеки країни та має безпосередній вплив на рівень захищеності конституційного ладу, територіальної цілісності, державного суверенітету та інших критично важливих інтересів держави, суспільства та кожного громадянина. Також у документі підкреслюється, що інформаційною безпекою є гарантування конституційних



прав населення на вільне користування інформацією, доступ до неї та її захист. Захист інформації передбачає протидію дезінформації, пропаганді і ворожим інформаційним кампаніям, а також забезпечення безпеки для носіїв інформації [58].

Важливим нормативним документом у протидії деструктивним інформаційним впливам став ЗУ «Про внесення змін до деяких законів України щодо заборони виготовлення і поширення інформаційної продукції, націленої на пропагування дій країни-агресора» 2022 р. Згідно із цим документом, в Україні було заборонено виправдання російської агресії і прославлення російських військ, визначення російсько-української війни як громадянського конфлікту [2].

У відповідності із президентським указом «Про рішення РНБО України від 18 березня 2022 р. «Щодо реалізації єдиної інформаційної політики в умовах воєнного стану», частину загальнонаціональних телеканалів були в цілодобовому інформаційному марафоні «Єдині новини #UA разом», під час якого в інформаційних та інформаційно-аналітичних передачах роз'яснюється об'єктивна інформація щодо розгортання російсько-української війни [12].

Постановою ВРУ» Про прийняття за основу проєкту Закону України про внесення змін до Закону України «Про Державну службу спеціального зв'язку і захисту інформації України» було відзначено важливість забезпечення втілення державної політики у сфері кібербезпеки [3].

При державній службі спеціального зв'язку і захисту інформації діяв також урядовий фельд'єгерський зв'язок. До його повноважень входило прийняття, оброблення й доставка кореспонденції, яка містить таємну інформацію або інформацію, призначену тільки для службового користування. Оскільки такі документи передавались через кур'єра, що було доволі ненадійним способом передачі інформації, до законодавства було внесено відповідні зміни [4].

В умовах війни значну технічну, фінансову та консультативну допомогу надає Україні НАТО. Зокрема для того, щоб нормативно врегулювати процес формування і процедуру акредитації безпеки інформаційно-комунікаційних систем, створених для здійснення обробки і передачі інформації НАТО із

обмеженим доступом використовуються різні нормативні документи НАТО і військові стандарти України, перелічені у наказі Державної служби спеціального зв'язку і захисту інформації України [9]. У сфері інформаційної безпеки співпраця України з НАТО набуває особливої значущості, особливо в умовах воєнного часу. Альянс надає комплексну підтримку, яка виходить далеко за межі традиційної технічної допомоги.

Зокрема, НАТО активно сприяє вдосконаленню систем захисту інформації в українських державних структурах. Ключовим аспектом такої співпраці є впровадження стандартизованих підходів до забезпечення інформаційної безпеки, гармонізація вітчизняних нормативних документів з міжнародними стандартами альянсу.

Державна служба спеціального зв'язку і захисту інформації України послідовно імплементує механізми акредитації безпеки інформаційно-комунікаційних систем, використовуючи найкращі практики НАТО. Це включає:

1. Адаптацію військових стандартів України
2. Впровадження уніфікованих процедур захисту інформації з обмеженим доступом
3. Розвиток спеціалізованих методик технічного захисту інформаційних систем

Поступальний рух у цьому напрямку демонструє глибоку інтеграцію України до європейської системи кібербезпеки та інформаційного захисту, що є важливим кроком на шляху до повноправного членства в НАТО.

Таким чином, російська федерація досі залишається однією із основних загроз національній і насамперед інформаційній безпеці нашої країни. Країна-агресор постійно здійснює атаки на український інформаційний простір. Дії росії ґрунтуються на комбінації дестабілізуючих дій у кіберпросторі й інформаційно-психологічних кампаніях, які доповнюють військову агресію, здійснюючи вплив на морально-психологічний стан українського населення і діяльність інформаційно-комунікаційних мереж України.

Російсько-українське протистояння стало потужним рушієм змін в українському законодавстві. Об'єктами атак ворога стали інформаційно-комунікаційна система й свідомість українських громадян. Нові реалії цілком змінили державну політику України у сфері інформаційної безпеки. Від 2014 р. було чітко визначено головні загрози й виклики зі сторони російської федерації. Також було вироблено стратегію інформаційної безпеки країни, втілення якої заплановане до 2025 р. та становить частину української національної безпеки.

Окрім цього, було створено стратегію кібербезпеки і проводиться масштабна робота у напрямку виявлення і протидії кіберзагрозам. Вдосконалено і внесено зміни в українське законодавство стосовно регулювання інформаційної безпеки у різних сферах суспільного життя. Втім, важливою досі залишається реалізація усієї нормативно-правової бази. Діючи у цьому напрямку, можна буде значною мірою зміцнити українські позиції в інформаційному просторі та кіберпросторі.

### **2.3. Діяльність державних інститутів у протидії деструктивним інформаційним впливам**

В умовах кардинальних суспільних зрушень та становлення спільного міжнародного інформаційного простору, інформаційна безпека стає головним компонентом всієї системи національної безпеки нашої країни, оскільки інформаційно-комунікаційні технології «за своїм впливом на політику, духовно-ідеологічну сферу, господарсько-економічне життя і настрої населення стали всеохоплюючими та вирішальними» [33, с. 25]. Державні інститути відіграють вагомую роль у протидії інформаційним небезпекам, таким як кібератаки, пропаганда, дезінформація й інші способи маніпулювання інформацією.

Важливою інституцією виступає центр протидії дезінформації при РНБО України, який відіграє чималу роль у протидії дезінформації та інформаційним загрозам національній безпеці країни. Це є робочий орган РНБО України,

створений згідно з відповідним рішенням РНБО України від 11 березня 2021 р. «Про створення Центру протидії дезінформації»[7].

Центр протидії дезінформації забезпечує проведення заходів стосовно протидії актуальним та потенційним загрозам національній безпеці й українським національним інтересам у інформаційній сфері, виявлення й боротьби з дезінформацією, пропагандою, дестабілізуючими інформаційними чинниками й кампаніями, запобігання спробам маніпуляцій громадською думкою [67, с. 156].

Головними завданнями Центру протидії дезінформації є:

1) здійснення аналізу й моніторингу подій та явищ в українському інформаційному просторі, становища інформаційної безпеки й присутності Української держави у міжнародному інформаційному просторі;

2) виявлення й вивчення існуючих та можливих загроз інформаційній безпеці, факторів, які мають вплив на їх виникнення, прогнозування, а також оцінювання наслідків для безпеки українських національних інтересів;

3) надання РНБО України, Голові РНБО України інформаційно-аналітичних матеріалів щодо питань забезпечення інформаційної безпеки в Україні, фіксації та боротьби з дезінформацією, пропагандою, деструктивними чинниками та інформаційними кампаніями;

4) підготовка і внесення РНБО України, Голові РНБО України відповідних пропозицій;

5) участь у процесі формування системи стратегічних комунікацій, організації і координуванні заходів стосовно її розвитку;

6) участь у процесі розроблення та втілення Стратегії інформаційної безпеки України, проведення аналізу стану її реалізації, насамперед щодо питань ефективності заходів стосовно боротьби із дезінформацією;

7) участь у процесі створення інтегрованої системи оцінювання інформаційних загроз й відповідного оперативного реагування;

8) вироблення методології виявлення небезпечних інформаційних матеріалів дезінформаційного й маніпулятивного характеру;

9) налагодження взаємодії держави й інститутів громадянського суспільства стосовно боротьби із дезінформацією й деструктивним чинниками, організація й участь у інформаційно-просвітницьких заходах щодо питань покращення рівня медіа-грамотності нашого суспільства;

10) дослідження, узагальнення та належний аналіз досвіду зарубіжних держав та міжнародних організацій щодо протидії дезінформації, а також підготування пропозицій стосовно його застосування в українських реаліях;

11) участь у залученні міжнародної технічної допомоги щодо питань гарантування інформаційної безпеки, фіксації і протидії дезінформації, пропаганді, дестабілізуючим інформаційним впливам та кампаніям, запобігання маніпулюванню громадською думкою [14, с. 16].

Центр протидії дезінформації при Раді національної безпеки і оборони України постає як надзвичайно важливий інституційний механізм забезпечення інформаційної безпеки держави в умовах гібридної війни. Він очолює Анатолій Баринів - професійний фахівець у сфері стратегічних комунікацій та інформаційної безпеки, який має значний досвід роботи в державних структурах і глибоке розуміння викликів інформаційного простору. Діяльність Центру характеризується комплексним підходом до протидії інформаційним загрозам. Основний фокус спрямований на системний моніторинг українського та міжнародного інформаційних просторів, виявлення деструктивних наративів, маніпулятивних впливів і потенційних загроз національним інтересам України. Центр активно впроваджує інноваційні методики аналізу інформаційних потоків, зокрема використовуючи сучасні технології штучного інтелекту та автоматизованого контент-аналізу. Важливим напрямком є не лише фіксація та нейтралізація дезінформації, але й випередження потенційних інформаційних атак.

Основні проекти Центру - створення онлайн-платформ для швидкого реагування на поширення неправдивої інформації, розроблення методичних рекомендацій для журналістів та громадських активістів щодо протидії пропаганді, організація освітніх програм з медіаграмотності.

Центр тісно співпрацює з міжнародними організаціями, зокрема з інституціями ЄС та НАТО, обмінюючись досвідом та напрацюваннями у сфері стратегічних комунікацій. Особлива увага приділяється вивченню та адаптації кращих світових практик протидії інформаційним маніпуляціям.

Аналіз публікацій та звітів Центру протидії дезінформації демонструє його системну роботу з виявлення та нейтралізації деструктивних інформаційних впливів. Центр не лише фіксує факти дезінформації, але й проводить глибокий аналіз витоків, механізмів поширення та потенційних наслідків інформаційних атак.

Важливим аспектом діяльності є налагодження взаємодії між державними інституціями, медіа та громадянським суспільством для створення ефективної системи протидії інформаційним загрозам. Центр виступає координаційним осередком, який забезпечує комунікацію та взаємодію різних суб'єктів інформаційного простору.

Водночас, важливу роль у забезпеченні стабільності національної інформаційної сфери відіграє Центр стратегічних комунікацій, створений при Міністерстві культури та інформаційної політики України. Його основна мета полягає в координації дій держави та громадських ініціатив у боротьбі з інформаційними загрозами, розробці стратегічних комунікаційних кампаній, які спрямовані на зміцнення внутрішнього фронту та захист від інформаційних атак ззовні. Окрім цього, центр займається поширенням правдивої та перевіреної інформації серед громадян, щоб попередити дезінформаційні впливи і сформувати стійкість до маніпуляцій.

Український уряд постійно працює над удосконаленням кібербезпеки життєво важливих інформаційних систем й інфраструктури нашої держави, насамперед державних мереж, банківських систем та енергетичної інфраструктури. Захист інформаційного простору й кіберпростору здійснює Ситуаційний центр забезпечення кібербезпеки СБУ. перші регіональні центри забезпечення кібербезпеки СБУ були створені в 2018 році (Дніпро) та 2019 році (Одеса). Це свідчить про те, що централізована структура, ймовірно, була

створена раніше. Україна активно співпрацює з міжнародними партнерами в галузі кібербезпеки, зокрема з НАТО. Ця співпраця могла стимулювати створення та розвиток Ситуаційного центру.

Пріоритетними завданнями цього напрямку діяльності спецслужби виступають:

- боротьба із кібертероризмом та кібершпигунством;
- розслідування кіберінцидентів та кібератак на державні цифрові інформаційні ресурси;
- боротьба зі здійсненням ворожих інформаційних кампаній.

Відстоюючи інформаційний простір своєї країни кіберфахівці СБУ блокують діяльність десятків ботоферм, численних антиукраїнських ютуб-каналів. Було викрито й притягнуто до кримінальної відповідальності сотні інтернет-агітаторів, які розповсюджували російські фейки і наративи.

Наявні ресурси дають можливість Україні не лише відбивати кібератаки й блокувати дестабілізуючу діяльність у інформаційному просторі, але й також атакувати противника.

Таблиця 1.

Загальна статистика кібератак (2022-2024)

| Рік          | Кількість зафіксованих атак | Критичні інциденти | Успішно відбиті (%) |
|--------------|-----------------------------|--------------------|---------------------|
| 2022         | 2,194                       | 362                | 83%                 |
| 2023         | 4,276                       | 436                | 86%                 |
| 2024 (I кв.) | 1,654                       | 178                | 89%                 |

Аналіз першої таблиці демонструє стрімке зростання кількості кібератак – майже вдвічі з 2022 по 2023 рік (з 2,194 до 4,276). Особливо показовим є перший квартал 2024 року, де вже зафіксовано 1,654 атаки, що свідчить про можливе перевищення показників попереднього року. Позитивною тенденцією є поступове підвищення відсотку успішно відбитих атак з 83% до 89%, що вказує

на вдосконалення систем захисту та підвищення ефективності реагування на кіберзагрози [12].

Розподіл за типами атак у 2023 році виявляє домінування DDoS-атак (38%), що пояснюється їх відносною простотою реалізації та високим дестабілізуючим потенціалом. Фішингові атаки (24%) та шкідливе програмне забезпечення (21%) формують другий ешелон загроз, становлячи разом 45% від загального обсягу. Особливу увагу привертає той факт, що найбільш небезпечними визнані саме шкідливе ПЗ та фішинг, які мають «критичний» та «високий» рівні загрози відповідно[12].

Таблиця 2

Розподіл за типами атак (2023)

| Тип атаки                       | Відсоток | Рівень загрози |
|---------------------------------|----------|----------------|
| DDoS-атаки                      | 38%      | Середній       |
| Фішинг                          | 24%      | Високий        |
| Шкідливе ПЗ                     | 21%      | Критичний      |
| Компрометація облікових записів | 9%       | Високий        |
| Веб-атаки                       | 5%       | Середній       |
| Інші                            | 3%       | Різний         |

Аналіз цільових секторів демонструє чітку концентрацію атак на державному секторі (34%) та об'єктах критичної інфраструктури (28%), що разом становить 62% усіх атак. Примітним є співвідношення часу виявлення та реагування – найшвидше реагування спостерігається в секторі критичної інфраструктури (1.5/2 години), тоді як приватний бізнес демонструє найповільніші показники (4/6 годин) [12]..

Таблиця 3.

Основні цілі кібератак (2023-2024)



| Сектор                  | Частка атак | Середній час виявлення (год) | Середній час реагування (год) |
|-------------------------|-------------|------------------------------|-------------------------------|
| Державний сектор        | 34%         | 2.5                          | 4                             |
| Критична інфраструктура | 28%         | 1.5                          | 2                             |
| Банківський сектор      | 17%         | 2                            | 3                             |
| Телекомунікації         | 12%         | 3                            | 5                             |
| Приватний бізнес        | 9%          | 4                            | 6                             |

На основі проаналізованих даних можна виділити основні проблеми у сфері кібербезпеки України. Постійне вдосконалення методів та інструментів кібератак вимагає безперервної модернізації систем захисту та підвищення кваліфікації фахівців з кібербезпеки. Застарілість технічної інфраструктури багатьох організацій створює додаткові вразливості для потенційних атак. Суттєвим викликом залишається недостатнє фінансування заходів кібербезпеки, особливо в державному секторі. Проблема нестачі кваліфікованих кадрів у сфері кібербезпеки загострюється через високу конкуренцію на ринку праці та відтік спеціалістів закордон. Недостатня координація між різними відомствами та організаціями ускладнює процес оперативного реагування на кіберзагрози. Низький рівень кіберграмотності користувачів створює додаткові ризики для інформаційної безпеки організацій. Використання застарілого програмного забезпечення та недотримання базових правил кібергігієни залишаються суттєвими факторами ризику. Складність виявлення та протидії новітнім типам кіберзагроз вимагає постійного вдосконалення методів захисту та моніторингу. Відсутність єдиних стандартів та протоколів реагування на кіберінциденти ускладнює процес координації дій різних організацій.

Таблиця 4.

Рівні серйозності кіберінцидентів

| Рівень    | Характеристика               | Час реагування | Частка інцидентів |
|-----------|------------------------------|----------------|-------------------|
| Критичний | Загроза національній безпеці | До 1 години    | 5%                |
| Високий   | Суттєвий вплив на діяльність | До 4 годин     | 15%               |
| Середній  | Обмежений вплив              | До 8 годин     | 35%               |
| Низький   | Мінімальний вплив            | До 24 годин    | 45%               |

Розподіл за рівнями серйозності показує, що більшість інцидентів (80%) належать до середнього та низького рівнів загроз. Проте 20% критичних та високорівневих інцидентів вимагають найбільше ресурсів та уваги. Важливо відзначити встановлення чітких часових рамок реагування – від 1 години для критичних до 24 годин для низькорівневих інцидентів [12].

Таблиця 5.

#### Географія атак (топ-5 джерел, 2023)

| Країна походження | Відсоток атак |
|-------------------|---------------|
| РФ                | 56.4%         |
| Невстановлені     | 21.3%         |
| Китай             | 8.7%          |
| Північна Корея    | 7.2%          |
| Іран              | 6.4%          |

Аналіз географії походження атак демонструє домінування РФ як джерела кібератак (56.4%). Значну частку становлять атаки з невстановленим походженням (21.3%), що вказує на використання складних методів маскування. Помітною є активність країн Азії (Китай, Північна Корея, Іран), які сумарно відповідальні за 22.3% атак [14].

Рекомендації щодо покращення ситуації:

1. Інвестування в модернізацію технічної інфраструктури та систем захисту[6].
2. Розробка та впровадження комплексних програм підготовки фахівців з кібербезпеки[6].
3. Посилення міжвідомчої координації та обміну інформацією.[4]
4. Впровадження регулярних програм підвищення кіберграмотності для всіх категорій користувачів[43]
5. Розробка та впровадження єдиних стандартів кібербезпеки на національному рівні[11]

Також наша країна налагоджує співпрацю із іншими країнами й міжнародними організаціями у галузі кібербезпеки й протидії дезінформації, обмінюючись практичним досвідом і координуючи спільні дії у цьому напрямку.

У статті 14 закону «Про основні засади забезпечення кібербезпеки України» встановлено, що Україна у відповідності із укладеними нею міжнародними домовленостями здійснює співпрацю у галузі кібербезпеки із зарубіжними партнерами, їхніми правоохоронними органами та спецслужбами, а також із міжнародними організаціями, які борються із міжнародною кіберзлочинністю. Інформацію щодо питань, які стосуються боротьби із міжнародною кіберзлочинністю, наша держава надає певній іноземній країні на підставі запиту, дотримуючись вимог українського законодавства та її міжнародно-правових зобов'язань. Подібна інформація може бути надана без попереднього запиту іноземної країни, якщо це не суперечить здійсненню досудового розслідування або судового розгляду справи та може сприяти відповідним органам іноземної країни припинити кібератаки, своєчасно виявити та зупинити кримінальне правопорушення із застосуванням кіберпростору [6].

Співпраця України із іншими країнами світу у сфері гарантування кібербезпеки може проводитись через:

- 1) взаємодію на міжнародному рівні для боротьби із кіберзагрозами та кібератаками;

2) обмін практичним досвідом формування й функціонування національних кібербезпекових систем;

3) вироблення відповідних стандартів кібербезпеки [69, с. 16].

Для запобігання та боротьби з інформаційними викликами в умовах війни українські державні структури здійснюють певні заходи.

По-перше, уряд України постійно вдосконалює законодавство у сфері регулювання інформаційної безпеки. Ухвалення законів про кібербезпеку, захист особистих даних і протидію дезінформації формує правову базу для протидії цим загрозам.

По-друге, Українська держава активно бере участь у міжнародній співпраці у сфері кібербезпеки й інформаційної безпеки. Співпраця із іноземними країнами і міжнародними організаціями дає можливість обмінюватися практичним досвідом, ресурсами й координувати взаємні заходи протидії інформаційним загрозам.

По-третє, державні інститути України концентрують свою увагу на удосконаленні рівня кібербезпеки життєво важливих інформаційних систем й інфраструктури нашої країни. Це включає в себе заходи стосовно захисту державних мереж, енергетичної інфраструктури та банківських систем.

Окрім цього, український уряд активно розвиває власні програми медіаграмотності, націлені на розвиток критичного мислення в українських громадян та розпізнавання дезінформації від правдивої інформації. Це сприяє формуванню міцного суспільства, здатного ефективно виявляти і боротися з інформаційними загрозами.

## Висновки до 2 розділу

Юридичні виміри та інституційні підходи до боротьби з дезінформацією та пропагандою в сучасному світі стають дедалі актуальнішими та важливими в міру того, як змінюється медіа-ландшафт та поширення дезінформації. Правові норми та інституційні механізми в цій сфері спрямовані на гарантування конфіденційності, цілісності та доступності інформації, а також на захист від маніпуляцій і впливу дезінформації та ворожої пропаганди.

Український уряд рішуче відповідає на актуальні виклики дезінформації та пропаганди шляхом розвитку правових та інституційних механізмів протистояння їм. В Україні на законодавчому рівні прийняті закони та підзаконні акти, спрямовані на боротьбу з дезінформацією та пропагандою. У нашій державі діє ряд законів і нормативних документів, які регулюють сферу інформаційної безпеки. Перш за все, це урядові стратегії інформаційної та кібербезпеки, а також спеціальні укази та розпорядження президента. Інституційний підхід також передбачає створення спеціальних інституцій та комітетів для боротьби з дезінформацією та пропагандою. Наприклад, Центр протидії дезінформації при РНБО.

Україна також продовжує співпрацювати з міжнародними партнерами у боротьбі з дезінформацією та пропагандою, наприклад з НАТО.

Загальний підхід передбачає поєднання інституційних, правових та міжнародних механізмів для створення ефективної системи захисту від дезінформації та пропаганди, що, у свою чергу, сприяє розвитку інформаційної безпеки та захисту демократичних цінностей. Громадські організації сьогодні відіграють важливу роль у боротьбі з дезінформацією. Це залежить від їх здатності залучати громадськість, створювати нові джерела інформації та вести просвітницьку роботу.

Співпраця між іноземними державами та громадськими організаціями у боротьбі з дезінформацією є важливою у процесі розробки стратегій та ефективних заходів щодо запобігання цьому явищу.

Урядові та неурядові організації також можуть обмінюватися інформацією про виявлені випадки дезінформації, а також надавати одна одній доступ до ресурсів, які можуть бути корисними для виявлення та боротьби з дезінформацією. Вони можуть об'єднати свої зусилля для реалізації освітніх кампаній щодо медіаграмотності, розвитку критичного мислення та виявлення дезінформації серед громадськості. Крім того, ці установи можуть співпрацювати у розробці та реалізації політичних і законодавчих напрямків, спрямованих на боротьбу з дезінформацією та підвищення рівня безпеки даних. Державні установи можуть співпрацювати з приватним сектором, щоб створювати та впроваджувати інноваційні технології та відповідні інструменти.

### РОЗДІЛ 3

## ПРАКТИЧНИЙ АНАЛІЗ ТА РЕКОМЕНДАЦІЇ ЗАХИСТУ СУЧАСНОГО ІНФОРМАЦІЙНОГО ПРОСТОРУ УКРАЇНИ

### 3.1. Медіаосвіта як інструмент протидії дезінформації та пропаганди в суспільстві

Медіаосвіта стає важливим елементом у сучасному суспільстві, де інформаційні потоки набувають надзвичайної інтенсивності. В умовах глобальної діджиталізації, коли інформація поширюється миттєво і доступ до неї відкритий майже для кожного, виникає загроза поширення дезінформації та пропаганди. Ці негативні явища можуть мати серйозні наслідки для суспільства, впливаючи на громадську думку, політичні процеси та соціальну стабільність [17, с. 33–41; 31, с. 45–52].

Медіаосвіта – це процес навчання, спрямований на розвиток у громадян критичного мислення щодо медіа, навичок аналізу та оцінки медіаконтенту, а також здатності ефективно користуватися медіаресурсами. Медіаосвіта дає можливість людям розпізнавати маніпуляції, фейки та пропаганду, а також формувати свою позицію на основі достовірної інформації [18, с. 89–96; 31, с. 45–52].

Медіаосвіта як засіб протидії дезінформації:

1. Медіаосвіта навчає критично аналізувати інформацію, що надходить з різних джерел. Це дозволяє людям розпізнавати маніпулятивні техніки, які використовуються в дезінформації, і приймати більш обґрунтовані рішення.
2. Одна з ключових навичок, що розвивається завдяки медіаосвіті, – це вміння перевіряти факти. Уміння знаходити першоджерела інформації, аналізувати достовірність і об'єктивність новин є важливим для протидії фейкам.
3. Медіаосвіта допомагає зрозуміти, як створюється новинний контент, як відбирається інформація та які чинники впливають на медіа. Це знання

дозволяє зрозуміти, чому деякі новини можуть бути упередженими або викривленими.

4. Медіаосвіта включає розгляд етичних аспектів роботи з інформацією. Це важливо для формування відповідального ставлення до створення та поширення контенту, а також для розвитку культури обміну правдивою інформацією [36, с. 56–63].

Медіаосвіта як інструмент протидії пропаганді:

1. Медіаосвіта вчить розпізнавати техніки, які використовуються в пропаганді, такі як викривлення фактів, створення фальшивих наративів, використання емоційних тригерів. Це дозволяє критично підходити до інформації і не піддаватися маніпуляціям.

2. Високий рівень медіаграмотності сприяє формуванню у громадян здатності протистояти пропаганді через усвідомлене споживання інформації. Люди, що пройшли медіаосвітні програми, краще розуміють, як працюють медіа, і можуть розпізнавати пропаганду.

3. Пропаганда часто спрямована на нав'язування певних поглядів. Медіаосвіта допомагає людям розвивати здатність до незалежного мислення, формування власної думки та світогляду на основі достовірних і різноманітних джерел інформації [18, с. 89–96].

Медіаосвіта стає потужним інструментом у боротьбі з дезінформацією та пропагандою. Вона сприяє формуванню критичного мислення, підвищенню медіаграмотності та розвитку етичної відповідальності в роботі з інформацією. У сучасному світі, де інформаційні війни стають все більш поширеними, медіаосвіта є ключовим елементом для забезпечення інформаційної безпеки суспільства та збереження демократичних цінностей [38, с. 117–124].

Медіаграмотність стає все важливішою у сучасному світі, де інформаційний потік надзвичайно швидкий і різноманітний. Освітні програми і проєкти є ключовим інструментом у підготовці громадян до розуміння інформації, яку вони споживають, і вони відіграють значну роль у забезпеченні інформаційної безпеки суспільства та медіаграмотності [42, с. 78–85].



На сьогоднішній день, в Україні діє реформа «Нова українська школа», яка передбачає виховання молодого грамотного покоління. Ці діти повинні володіти такими навичками, як:

- Спілкування державною мовою;
- Спілкування іноземними мовами;
- Математичні компетентності;
- Базові компетентності в галузі природничих наук і технологій;
- Інформаційна та цифрова компетентності;
- Можливість продовження навчання;
- Ініціативність та підприємливість;
- Громадянські та соціальні компетентності;
- Поінформованість та самовираження у сфері культури;
- Знання про навколишнє середовище та здоровий спосіб життя [31, с. 45–52].

Слід зазначити, що для всіх цих компетенцій є навички, які включають критичне мислення, уміння конструктивно керувати емоціями, а також уміння раціонально обґрунтовувати позицію. Можна сказати, що ці навички можна отримати, вивчаючи освітні медіа. Для цього розроблено навчальні програми, які дозволяють вивчати медіаосвіту як окремий предмет [35, с. 145–147].

Перша – освітня програма для учнів 8-9 класів, яка включає вивчення основ медіаграмотності. Він був створений в 2017 році. Всередині. Волошник , П . Кваленко та ін. Мукрогоз за підтримки американського проекту USAID. 2017 рік – це час інноваційного розвитку ЗМІ та поширення інформації: створення нових соціальних мереж, популяризація «пабліку» та поступова відмова від телебачення [30, с. 156–158].

Тим не менш, важливість курсу «Основи медіаосвіти» автори програми пояснюють «нагальною потребою студентів у вивченні різноманітних медіа, що стане основою для набуття теоретичних уявлень про медіаосвіту в майбутньому.

. як ефективний спосіб розвитку творчої, незалежної та критично мислячої особистості в умовах різкого збільшення потоку інформації...» [30, с. 156–158].

Метою курсу є формування у студентів основи теоретичних знань з основ медіаосвіти та практичних навичок ефективного та безпечного використання інформації, отриманої з медіаджерел, зокрема використання сучасних інформаційно-комунікаційних технологій у повсякденному житті, практиці, . особливо у підприємницькій та пізнавальній діяльності [30, с. 156–158].

Зокрема, пояснювальна записка містить знання та вміння студентів, які вони отримають після завершення навчання, структуру програми та організацію навчання, а також загальні принципи, на основі яких будуються заняття [ 30, стор. 156–158].

У 2023 році впровадження освітніх послуг у школах здійснюватиметься за допомогою компетентнісного підходу, однак у програмі курсу «Фундація медіаграмотності» в пояснювальній записці є розділ «Компетентнісний потенціал курсу». У ньому детально описано навички та ставлення, вироблені та набуті під час курсу «Основи медіаграмотності». Наступна програма, а саме проведення навчального медіа тренінгу, це часткова програма – для дітей дошкільного віку. За Василюк., о. Алексічик та ін. Проценко Як і в попередньому документі, автор отримав підтримку проекту USAID «Медійна програма в Україні» [43, с. 48].

Пояснювальна записка до цієї програми містить взаємозв'язок впровадження освітніх засобів масової інформації в освітній процес дошкільних навчальних закладів, науково-теоретичну реалізацію, мету, основні завдання та принципи документа. Зміст програми відображає рекомендовані методи і форми роботи, інвентаризацію знань, уявлень, умінь і навичок. Взагалі програма відрізняється наявністю практичного блоку, пріоритетним напрямом, визначеними функціями та основними напрямками формування медіаграмотності в дітей старшого дошкільного віку. Авторками визначено, що для забезпечення цих напрямів доречно використовувати медіа освітні ігри, сходинок кінематографії, телебачення, мультиплікації, журналістику, фотографії. Такий

підхід забезпечує дотримання принципу НУШ: навчання протягом життя. Наведені інструменти є життєвими, тому повністю відображають сутність медіаосвіти. Наявність та створення подібних освітніх програм свідчить про актуальність підвищення рівня медіаграмотності та медіабезпеки української нації. Бачимо, що науковці шукають творчі підходи для подачі матеріалу, як створення «Казки і фарби: парціальна програма розвитку творчих здібностей дітей 4-6 років на заняттях із малювання з використанням елементів медіаосвіти» та програми, автори яких – це Г. Дегтярьова, О. Тарасова та А. Фоменко. Якщо звернутись до програм для закладів загальної середньої освіти, то ми знайдемо два документи, які мають гриф МОН України [48, с.44].

Найновіша програма складена у 2023 р. О.Мокрогузом за підтримки USAID, Internews та Академії української преси. Наведена програма містить пояснювальну записку, власне програму, використані джерела та відомості про автора. На початку програми подано мету курсу, головні завдання, результати навчально-пізнавальної діяльності, наскрізні вміння, які набудуть учні після вивчення «Основ медіаосвіти». Остання програма, яку варто тут зазначити, створена так, як і минула – у 2023 р. Її авторами є О. Мокрогуз та О. Желібаза підтримки Академії української преси та Центру вільної преси. Такий документ укладений відповідно до Державного стандарту базової середньої освіти. Програма розрахована на учнів 7-8 класів [46–47].

Окрім цього, Українська держава розвиває власні програми медіаграмотності, спрямовані на те, щоб навчити українських громадян відрізняти дезінформацію від правдивої інформації. Медіаграмотність – це частина медіаосвіти, яка дає змогу споживачам інформації виважено аналізувати медіаповідомлення, щоб розпізнавати цензуру, пропаганду, однобічність, усвідомлено сприймати та критично інтерпретувати інформацію, виокремлювати реальність від її віртуальної симуляції, обмірковувати владні відносини, міфи та типи контролю, які вони формують, причини таких дій, а також щоб усвідомлювати значення структурних елементів, які мають вплив на інформацію (модель фінансування, власник медіа, політичні уподобання і т. д.).

Тобто, це є ті вміння, які дають нам, споживачам інформації, можливість чітко розрізняти правдиві повідомлення, націлені на якісне інформування, від тих повідомлень, що можуть містити у собі дезінформацію чи корисливі наміри [28, с. 120–129].

Українським проєктом із медіаграмотності на національному рівні є «Фільтр», розроблений МОН у 2021 році. Цей проєкт від МОН є продовженням попередніх ініціатив IREX та націлений на:

- формування вміння критично сприймати інформацію серед вчителів та учнів;
- вироблення навичок стосовно взаємодії із інформацією в контексті збереження психічного здоров'я;
- створення потреби отримання якісної інформації в системі української загальної середньої освіти;
- розгортання мережі «Вивчай і розрізняй: інфомедійна грамотність» через залучення до проєкту нових шкіл й освітян.

Очікування від даного проєкту є досить солідними. Зокрема, це формування кваліфікованих вчителів, які будуть:

- підготовленими до боротьби проти нових тенденцій у розвитку дезінформації;
- психологічно стійкими та знатимуть, як правильно формувати навички здорової взаємодії із інформацією й ставитимуть на перше місце власне психічне здоров'я;
- мати всі необхідні ресурси для розкриття проблеми критичного споживання інформації під час уроків із дітьми, застосовуючи універсальні методичні матеріали.

До стратегічних функцій проєкту «Фільтр» відносяться:

- інтеграційна – об'єднання з метою ефективної взаємодії й створення умов для створення нових проєктів по медіаграмотності;

- просвітницька – здійснення інформування щодо українських проєктів із медіаграмотності та ознайомлення певної цільової аудиторії із корисними матеріалами, що допомагатимуть їм як у повсякденному житті, так і у втіленні стратегічних завдань бізнесу й держави;
- дослідницька – підтримка досліджень у галузі медіаграмотності й створення передумов для поживлення наукової діяльності по цій темі, зокрема через залучення різних стейкхолдерів до співпраці;
- регуляційна – формування державної політики у контексті суспільних перемін, втілення державних ініціатив щодо розвитку медіаграмотності [58].

Робимо висновок, що курс охоплює всі галузі медіаосвіти: і медіабезпеку, і правила користування інтернетом, і пояснює про пропаганду, маніпуляції. Освітні програми сприяють розвитку критичного мислення серед учасників. Вони навчають аналізувати інформацію, ставити питання, перевіряти факти та розрізняти достовірну інформацію від дезінформації та маніпуляцій.

### **3.2. Роль, функції та завдання фактчекінгових організацій у протидії дезінформації**

У сучасному світі, де інформація поширюється зі швидкістю світла, питання правдивості та достовірності стають надзвичайно важливими. Дезінформація, фейкові новини та маніпулятивні матеріали можуть мати серйозні наслідки для суспільства, включаючи порушення соціальної гармонії, вплив на політичні процеси та загальне підірвання довіри до медіа. В таких умовах фактчекінгові організації відіграють ключову роль у боротьбі з дезінформацією.

Фактчекінгові організації виступають своєрідними «вартовими правди», які допомагають громадськості відрізнити факти від вигадок. Вони працюють над тим, щоб виявляти, аналізувати та спростовувати неправдиву інформацію, що поширюється в медіа та соціальних мережах. Завдяки своїй роботі,

фактчекери сприяють підвищенню медіаграмотності серед населення, допомагаючи людям критично оцінювати інформацію.

Фактчек, фактчекінг – один з напрямків журналістських розслідувань, спрямований на перевірку фактів у публічних заявах (топ-персон, політиків, експертів, державних діячів, лідерів думки) та знаходження і викриття фейків, неправди, маніпуляцій, пропаганди, дезінформації [23, с. 71; 68]. У порівнянні із звичною розслідувальною журналістикою, для перевірки інформації у фактчекінгу використовуються:

- дані тільки з відкритих офіційних визнаних джерел;
- експертна думка може бути використана як додатковий або другорядний елемент доказу;
- інсайдерські дані, або ті, на які може вплинути людський фактор, як аргументи у фактчекінгу не використовуються [23, с. 71; 68].

Потреба у фактчекінгу з'явилася ще на початку ХХ ст., для підвищення якості публікованих текстів. Лише 1913 р. Р. Пулітцер та І. Вайт створили «Бюро точності та чесної гри» («Bureau of Accuracy and Fair Play») у журналі «Нью Йорк Ворлд» («New York World»). А через 10 років журнал «Тайм» («Time») починає наймати працівників для перевірки легітимності публікаційного матеріалу [21].

Всі ці фактчекінгові праці допомагали виданню ставати джерелом інформації із достовірними відомостями. І як наслідок, видання ставало все популярнішим, адже купуючи його, читачі могли бути впевненими в тому, що написане є правдою. Як відомо, чим вища популярність – тим вищий прибуток [48].

Послідовність роботи фактчекінгу:

- обрання матеріалу і виділення з нього твердження, які потребують перевірки;
- пошук в авторитетних джерелах інформації, для класифікування повідомлення як правдивого, неправдивого, оманливого чи такого, що не можна перевірити;
- проаналізоване твердження супроводжується коментарем;

- експерт перевіряє коментар;
- потім залучується зовнішній експерт: якщо робота невідповідна, то відправляється на доопрацювання, якщо ж все гаразд – то на публікацію;
- публікація перевірених фактів [53].

На думку українського публіциста та науковця О. Жадька, фактчекінг – це сучасний інструмент журналістського розслідування з унікальною концепцією та технічними можливостями, метою якого є викриття популізму, маніпуляцій, неправдивих фактів у риториці спікерів різних рівнів, публікаціях у ЗМІ [48, с. 356]..

Головний редактор ресурсу FactCheck-Україна, куратор Checkregion-ua О.Гороховський стверджує, що фактчекінг – це дієвий і потужний інструмент по виявленню реальних спекуляцій і політичних маніпуляцій на болючі соціальні теми, виразний метод показати реальну компетентність чиновників і політиків, майданчик для глибинних досліджень, що підкріплені фактами із відкритих джерел, які практично унеможливлюють звинувачення в суб'єктивності та заангажованості [49, с. 6].

Існує Міжнародна фактчек-асоціація, яка проводить наукові конференції для обміну досвідом і підтримки різних фактчекінгових організацій. Фактчекери з усіх країн світу керуються правилами цієї організації. «Міжнародна мережа фактчекінгу Інституту Пойнтера прийняла міжнародний Кодекс фактчекінгу, в якому вказані наступні принципи: прозорість джерел, чесність і неупередженість, прозорість організації і фінансування, прозорість методології, чесні і відкриті виправлення» [48, с. 132].

Виконавчий директор фактчекінгової організації «PolitiFact» А.Шарокман стверджує, що фактчекінг у порівнянні із журналістикою витратна справа, адже для того, щоб перевірити одну статтю у фактчекера це займає один-два дні, а журналісту іноді потрібно всього день, щоб написати три статті. Власники ж зазвичай просять писати про політику знаменитостей та футбол. І в гонитві за сенсацією все вирішує час, тому перевіряти факти це затратно і в рамках відведеного часу для цього, і в грошовому плані [48, с. 132].

Об'єктом дослідження фактчекінгу є публічна заява. Перевіряються ті заяви, які містять посилення на факти:

- соціологічні чи статистичні дані у відсотках;
- результати діяльності певних осіб в минулому на основі наявності відео чи підпису на документах [48, с. 132–133].

Не перевіряються суб'єктивні оцінки, висловлювання власної думки щодо тієї чи іншої події, прогнози наслідків політичних чи неpolітичних подій [49, т. 14].

Для перевірки фактів журналісти шукають обіцянки політиків у друкованих виданнях, теле- та радіопередачах, особистих сторінках у соціальних мережах, публічних виступах. Обіцянка – це те, що політик робить або не виконує. Але довести це може лише те твердження, яке є обіцянкою [21, с. 133].

Аналітичний портал «Слова і Діла» став першою в Україні фактчекінговою організацією, яка з 2008 року фіксує обіцянки політиків і стежить за їх виконанням. Цінність цього portalу полягає в тому, щоб допомогти боротися з корупцією та відстоювати права і свободи людей, щоб ніхто не почувався обманутим [66].

У 2014 році з'явився сайт StopFake, який бореться з фейковою російською рекламою. Цей сайт створений на замовлення епохи, коли раніше відбувалися історичні та політичні події. Важливо уникати пропаганди для перемоги над противником в інформаційній війні [64].

За даними американського portalу, у 2016 р. створено FaktCheck Ukraine, який у 2018 р. отримав назву «StopFake». Сайт зайнятий перевіркою достовірності висловлювань публічних діячів, публікацій у ЗМІ, дописів у соціальних мережах. Випускниця факультету журналістики та журналістсько-редакторської програми «Цифрове майбутнє журналістики». Цей додаток створено для спростування дезінформації та виявлення спотворених повідомлень, а також для пошуку реклами інцидентів в Україні [22, с. 12].

Становлення та розвиток фактчекінгових організацій в Україні відбувалося на тлі складних суспільно-політичних подій, які супроводжувалися



зростанням кількості дезінформаційних загроз та впливу маніпуляцій на суспільну свідомість [64, с. 78]. Слід зазначити, що створення системи протидії дезінформації почалося задовго до масштабної інвазії, коли вітчизняні медіапрофесіонали усвідомили необхідність створення спеціальних майданчиків для перевірки інформації та викриття неправдивої інформації [50, с. 89]. Піонером у цій галузі став проект StopFake, заснований у 2014 році викладачами та випускниками Могиллянської школи журналістики, який швидко став потужним інструментом протидії російській дезінформації, розширивши свою діяльність на міжнародному рівні та почавши публікувати матеріали тринадцятьма мовами [27, стор. 156]. Особливу увагу привертає той факт, що методика роботи StopFake, яка базується на ретельній перевірці фактів та використанні відкритих джерел інформації, стала зразком для інших фактчекінгових проєктів не лише в Україні, а й за кордоном [42, С. 81].

Вагомий внесок у розвиток внутрішнього фактчекінгу зробив аналітичний центр Texty.org.ua, який, окрім традиційної журналістської діяльності, Важливо підкреслити, що вітчизняні фактчекери активно долучаються до розробки міжнародних стандартів верифікації інформації та впровадження інноваційних методів виявлення фейків, що дозволяє підтримувати високий рівень ефективності їхньої роботи в умовах постійної еволюції дезінформаційних загроз [71, с. 112]. Особливу роль у розвитку фактчекінгу відіграє просвітницька діяльність, спрямована на формування у громадян навичок критичного мислення та медіаграмотності, що є необхідною передумовою створення стійкого до дезінформації суспільства.

### **3.3. Рекомендації щодо подальших заходів у виявленні та протидії дезінформації**

У роботі з викладачами в системі післядипломної педагогічної освіти звертається увага на специфіку роботи викладачів у період інфодемії постправди

– поширення дезінформації, яка апелює до емоцій її реципієнтів, та ігнорування об’єктивних фактів. Підкреслимо, що в інформаційному суспільстві суспільство формує власний світогляд, своє ставлення до подій і людей, виходячи не тільки з фактів, а й з того, як ці факти подаються в ЗМІ [18, с. 123]. Проте засоби масової інформації, які використовують новітні технології та цифрові пристрої, наразі не лише відтворюють реальність, а й фабрикують повідомлення та подають громадськості дезінформацію. Спираючись на роботу експертів АУП, вони методично намагаються допомогти учням розвинути вміння критично аналізувати контент, розкривати приховані сенси, розвінчувати брехню за допомогою освітніх медіа-інструментів [45, с. 24].

Після 24 лютого 2022 року майже всі українці усвідомили, що інформаційна війна є частиною великої війни. Тому нікого не потрібно переконувати, що медіаосвіта та боротьба з дезінформацією є питанням національної безпеки. Ми бачили, як з початку повномасштабної війни Росія робила все, щоб дискредитувати українців в очах світової спільноти та зруйнувати соціальну єдність нашої країни. Вони спрямовують свої зусилля на поширення ворожих наративів та проросійської ідеології [54, с. 89].

Свідомість українського народу, як індивідуальна, так і колективна, знаходиться під ударом, і кожного разу, коли вони намагаються атакувати наші слабкості, виявляється війна». Це усвідомлення необхідності після відновлення навчального процесу в березні для протидії ворожій пропаганді. , чия освітня програма була спрямована на підвищення кваліфікації працівників освіти на базі Валенського обласного інституту післядипломної освіти, заклала основу для встановлення медіагігієни під час війни та розшифровки медіа-повідомлень підозрілого чи відверто ворожого змісту, як і багатьох інших речей. . медіаінструктори, переглядаючи інформацію, акцентують увагу аудиторії лише на роботі з офіційними джерелами [18, с.124].

Підготовлено та розповсюджено серед студентів рекомендації Центру протидії дезінформації при РНБО України [8, с. 4]; Критично аналізуються міфи про країни-агресори, які дедалі частіше виникають у суспільстві; І що

найважливіше, ми почали заохочувати наших викладачів вивчати ці приклади зі своїми студентами. Отже, використовуючи засоби медіаосвіти, вчителі руйнують насаджені росіянами стереотипи.

Вчителям важливо перейти від розмов про те, що таке медіаосвіта і чому вона важлива, безпосередньо до перевірки фактів, верифікації медіатекстів, навчання учнів самостійно визначати механізми впливу на їх реципієнтів.

Виділимо сім заповідей російської пропаганди під час війни:

1. Знайти тріщини в суспільстві. Це - пошук економічних, соціальних, демографічних, расових та будь-яких інших відмінностей у суспільстві, що потім використовують для його розколу.

2. Створити зухвалу брехню. Брехня має бути настільки неймовірною, щоб ніхто не повірив, що таке можна вигадати взагалі. Якщо люди повірять у таке, наслідки будуть катастрофічними.

3. Додати трохи правди. Це виражається у поєднанні правди та брехні, як відомого інструменту пропаганди Геббельса. На користь правди співвідношення лише 15-20%, а 80-85% на користь брехні. Наприклад, факт передбачає суб'єктивні висновки та його довільне тлумачення.

4. «Сховати руки». Це вимагає перекладання відповідальності на іншу сторону конфлікту та створення фейкових ЗМІ іпсевдоукраїнських сторінок у соцмережах, що зараз активно реалізується в нашому інформаційному просторі.

5. Увімкнути «корисних ідіотів», тобто тих, хто бездумно сприймає та нав'язує своїй цільовій групі ворожі меседжі Кремля. Цими людьми можна маніпулювати в політичних цілях. В Україні ці люди підтримують ідею «руського мира».

6. Заперечувати все.

7. Грати на довгострокову перспективу: росія схильна реалізовувати тривалі кампанії з дезінформації, використовуючи на них величезні кошти протягом багатьох років. Це розроблення системи, що може бути неочевидною на перший погляд для нас, тому що ніби не видно прямих ефектів, але все це працює за принципом накопичення [17, с. 48].

При встановленні стандартів на шкідливі засоби необхідно щодня усувати їх руйнівний вплив на споживачів. Навчаючи цьому та заохочуючи вчителів розвивати ці навички, ми робимо кроки, які наближають нас до перемоги в інформаційній війні.

Щоб зрозуміти та генерувати повідомлення, вивчіть терміни: інформаційна війна, кібервійна, психологічна війна, інформаційний тероризм тощо.

Протистояти інформаційній агресії можна, лише розуміючи принципи побудови події, її мету, а отже розуміючи масштаб реальних і реальних втрат. Іншими словами, ми можемо чітко бачити, чому той чи інший інструмент пропаганди чи маніпуляції використовується в певному медіа-контексті, яка функція цього медіа-контексту.

Стереотипна ідеологія є складовою інформаційної агресії. Це можна зрозуміти, вивчивши деякі ворожі медійні тексти. Коли ми починаємо вивчати факти, то помічаємо іншу закономірність: у промовах і текстах проповідників з різних джерел ми бачимо одні й ті ж формули, мовні фрази та одноманітні твердження. Це явно ознака темряви.

Це розкриття дітям того, що держава може давати певні вказівки ЗМІ, як висвітлювати ту чи іншу подію. Завдяки українським фактчекерам, які публікують фотографії темношкірих людей в Інтернеті, ми можемо відстежувати не тільки маніпульовані погляди та пропаганду. Що дивує, так це вказівка терміну, до якого рекламодавці мають подати звіти про реалізацію плану data aggression в Україні. Як бачите, це дуже серйозний спосіб домінувати над свідомістю українців.

Розглядаємо медійний контекст на прикладі новин про розстріл російськими бойовиками дитсадка в Луганській області 17 лютого 2022 року та звертаємо увагу на те, як цю подію подали ворожі ЗМІ. Ми стверджуємо, що висвітлення деяких новин російськими ЗМІ є яскравим прикладом використання інструменту «сховай руки»: пропагандисти одразу звинуватили у всьому українську армію. Тоді вони застосували підхід «все заперечувати»,

опублікувавши фотографії місця події та стверджуючи, що стрілянина не відбулася, оскільки стіна на фотографії була пошкоджена, а сусіднє вікно недоторкане.

Це поширив пропагандист Е.Шрі за допомогою іншого інструменту – «включення корисних ідіотів», який перепублікував його пости, створивши інформаційний кокон: справжня правда була спростована, і це заперечення швидко набуло популярності в Інтернеті.

Після обробки деталей ми розкриємо ще одну маніпуляцію, в даному випадку фото. Є чотири фотографії руїн стіни дитсадка, але пропагандисти вибрали те, що було зроблено здалеку, через що було важко побачити вікна, легше було маніпулювати інформацією. Звертаємо увагу на перспективу, положення кадру, повноту об'єктів у кадрі. Це все важливі деталі, яким навчає вчитель медіа під час роботи з зображеннями

Медіаосвіта є актуальною. Тим не менш, здатність України протистояти викликам ворожої пропаганди та дезінформації зростає, і велику роль у цьому відіграють проекти, спрямовані на розвиток медійних навичок українського суспільства. Важливо, що є державні ініціативи: в МОН діє нацпроект «Flutter», Мінцифри розвиває цифрові навички з елементами розвитку критичного мислення та інформаційної безпеки. Координаційний центр психічного здоров'я при Кабінеті Міністрів за ініціативи О. Зеленської розробив інформаційну кампанію, присвячену освіті психічного здоров'я, доповнену рекомендаціями щодо здорового користування медіа, розробленими Науково-дослідною лабораторією психології психічного здоров'я «Мас-комунікації у нас». , проводити та навчати ЗМІ. Медійна спільнота співпрацює з міжнародними партнерами, щоб підтримати ініціативи з медіаграмотності в місцевих громадах.

Серед наукових ініціатив хочеться відзначити дуже цікаві та важливі дослідження, які показують, на якому рівні доказів нам потрібно працювати. Тому вперше на репрезентативній українській вибірці досліджено рівень медіатравми, пов'язаної з війною, і показано, яка частка загального стресу, пов'язаного з війною в суспільстві, спричинена медіаспоживанням.

Проведено дослідження старшого покоління 60+ та 70+, яке раніше не було охоплено медіаосвітньою діяльністю. Викликає інтерес інформація про медіаспоживання та конкретну динаміку проросійських каналів у соціальних мережах, особливо каналів Telegram, через які ведеться ворожа пропаганда; Важливими також є результати дослідження ставлення бізнесу до медіаосвіти.

Цього року Інститут соціальної та політичної психології НАН України розробив концепцію цифрової медіаосвіти на засадах цифрового гуманізму та готується до широкого громадського обговорення. Більше того, це дуже відповідає завданням євроінтеграції, адже відомо, що Європа започаткувала десятиліття цифровізації, суть якої – людяність і людяність у розвитку цифрових технологій та штучного інтелекту. Війна не може зупинити наш прогрес на цьому важливому шляху розвитку [50, с. 220].

Ініціативи з навчання ЗМІ в державному секторі, націлені на різні середовища та групи цього року, були настільки різноманітними та різноманітними, що вимагали окремих досліджень – як для оцінки їх ефективності, так і для обміну досвідом організацій, наприклад організацій із подібними цілями. Популярні формати партнерства з державним сектором у 2023 році включають ряд заходів:

- від моніторингу російської пропаганди та дезінформації до досліджень споживання інформації та зусиль залучити нову аудиторію;
- людей поважного віку, які зазвичай не були в центрі уваги організації медіаосвіти, але на даний момент вони становлять близько 30% населення, і більшість із них розташовані в країні;
- жителі неокупованих та окупованих територій, де реконструкція та розвиток громадянської ідентичності є важливими для реінтеграції та побудови критичного захисту від дезінформації на всіх рівнях суспільства.

Поки що ми мало знаємо про медіапросвітницькі ініціативи для українських вимушених переселенців. Цього року Академія української преси ще більше посилила свій освітній напрямок, передусім шляхом створення актуального контенту для вчителів, тренінгів для різних аудиторій (з метою

підвищення рівня критичного розуміння інформації, медіаграмотності у воєнний час тощо), а також доповненням. кілька нових розділів. Зокрема, у 2023 році було видано декілька підручників – «Медіаосвіта у вогні», «Методика декодування російської пропаганди на уроках історії та громадянської освіти», «Інформаційна гігієна та медіаосвіта: що нового у воєнний час», «Медіаосвіта у воєнний час». : теорія, методологія, взаємодія», а також «Нариси історії Криму (2015-2022)», призначені для вчителів історії та громадянської освіти, журналістики, медіапедагогів, тренерів з медіаосвіти, які бажають отримати додаткові можливості практичної роботи в формування освітніх ЗМІ у випускників коледжу в умовах інформаційно-ідеологічного протистояння.

Окрема робоча зона – це креативний спосіб тренування медіа у роботі з дітьми, особливо веселих мультфільмів. У 2023 році вийшов комікс «My Eyes». Його характерною рисою є наявність молодих супергероїв, які під час війни стикаються не лише з фізичними, а й з інформаційними загрозами. Цього року АУП отримала підтримку Центру медіа та інформаційної освіти Вільного університету Берліна для реалізації проекту з підготовки викладачів медіаосвіти під назвою «Протидія дезінформації в контексті російсько-української війни як інструмент подолання довіри». прогалини». Усі заходи спрямовані на те, щоб викладачі медіаосвіти могли ділитися отриманими знаннями з іншими.

Підготовлено 105 тренерів. За запланованими результатами тренери мали провести програму для 3000 учасників, а саме цільової групи. Проте майже втричі збільшив обсяги виробництва та навчив понад 9,5 тис. осіб.

Також було проведено серію вебінарів про медіаосвіту, розвиток критичного мислення при споживанні та поширенні інформації та протидію кремлівській пропаганді. Інший проект – «Маніпулятор ув'язнення» – АУР розроблений спільно з Freedom Foundation. Ф. Науманн Спеціально для студентів. Це покоління – покоління, яке швидко розбирається в трендах, тому навчальна програма (проходить у Полтаві, Києві та Чернігові) охоплює не лише виявлення медіа-маніпуляцій, а й міжособистісних маніпуляцій.

Загалом є відчуття, що медіаосвіта стала більш актуальною темою, ніж у перший рік повномасштабного вторгнення. Ми бачимо, як все більше організацій та ініціатив, які займаються не лише медіаосвітою, починають включати елементи медіаосвіти у свою основну діяльність.

Загалом, цього року з'явилося багато організацій, які починають займатися медіаосвітою, і ми відчуваємо, що ми не маємо однакового розуміння того, що таке медіаосвіта. Тому що якщо ви розмістите організації, які беруть участь у цьому, в одній кімнаті, ми вважаємо, що кожен представник, ймовірно, має різні визначення, тому для нас важливо стандартизувати це розуміння. Є ті, хто розуміє медіаосвіту у вузькому сенсі, а саме перевірку джерел, уміння розрізняти фактичну та неправдиву інформацію, є й ті, хто розуміє її у ширшому сенсі, включаючи цифрові навички [50, с. 220].

Особливо актуальним у цьому проекті є питання емоційної саморегуляції під час споживання медіа. Це ключова та фундаментальна медіа-навичка, якою повинен володіти кожен – здатність перемикатися між ірраціональним і раціональним. Тому що наступний крок – перевірка інформації та звернення уваги на джерело – можливий лише тоді, коли ми здатні регулювати нашу емоційну реакцію на певний контент. Тоді є можливість перевірити джерела та факти. Немає жодних ілюзій, що ви витратите багато часу на перевірку фактів, але важливо звернути увагу на джерело та хоча б трохи перевірити факти. Також важливим є відповідальне поширення інформації, наприклад лексики, яка використовується при поширенні повідомлень [31, с. 20].

Щороку нам кажуть, що нам не вистачає злагодженості, але зараз настав час швидко реагувати на виклик, особливо тому, що люди в нашій галузі часто перевантажені роботою і, як правило, не мають часу. Але для координації ми вважаємо, що нам потрібен простір, де ми можемо поділитися методами, ефективними інструментами та поясненнями того, чому вони працюють. І вже не доводиться сумніватися в конкуренції, адже медіаосвіта стала фактором національної безпеки. Тому розмови та довіра до цих розмов допоможуть покращити інструменти, які довели свою ефективність.



В ідеалі ми повинні поділитися інструментами, які ще не працюють, тому що, на жаль, ми бачимо деякі ініціативи, які витрачають ресурси, але здаються неефективними. Можливо, маючи певні знання, ці ресурси можна було б використати інакше, перенаправити на інші завдання – і було б ефективніше. Існує загальний брак розуміння груп, які є найбільш вразливими до дезінформації та пропаганди, розглядаючи соціально-демографічний профіль цих груп, а потім орієнтуючись на ці вразливі групи.

У нас також є кілька досліджень, у тому числі від NDI, які показують, що люди, які підтримують Московський патріархат або виступають проти ЛГБТ, більш схильні до маніпуляцій або дезінформації, ніж інші групи. Тому серед позитивних моментів року хочеться відзначити проект, започаткований Інститутом медіа та комунікації України за підтримки Deutsche Welle – робота з людьми похилого віку, адже тут ми маємо реагувати дуже гнучко, створювати інформаційні кампанії та нові освітні програми навчання.

### Висновки до 3 розділу

У третій частині роботи детально розглянуто практичні аспекти захисту інформаційного простору України від дезінформації та пропаганди, зокрема фактчекінгових організацій, важливість просвітницької ролі ЗМІ та рекомендації щодо подальших дій у цій сфері. У цьому розділі підкреслюється важливість інтегрованого підходу до вирішення проблем і окреслюються ключові напрямки для майбутньої практики.

Організації з перевірки фактів мають позитивний вплив на боротьбу з дезінформацією. Їх головне завдання – перевіряти факти та розвіювати дезінформацію, яка поширюється в ЗМІ та соціальних мережах. Організації, що перевіряють факти, не лише виявляють та виправляють неправдиві твердження, а й допомагають підвищити рівень прозорості та достовірності інформації. Вони працюють як незалежні арбітри правди та допомагають громадянам отримати об'єктивну інформацію. Діяльність цих організацій є важливим інструментом у боротьбі з інформаційними загрозами, оскільки вони забезпечують суспільство критичним аналізом інформації.

Медіаосвіта є потужним інструментом боротьби з дезінформацією та пропагандою. Освітні програми, спрямовані на розвиток медіаграмотності, вчать людей критично сприймати інформацію, аналізувати джерела та відкривати маніпулятивні техніки. Важливість медіаосвіти зумовлена тим, що ЗМІ протягом тривалого часу формують стійкість суспільства до проникнення дезінформації. Це розвиває здатність людей самостійно перевіряти факти, роблячи їх менш сприйнятливими до пропаганди. Крім того, медіаосвіта сприяє формуванню активної громадянської позиції та підвищує соціальну відповідальність.

Виходячи з вищесказаного, можна прийти до висновку, що основними заходами, які б забезпечували протидію дезінформації та пропаганді є:

- ☐ підвищення рівня медіаграмотності населення;
- ☐ посилення підтримки фактчекінгових організацій;
- ☐ створення законодавчих ініціатив;

- міжнародне співробітництво;
- розвиток технологічних рішень.

Підвищення рівня медіаграмотності населення передбачає розробку та реалізацію освітніх програм, спрямованих на навчання громадян критичному мисленню та аналізу інформації, а також особливу увагу приділяється підростаючому поколінню, яке активно користується соціальними мережами.

Гарантування фінансової незалежності та стабільності та підтримка фактчекінгових організацій загалом, а також заохочення їхньої співпраці зі ЗМІ та державними органами значно посилять боротьбу з дезінформацією та пропагандою в українському інформаційному просторі.

Створення законодавчих ініціатив, а також розробка та імплементація законів, що регулюють діяльність ЗМІ у сфері протидії дезінформації та забезпечують відповідальність за поширення дезінформації, також мають на меті створити безпечне інформаційне середовище.

Активно брати участь у міжнародних ініціативах та обмінюватися досвідом з іншими країнами, які мають успішний досвід протидії інформаційним загрозам та використовують сучасні технології для виявлення та нейтралізації дезінформації, включаючи алгоритми AI та інші інноваційні підходи.

Тому у третьому розділі наголошується на необхідності комплексного підходу до захисту інформаційного простору України. Важливість організацій, які перевіряють факти, просвітницька роль ЗМІ та чіткі вказівки допомагають створити надійну систему протидії дезінформації та пропаганді. Реалізація цих заходів сприятиме зміцненню інформаційної безпеки України та підвищенню рівня довіри громадян до ЗМІ.

## ВИСНОВКИ

Проведене дослідження дозволяє дійти низки важливих висновків, які відповідають структурі та завданням роботи. У першому розділі проаналізовано теоретико-методологічні засади протидії дезінформації та пропаганді, що дозволило визначити основні поняття, їхні характеристики та види. Дезінформація була визначена як свідоме поширення неправдивої інформації з метою маніпуляції громадською думкою, тоді як пропаганда — як система інформаційного впливу на суспільну свідомість з метою досягнення певних ідеологічних чи політичних цілей. Було також охарактеризовано основні підходи до аналізу дезінформації, зокрема^

- Інформація, яка є неправдивою та навмисно створена для заподіяння шкоди людині, соціальній групі, організації чи країні («dis-information»).
- Невірна, хибна інформація («mis-information»). Інформація, яка є неправдивою, але не створена з метою заподіяння шкоди.
- Шкідлива, зловмисна інформація («mal-information»). Інформація, яка базується на реальних подіях та використовується для заподіяння шкоди людині, організації чи країні».

У другому розділі зосереджено увагу на правових та інституційних механізмах протидії дезінформації в Україні. Дослідження показало, що в умовах гібридної війни проти України інформаційний простір стає ключовим полем битви. Наявні виклики та загрози включають широкомасштабну інформаційну агресію з боку Російської Федерації, яка активно використовує дезінформацію для підриву стабільності в Україні. Було проаналізовано чинну нормативно-правову базу та виявлено її недоліки, які потребують вдосконалення. Зокрема, зазначено важливість реалізації положень Доктрини інформаційної безпеки України, яка визначає основні напрями державної інформаційної політики. Також охарактеризовано діяльність ключових державних інституцій, таких як Рада національної безпеки і оборони, Міністерство інформаційної політики та

Служба безпеки України, які виконують важливу роль у забезпеченні захисту національного інформаційного простору.

У третьому розділі розглянуто практичні аспекти протидії дезінформації та надано рекомендації щодо захисту інформаційного суверенітету України. Визначено, що підвищення рівня медіаграмотності серед населення є ключовим інструментом зменшення впливу фейкових новин та маніпуляцій. Особливу увагу приділено ролі фактчекінгових організацій, які забезпечують перевірку інформації та спростовують недостовірні відомості. Запропоновано використання сучасних технологій, таких як штучний інтелект, для автоматизації процесів виявлення та аналізу дезінформації. Наголошено на необхідності посилення міжнародної співпраці у цій сфері, що дозволить Україні інтегрувати найкращі світові практики.

Україна демонструє прогрес у правовому та інституційному забезпеченні інформаційної безпеки, зокрема через ухвалення стратегій інформаційної та кібербезпеки. Проте актуальним залишається питання їх імплементації на всіх рівнях державного управління. Також ефективною є співпраця України з міжнародними партнерами, зокрема Європейським Союзом і НАТО, у питаннях протидії дезінформації.

За роки війни в Україні сформована нормативно-правова база щодо захисту національного інформаційного простору. У 2016 р. РНБО України було прийнято Доктрину інформаційної безпеки, юридичною основою якої стала Стратегія національної безпеки України, затвердженої відповідним президентським указом від 26 травня 2015 р. Метою цієї Доктрини стало вироблення основ формування і реалізації державної політики у сфері інформаційної безпеки, насамперед стосовно протидії інформаційному впливу РФ в умовах розпочатої нею гібридної війни. У 2021 р. було вироблено оновлену стратегію інформаційної безпеки. Однією із актуальних загроз, як і раніше, визначалася інформаційна політика росії.

Важливою інституцією у протидії дезінформації та інформаційним загрозам національній безпеці країни відіграє Центр протидії дезінформації при

РНБО України. Це є робочий орган РНБО України, створений згідно з відповідним рішенням РНБО України від 11 березня 2021 р. «Про створення Центру протидії дезінформації». Центр забезпечує проведення заходів стосовно протидії актуальним та потенційним загрозам національній безпеці й українським національним інтересам у інформаційній сфері, виявлення й боротьби з дезінформацією, пропагандою, дестабілізуючими інформаційними чинниками й кампаніями, запобігання спробам маніпуляцій громадською думкою.

Ще однією структурою у забезпеченні стабільності національної інформаційної сфери виступає Центр стратегічних комунікацій, створений при Міністерстві культури та інформаційної політики України теж 2021 р. Його основна мета полягає в координації дій держави та громадських ініціатив у боротьбі з інформаційними загрозами, розробці стратегічних комунікаційних кампаній, які спрямовані на зміцнення внутрішнього фронту та захист від інформаційних атак ззовні. Окрім цього, центр займається поширенням правдивої та перевіреної інформації серед громадян, щоб попередити дезінформаційні впливи і сформувати стійкість до маніпуляцій.

Організації з перевірки фактів мають позитивний вплив на боротьбу з дезінформацією. Їх головне завдання – перевіряти факти та розвіювати дезінформацію, яка поширюється в ЗМІ та соціальних мережах. Організації, що перевіряють факти, не лише виявляють та виправляють неправдиві твердження, а й допомагають підвищити рівень прозорості та достовірності інформації. Вони працюють як незалежні арбітри правди та допомагають громадянам отримати об'єктивну інформацію. Діяльність цих організацій є важливим інструментом у боротьбі з інформаційними загрозами, оскільки вони забезпечують суспільство критичним аналізом інформації.

Медіаосвіта є потужним інструментом боротьби з дезінформацією та пропагандою. Освітні програми, спрямовані на розвиток медіаграмотності, вчать людей критично сприймати інформацію, аналізувати джерела та відкривати маніпулятивні техніки. Важливість медіаосвіти зумовлена тим, що ЗМІ протягом

тривалого часу формують стійкість суспільства до проникнення дезінформації. Це розвиває здатність людей самостійно перевіряти факти, роблячи їх менш сприйнятливими до пропаганди. Крім того, медіаосвіта сприяє формуванню активної громадянської позиції та підвищує соціальну відповідальність.

Основними заходами, які б забезпечували протидію дезінформації та пропаганді є:

- ☐ підвищення рівня медіаграмотності населення;
- ☐ посилення підтримки фактчекінгових організацій;
- ☐ створення законодавчих ініціатив;
- ☐ міжнародне співробітництво;
- ☐ розвиток технологічних рішень.

## СПИСОК ВИКОРИСТАНИХ ДЖЕРЕЛ

### Закони, укази, постанови

1. Конституція України: Закон України від 28.06.1996 № 254к/96-ВР. URL: <https://zakon.rada.gov.ua/laws/show/254к/96-вр>
2. Про внесення змін до деяких законів України щодо заборони виготовлення та поширення інформаційної продукції: Закон України від 03.03.2022 № 2109-IX. URL: <https://zakon.rada.gov.ua/laws/show/2109-20>
3. Про внесення зміни до статті 10 Закону України «Про Державну службу спеціального зв'язку»: Закон України від 24.11.2021 № 1089-IX. URL: <https://zakon.rada.gov.ua/laws/show/1089-20>
4. Про Державну службу спеціального зв'язку та захисту інформації України: Закон України від 23.02.2006 № 3475-IV. URL: <https://zakon.rada.gov.ua/laws/show/3475-15>
5. Про інформацію: Закон України від 02.10.1992 № 2657-XII. URL: <https://zakon.rada.gov.ua/laws/show/2657-12>
6. Про основні засади забезпечення кібербезпеки України: Закон України від 05.10.2017 № 2163-VIII. URL: <https://zakon.rada.gov.ua/laws/show/2163-19>
7. Питання Центру протидії дезінформації: Указ Президента України від 07.05.2021 № 187/2021. URL: <https://zakon.rada.gov.ua/laws/show/187/2021>
8. Про деякі заходи щодо забезпечення безпеки в інформаційній сфері: Розпорядження Президента України від 15.03.2023 № 45/2023-рп. URL: <https://zakon.rada.gov.ua/laws/show/45/2023-рп>
9. Про застосування окремих нормативних документів НАТО...: Наказ Адміністрації державної служби спеціального зв'язку та захисту інформації України від 19.08.2021 № 509. URL: <https://zakon.rada.gov.ua/laws/show/z1181-21>
10. Про заходи щодо вдосконалення формування та реалізації державної політики...: Рішення РНБО України від 28.04.2014 № 449/2014. URL: <https://zakon.rada.gov.ua/laws/show/n0004525-14>



11. Про Стратегію кібербезпеки України: Рішення РНБО України від 27.01.2016 № 96/2016. URL: <https://zakon.rada.gov.ua/laws/show/n0005525-16>
12. Щодо реалізації єдиної інформаційної політики в умовах воєнного часу: Рішення РНБО України від 18.03.2022 № 152/2022. URL: <https://zakon.rada.gov.ua/laws/show/n0004525-22>
13. Даниленко Ю. Як розпізнати фейк та дезінформацію. URL: <https://ms.detector.media/fake-vs-fact/post/25789/>
14. Ейсмунт В. Протидія дезінформації: практичні поради. URL: <https://imi.org.ua/articles/protydiya-dezinformatsiyi> (дата звернення: 07.09.2023).
15. StopFake: інформаційний ресурс з викриття фейків. URL: <https://www.stopfake.org>
16. Texty.org.ua: аналітичний центр. URL: <https://texty.org.ua>
17. Золотухін Д. Біла книга спеціальних інформаційних операцій проти України. *УКРІНФОРМ*. 28 листопада 2024. URL: [https://mip.gov.ua/files/pdf/white\\_book\\_2023.pdf](https://mip.gov.ua/files/pdf/white_book_2023.pdf)
18. Маркова В. Інформаційна культура особистості. Науковий вісник імені Драгоманова. 2016. Вип. 53. Серія 5. Педагогічні науки. С. 129-141. URL: <https://nbuviap.gov.ua/informacijna-kultura>
19. Степанюк В., Сліпченко С. Інформаційна гігієна: як не потрапити на гачок пропаганди. *Горинь*. 18 жовтня 2024. URL: <https://media.org.ua/articles/info-hygiene>
20. 7 стратегічних цілей інформаційної безпеки України. URL: [https://mip.gov.ua/files/pdf/info\\_security\\_strategy.pdf](https://mip.gov.ua/files/pdf/info_security_strategy.pdf)
21. Про проєкт Фільтр. URL: <https://filter.mkip.gov.ua/about>
22. Про рішення Ради національної безпеки і оборони України від 14 травня 2021 року «Про Стратегію кібербезпеки України». Указ Президента України №447/2021. URL: <https://zakon.rada.gov.ua/laws/show/n0005525-21>
23. У чому небезпека «інформаційної бульбашки». *Громадське радіо*. 26.07.2022 URL: <https://mind.ua/publications/info-bubble>
24. Stopfake: інформаційний ресурс з викриття фейків. URL:

<https://www.stopfake.org> (дата звернення: 19.11.2024).

25. Texty.org.ua: аналітичний центр. URL: <https://texty.org.ua>
26. Слово і Діло: аналітичний портал. URL: <https://www.slovoidilo.ua>
27. 7 стратегічних цілей інформаційної безпеки України. URL: [https://mip.gov.ua/files/pdf/info\\_security\\_strategy.pdf](https://mip.gov.ua/files/pdf/info_security_strategy.pdf)
28. Золотухін Д. Біла книга спеціальних інформаційних операцій проти України. УКРІНФОРМ. 2 квітня 2024. URL: [https://mip.gov.ua/files/pdf/white\\_book\\_2023.pdf](https://mip.gov.ua/files/pdf/white_book_2023.pdf)
29. Маркова В. Інформаційна культура особистості. Науковий вісник імені Драгоманова. 2016. Вип. 53. Серія 5. Педагогічні науки. С. 129-141. URL: <https://nbuviar.gov.ua/informacijna-kultura>
30. Степанюк В., Сліпченко С. Інформаційна гігієна: як не потрапити на гачок пропаганди. URL: <https://media.org.ua/articles/info-hygiene>
31. 7 стратегічних цілей інформаційної безпеки України. URL: [https://mip.gov.ua/files/pdf/info\\_security\\_strategy.pdf](https://mip.gov.ua/files/pdf/info_security_strategy.pdf)
32. Про проєкт Фільтр. URL: <https://filter.mkip.gov.ua/about>
33. Стратегія кібербезпеки України. URL: <https://zakon.rada.gov.ua/laws/show/n0005525-21>
34. У чому небезпека «інформаційної бульбашки». URL: <https://mind.ua/publications/info-bubble>

#### **Аналітичні звіти**

35. A Multi-Dimensional Approach to Disinformation: звіт Європейської Комісії. Brussels: EU Commission, 2023. 148 р. URL: <https://op.europa.eu/en/publication-detail/-/publication/6ef4df8b-4cea-11e8-be1d-01aa75ed71a1>
36. GEC Special Report: Pillars of Russia's Disinformation: звіт Держдепартаменту США. Washington: GEC, 2023. 86 р. URL: <https://www.state.gov/russias-pillars-of-disinformation-and-propaganda-report/>

37. Hate Speech in the Media Landscape of Crimea: report. Kyiv: Human Rights House Foundation, 2023. 124 p. URL: <https://zmina.ua/en/publication-en/hate-speech-in-the-media-landscape-of-crimea/>

### **Наукові статті, матеріали конференцій, довідники**

38. Капля О.М. Правове регулювання інформаційної безпеки в Україні. *Інформаційне право*. 2023. № 2. С. 17-19. URL: <https://journals.maup.com.ua/index.php/expert/article/view/2329/2811>

39. Ухаль П.О. Інформаційні війни: причини та технології ведення 2023. С. 31–41. URL: <https://www.uzhnu.edu.ua/en/infocentre/get/70319>

40. Вербицька А. Медіаграмотність як протидія інформаційній агресії: як не стати «корисним ідіотом» у руках пропагандистів. URL: <https://argumentua.com/reportazh/med-agramotn-st-yak-protid-ya-nformats-i-agres-yak-ne-stati-korisnim-d-otom-u-rukakh-propa>

41. Ільницька У. Інформаційна безпека України: сучасні виклики, загрози та механізми протидії негативним інформаційно-психологічним впливам. *Humanitarian vision*. 2016. Vol. 2, Num. 1. С. 27-32. URL: [http://nbuv.gov.ua/UJRN/hv\\_2016\\_2\\_1\\_7](http://nbuv.gov.ua/UJRN/hv_2016_2_1_7)

### **Словники**

42. Cambridge English Dictionary. URL: [https://dictionary.cambridge.org/dictionary/english/#google\\_vignette](https://dictionary.cambridge.org/dictionary/english/#google_vignette)

43. Oxford English Dictionary. URL: <https://www.oed.com/?tl=true>

44. Політологічний словник. Міжрегіональна академія управління персоналом. Київ: МАУП, 2005. URL: [https://maup.com.ua/assets/files/lib/book/kv\\_08.pdf](https://maup.com.ua/assets/files/lib/book/kv_08.pdf)

59. Словник термінів з медіаграмотності / Міністерство культури та інформаційної політики України. URL: <https://filter.mkip.gov.ua/wp-content/uploads/2022/10/slovnyk.pdf>

## Навчальні програми та посібники

60. Виздрик В. С., Мельник О. М. Інформаційна складова національної безпеки України // Військово-науковий вісник. 2023. № 39. С. 120–129. info@vnnv.com
61. Волошенюк О., Коваленко П., Мокрогуз О. Медіаосвіта та медіаграмотність: програма. Київ: АУП, 2023. 65 с. voloshenyuk@aur.org
62. Дегтярова Г. А., Тарасова О. С., Фоменко А. П. Основи медіаграмотності: програма. Харків: ХАНО, 2023. 54 с. dehtyarova@khano.edu
63. Мокрогуз О. П. Медіаграмотність: навчальна програма. Чернігів: ЧОППО, 2023. 42 с. mokroguz@chou.edu
64. Мокрогуз О. П., Желіба О. В. Основи критичного мислення: програма. Чернігів: ЧНПУ, 2023. 36 с. mokroguz@chou.edu
65. Чашка Т. М. Медіаосвіта в школі: програма. Київ: Шкільний світ, 2023. 44 с. chashka@schoolworld.com
66. Фейки, пропаганда, дезінформація: проблеми, виклики, перспективи: аналіт. доп. / за заг. ред. В. Мартинюка. Київ: НІСД, 2023. 248 с. martyniuk@nisd.org
67. A Multi-Dimensional Approach to Disinformation: Report of the Independent High Level Group on Fake News and Online Disinformation. Brussels: EU Commission, 2023. 148 p. disinformation@eucommission.eu
68. GEC Special Report: Pillars of Russia's Disinformation and Propaganda Ecosystem. Washington: GEC, 2023. 86 p. gec@state.gov
69. Hate Speech in the Media Landscape of Crimea: An Analytical Report. Kyiv: Human Rights House Foundation, 2023. 124 p. hrf@humanrightshouse.org
70. Гібридна війна і журналістика: навч. посіб. / за ред. В. О. Жадька. Київ: КНУ, 2023. 352 с. info@knu.edu
71. Гороховський О. М. Фактчек як тренд розслідувань: можливості та перспективи: практ. посіб. Київ: АУП, 2023. 112 с. gorohovsky@aur.edu
72. Kubey R. Media Literacy in the Information Age. New York: Routledge, 2023. 484 p. kubey@routledge.com
73. Нашинець-Наумова А. Ю. Інформаційна безпека: питання правового регулювання: монографія / А.Ю. Нашинець-Наумова. Київ: Видавничий дім «Гельветика», 2017. 168 с. [https://elibrary.kubg.edu.ua/id/eprint/18860/1/A\\_Nashinets-Naumova\\_monografia\\_1\\_FPMV.pdf](https://elibrary.kubg.edu.ua/id/eprint/18860/1/A_Nashinets-Naumova_monografia_1_FPMV.pdf)

## SUMMARY

The conducted research allows us to draw a number of important conclusions that correspond to the structure and objectives of the work. The first section analyzes the theoretical and methodological principles of countering disinformation and propaganda, which allowed us to identify the main concepts, their characteristics and types. Disinformation was defined as the deliberate dissemination of false information with the aim of manipulating public opinion, while propaganda is defined as a system of informational influence on public consciousness in order to achieve certain ideological or political goals. The main approaches to the analysis of disinformation were also characterized, in particular^

- Information that is false and intentionally created to harm a person, social group, organization or country ("dis-information").
  - Incorrect, false information ("mis-information"). Information that is false, but not created with the aim of causing harm.
  - Harmful, malicious information ("mal-information"). Information that is based on real events and is used to cause harm to a person, organization or country.
- The second section focuses on the legal and institutional mechanisms for countering disinformation in Ukraine. The study showed that in the conditions of a hybrid war against Ukraine, the information space is becoming a key battlefield. Existing challenges and threats include large-scale information aggression from the Russian Federation, which is actively using disinformation to undermine stability in Ukraine. The current regulatory framework was analyzed and its shortcomings that need to be improved were identified. In particular, the importance of implementing the provisions of the Information Security Doctrine of Ukraine, which defines the main directions of state information policy, is noted. The activities of key state institutions, such as the National Security and Defense Council, the Ministry of Information Policy, and the Security Service of Ukraine, which play an important role in ensuring the protection of the national information space, are also described.

The third section considers practical aspects of countering disinformation and provides recommendations for protecting Ukraine's information sovereignty. It is

determined that increasing the level of media literacy among the population is a key tool for reducing the impact of fake news and manipulation. Particular attention is paid to the role of fact-checking organizations that ensure information verification and refute unreliable information. The use of modern technologies, such as artificial intelligence, is proposed to automate the processes of detecting and analyzing disinformation. The need to strengthen international cooperation in this area is emphasized, which will allow Ukraine to integrate the best world practices.

Ukraine demonstrates progress in the legal and institutional provision of information security, in particular through the adoption of information and cybersecurity strategies. However, the issue of their implementation at all levels of government remains relevant. Ukraine's cooperation with international partners, in particular the European Union and NATO, in combating disinformation is also effective.

During the years of war, a regulatory and legal framework for the protection of the national information space has been formed in Ukraine. In 2016, The NSDC of Ukraine adopted the Information Security Doctrine, the legal basis of which was the National Security Strategy of Ukraine, approved by the relevant presidential decree of May 26, 2015. The purpose of this Doctrine was to develop the foundations for the formation and implementation of state policy in the field of information security, primarily in terms of countering the information influence of the Russian Federation in the context of the hybrid war it launched. In 2021, an updated information security strategy was developed. One of the current threats, as before, was identified as Russia's information policy. The Center for Countering Disinformation under the NSDC of Ukraine plays an important role in countering disinformation and information threats to the country's national security. This is a working body of the NSDC of Ukraine, established in accordance with the relevant decision of the NSDC of Ukraine dated March 11, 2021 "On the Creation of the Center for Countering Disinformation". The Center ensures the implementation of measures to counter current and potential threats to national security and Ukrainian national interests in the information sphere, identify and combat disinformation, propaganda,

destabilizing information factors and campaigns, and prevent attempts to manipulate public opinion.

Another structure in ensuring the stability of the national information sphere is the Center for Strategic Communications, established under the Ministry of Culture and Information Policy of Ukraine also in 2021. Its main goal is to coordinate the actions of the state and public initiatives in the fight against information threats, develop strategic communication campaigns aimed at strengthening the domestic front and protecting against information attacks from the outside. In addition, the center is engaged in the dissemination of truthful and verified information among citizens in order to prevent disinformation influences and build resilience to manipulation. Fact-checking organizations have a positive impact on the fight against disinformation. Their main task is to verify facts and dispel disinformation that is spread in the media and social networks. Fact-checking organizations not only identify and correct false statements, but also help increase the level of transparency and reliability of information. They work as independent arbiters of truth and help citizens obtain objective information. The activities of these organizations are an important tool in the fight against information threats, as they provide society with critical analysis of information.

Media education is a powerful tool in the fight against disinformation and propaganda. Educational programs aimed at developing media literacy teach people to perceive information critically, analyze sources and discover manipulative techniques. The importance of media education is due to the fact that the media have long formed the resistance of society to the penetration of disinformation. This develops people's ability to independently check facts, making them less susceptible to propaganda. In addition, media education contributes to the formation of an active civic position and increases social responsibility.

The main measures that would ensure the counteraction to disinformation and propaganda are:

- ☐ increasing the level of media literacy of the population;
- ☐ increasing support for fact-checking organizations;

- creating legislative initiatives;
- international cooperation;
- developing technological solutions.