

МІНІСТЕРСТВО ОСВІТИ І НАУКИ УКРАЇНИ
НАЦІОНАЛЬНИЙ АВІАЦІЙНИЙ УНІВЕРСИТЕТ
ФАКУЛЬТЕТ ЛІНГВІСТИКИ ТА СОЦІАЛЬНИХ КОМУНІКАЦІЙ
КАФЕДРА ІСТОРІЇ ТА ДОКУМЕНТОЗНАВСТВА

ДОПУСТИТИ ДО ЗАХИСТУ
Завідувач випускової кафедри
_____ (І.І. Тюрменко)
« ____ » _____ 2022 р.

**КВАЛІФІКАЦІЙНА РОБОТА
(ПОЯСНЮВАЛЬНА ЗАПИСКА)**

ЗДОБУВАЧА ВИЩОЇ ОСВІТИ
ОС «МАГІСТР»

Тема: «Протидія дезінформації та фейкам в інформаційному середовищі України у період війни Росії проти України»

Виконавець: здобувачка вищої освіти ДК-621 Драговоз Вікторія Юріївна

Керівник: доктор історичних наук, професор Тюрменко Ірина Іванівна

Нормоконтролер: кандидат історичних наук, доцент Халецька Леся Пилипівна

(підпис)

Київ 2022

НАЦІОНАЛЬНИЙ АВІАЦІЙНИЙ УНІВЕРСИТЕТ

Факультет лінгвістики та соціальних комунікацій

Кафедра історії та документознавства

Галузь знань – 02 «Культура і мистецтво»

Спеціальність – 029 «Інформаційна, бібліотечна та архівна справа»

Освітньо-професійна програма – «Документознавство та інформаційна діяльність»

ЗАТВЕРДЖУЮ

Завідувач кафедри

_____ І.І. Тюрменко
« ____ » _____ 2022 р.

ЗАВДАННЯ

на виконання кваліфікаційної роботи

Драговоз Вікторії Юріївни

1. Тема кваліфікаційної роботи: «Протидія дезінформації та фейкам в інформаційному середовищі України у період війни Росії проти України», затверджена наказом ректора від «31» серпня 2022 р. № 1187/ст.
2. Термін виконання роботи: з 29.08.2022 до 31.11.2022 рр.
3. Вихідні дані до роботи: робота складається зі вступу, трьох розділів, висновків, списку використаних джерел загальним обсягом 99 сторінок, список використаних джерел нараховує 80 позицій.
4. Зміст пояснювальної записки: Вступ. Розділ 1. Теоретичні засади протидії інформаційним маніпуляціям. Розділ 2. Дезінформація та фейки як засіб інформаційних маніпуляцій. Розділ 3. Методи протидії інформаційним маніпуляціям. Висновки. Список використаних джерел. Додатки.
5. Перелік обов'язкового ілюстративного матеріалу: знімок екрану сайту Центру протидії дезінформації при РНБО; принтскрін сайту видання «Українська правда»; знімок екрану новинної стрічки сайту видання «Українська правда»; принтскрін статті з сайту видання «Українська правда»; принтскрін новинної стрічки сайту Центру протидії дезінформації при РНБО; емблема Центру протидії дезінформації при РНБО.

6. Календарний план-графік

№ пор.	Завдання	Термін виконання	Відмітка про виконання
1.	Визначення та обґрунтування теми кваліфікаційної роботи	26.08.2022	
2.	Оформлення завдання на виконання кваліфікаційної роботи	01.09.2022	
3.	Визначення об'єкта, предмета, мети, завдань дослідження. Підбір, опрацювання та вивчення літератури та джерел з теми дослідження	10.09.2022	
4.	Виконання індивідуальних завдань з теми роботи	15.09.2022	
5.	Написання основної частини, вступу та висновків	17.10.2022	
6.	Оформлення роботи та подання її на перше читання керівникові	19.10.2022	
7.	Опрацювання зауважень та виправлення недоліків	24.10.2022	
8.	Попередній захист кваліфікаційної роботи	27.10.2022	
9	Проходження нормоконтролю	10.11.2022	
11	Подання роботи на перевірку на плагіат	14.11.2022	
12.	Подання роботи на рецензування	16.11.2022	
13.	Подання остаточного варіанта на кафедрі	21.11.2022	
14.	Захист роботи	24.11.2022	

7. Консультанти з окремих розділів

Розділ	Консультант (посада, П.І.Б.)	Дата, підпис	
		Завдання видав	Завдання прийняв

8. Дата видачі завдання: « 22 » серпня 2022 р.

Керівник кваліфікаційної роботи _____ І. І. Тюрменко
(підпис керівника)

Завдання прийняв до виконання _____ В. Ю. Драговоз
(підпис випускника)

РЕФЕРАТ

Пояснювальна записка до кваліфікаційної роботи ОС «Магістр» на тему: «Протидія дезінформації та фейкам в інформаційному середовищі України у період війни Росії проти України»: 99 сторінок, 80 використаних джерел, 6 додатків.

Об'єкт дослідження – інформаційні маніпуляції.

Предмет дослідження – визначення сутності дезінформації, фейків, їх структури, методи боротьби з ними.

Мета дипломної роботи – узагальнити український досвід боротьби з фейками та дезінформацією.

Методи дослідження. На різних етапах роботи, відповідно до поставлених завдань у дослідженні були використані такі методи: спостереження, порівняння, історичний метод, методи аналізу та узагальнення.

У кваліфікаційній роботі було проаналізовано наукову літературу та джерала присвячені вивченню проблеми поширення та боротьби з фейками та дезінформацією; розглянуто етапи поширення та структуру дезінформації та фейків в умовах війни Росії проти України; проаналізовано як соціальні мережі та месенджери впливають на поширення фейкової інформації; визначено методи протидії дезінформації та фейків в інформаційних медіа-потоках, що дозволить підвищити інформаційну безпеку держави в умовах війни; проведено моніторингове дослідження протидії дезінформації та фейкам в інформаційному просторі України; проаналізовано український та європейський досвід організаційних і практичних заходів, спрямованих на боротьбу з прокремлівською пропагандою та дезінформацією.

Наукова новизна отриманих результатів полягає у тому, що на сьогодні є лише незначна кількість праць, присвячених дослідженню інформаційних маніпуляцій. Дезінформацію та фейкові новини як явище в українських медіа досліджено з точки зору каналів їх розповсюдження, проаналізовано нові канали поширення фейкових новин. Вперше був узагальнений матеріал щодо протидії дезінформації та фейкам у період війни Росії проти України на прикладі Центру протидії дезінформації при РНБО України та інтернет-виданні «Українська правда», було визначено кількість фейкової інформації, яка публікується в інформаційному просторі за період з лютого по листопад 2022 року.

Практичне значення дослідження полягає у тому, що результати дослідження кваліфікаційної роботи можуть бути використані в навчальному процесі, зокрема для написання курсових та кваліфікаційних робіт, під час підготовки лекцій, практичних занять, навчально-методичних комплексів до курсів дисциплін інформаційно-документаційного циклу.

ЗМІСТ

ВСТУП	6
РОЗДІЛ 1. ТЕОРЕТИЧНІ ЗАСАДИ ПРОТИДІЇ ІНФОРМАЦІЙНИМ МАНІПУЛЯЦІЯМ	9
1.1. Наукові дослідження та джерела з теми магістерської роботи.....	9
1.2. Методи дослідження.....	18
1.3. Сутність понять «дезінформація», «фейк».....	19
1.4. Нормативно-правові засади інформаційної безпеки України.....	24
РОЗДІЛ 2. ДЕЗІНФОРМАЦІЯ ТА ФЕЙКИ ЯК ЗАСІБ ІНФОРМАЦІЙНИХ МАНІПУЛЯЦІЙ	29
2.1. Структура дезінформації та фейків в умовах війни Росії проти України, їх класифікація та канали поширення.....	29
2.2. Соціальні мережі та месенджери як канали поширення фейкової інформації (на прикладі тіктоку та вайбер).....	41
РОЗДІЛ 3. МЕТОДИ ПРОТИДІЇ ІНФОРМАЦІЙНИМ МАНІПУЛЯЦІЯМ	45
3.1. Моніторингове дослідження протидії дезінформації та фейкам в інформаційному просторі України на прикладі Центру протидії дезінформації та видання «Українська правда» (лютий–листопад 2022 р.).....	45
3.2. Досвід України з протидії інформаційним маніпуляціям в умовах інформаційної війни Росії проти України.....	50
3.3. Європейський досвід протидії російській дезінформації.....	63
ВИСНОВКИ	79
СПИСОК ВИКОРИСТАНИХ ДЖЕРЕЛ	81
ДОДАТКИ	90

ВСТУП

Актуальність дослідження. Інформація – глобальний ресурс сьогодення, за допомогою якого збільшується ефективність керування в усіх сферах життя. Практично в усіх збройних конфліктах за останні десятиліття ефективно використовувалися методи та засоби інформаційної боротьби, які можуть призвести до таких трагічних наслідків, як: зміна суспільного ладу та політичного устрою; розпад держави; втрата армії; розвал економічної системи в країні; страта національної ідеї та духовних цінностей; загибель людей тощо.

З приходом ери інформаційних технологій людству довелося зіткнутися з безліччю проблем. Однією з таких проблем постала загроза інформаційній безпеці держав та її громадян зокрема. На сьогодні, у світі і досі не існує ефективної системи захисту сфери інформації. В умовах максимальної інформатизації суспільства, жодна держава не може почуватися у безпеці, адже її громадяни у будь-який момент можуть піддатися впливу ворожої інформаційної атаки. Відомо, що у наш час чимало держав розглядають інформаційну війну як ефективний інструмент реалізації власної зовнішньої політики. До таких країн можна віднести і Україну, яка за виняткових обставин вимушена була розпочати ведення інформаційної війни проти Російської Федерації.

Стрімкий розвиток науки і техніки, а також соціально-економічний стан сучасного суспільства зумовив значні зміни в інформаційному та комунікативному середовищі. XXI століття стало початком формування нової реальності, в основу якої закладено значну кількість подій, що досить часто знаходять своє відображення в транслюванні фейкових новин. Для розрізнення фейкових новин та дійсних варто дослідити сфери, які найбільше піддаються впливу, методи та способи їх поширення

Проблеми інформаційних маніпуляцій актуалізувалися у зв'язку з глобалізацією інформаційних процесів, бурхливим розвитком і пануванням інформаційних технологій, що дозволяють політикам експлуатувати

інформаційний простір, процес взаємодії масових комунікацій і їх аудиторії. Тому, сьогодні постають актуальними питання виявлення розповсюдження фейкових новин та дезінформації, яку вони містять, задля спричинення умисної шкоди в умовах інформаційного протистояння.

Зв'язок з науковими програмами, планами і темами. Тема дослідження пов'язана з такими дисциплінами як «Історія пропаганди і інформаційних війн», «Технології інформаційного впливу», «Організація діяльності інформаційних та аналітичних служб».

Мета і завдання дослідження. Мета роботи – узагальнити український досвід боротьби з фейками та дезінформацією.

Для досягнення поставленої мети потрібно розглянути такі **завдання**:

- проаналізувати наукову літературу та джерела присвячені вивченню проблеми поширення та боротьби з фейками та дезінформацією;
- розглянути етапи поширення та структуру дезінформації та фейків в умовах війни Росії проти України;
- проаналізувати як соціальні мережі та месенджери впливають на поширення фейкової інформації;
- визначити методи протидії дезінформації та фейків в інформаційних медіа-потоках, що дозволить підвищити інформаційну безпеку держави в умовах війни;
- провести моніторингове дослідження протидії дезінформації та фейкам в інформаційному просторі України;
- проаналізувати український та європейський досвід організаційних і практичних заходів, спрямованих на боротьбу з прокремлівською пропагандою та дезінформацією.

Об'єктом дослідження є інформаційні маніпуляції.

Предметом дослідження є визначення сутності дезінформації, фейків, їх структури, методи боротьби з ними.

Методи дослідження. На різних етапах роботи, відповідно до поставлених завдань у дослідженні були використані такі методи: спостереження, порівняння, історичний метод, методи аналізу та узагальнення.

Наукова новизна отриманих результатів полягає у тому, що на сьогодні є лише незначна кількість праць, присвячених дослідженню інформаційних маніпуляцій. У дослідженні здійснено систематизацію наукових джерел та аналіз ілюстративного матеріалу взятого з відомих періодичних видань. Дезінформацію та фейкові новини як явище в українських медіа досліджено з точки зору каналів їх розповсюдження, проаналізовано нові канали поширення фейкових новин, зокрема встановлено тенденції їх розповсюдження через соціальні мережі та месенджери. Вперше був узагальнений матеріал щодо протидії дезінформації та фейкам у період війни Росії проти України на прикладі Центру протидії дезінформації при Раді національної безпеки і оборони України та інтернет-виданні «Українська правда», було визначено кількість фейкової інформації, яка публікується в інформаційному просторі за період з лютого по листопад 2022 року.

Практичне значення одержаних результатів. Основні положення кваліфікаційної роботи можуть бути використані в навчальному процесі, зокрема для написання курсових та кваліфікаційних робіт, під час підготовки лекцій, практичних занять, навчально-методичних комплексів до курсів дисциплін інформаційно-документаційного циклу.

Особистий внесок. Кваліфікаційна робота виконана самостійно. Усі основні результати дослідження належать авторові особисто.

Апробація результатів. Кваліфікаційна робота пройшла апробацію на засідання Методологічного семінару для здобувачів вищої освіти, який відбувся 27.10.2022 року.

Структура кваліфікаційної роботи. Робота складається зі вступу, трьох розділів з підрозділами, висновків, списку використаних джерел та додатків. Список використаних джерел налічує 80 найменувань. Загальний обсяг роботи – 99 сторінок.

РОЗДІЛ 1

ТЕОРЕТИЧНІ ЗАСАДИ ПРОТИДІЇ ІНФОРМАЦІЙНИМ МАНІПУЛЯЦІЯМ

1.1. Наукові дослідження та джерела з теми магістерської роботи

Аналізуючи джерельну базу магістерської роботи, її можна систематизувати за наступними категоріями:

- вітчизняні та зарубіжні дослідження;
- нормативно-правова база у сфері протидії дезінформації та пропаганді;
- офіційні вебресурси та новинні сайти.

Теоретичні аспекти явищ «дезінформації» та «фейк» досліджували як вітчизняні, так і зарубіжні науковці. У своїх роботах автори розкривають зміст цих понять, їх основних інструментів та каналів поширення, а також аналізують як саме реалізується стратегія протидії дезінформації в Україні та Європейському Союзі.

Дослідженням проблем впливу дезінформації на суспільну свідомість займалися такі вітчизняні дослідники, як Г. Почепцов та В. Шлапаченко.

Провідним вітчизняним дослідником дезінформації та фейків є Г. Почепцов. Зокрема, у своїй праці «(Дез)інформація» він досліджує питання маніпуляції інформацією цифровими медіа, а також гібридні та віртуальні війни, інструменти розповсюдження дезінформації та засоби управління масовою свідомістю [60].

Окрім дезінформації та пропаганди, серед сучасних загроз суспільству виділяють фейки. Дослідженням цього займаються такі вітчизняні дослідники, як М. Кіца та І. Мудра. Вони визначають поняття «фейк», подають його класифікацію і методи виявлення. Крім того, доводять, що «фейкова інформація розповсюджується з метою ввести в оману, викликати сумніви і переконати

аудиторію у правдивості повідомлення, а також аналізують приклади фейків, які поширюють ЗМІ та методи їх знешкодження» [52], [58].

Значна кількість наукових праць присвячена ролі журналістики у протидії інформаційним маніпуляціям. Зокрема, К. Удовиченко, у якій вона також звертається до є поняття «фейк», аналізує методи та засоби перевірки фактажу, з'ясовує роль і місце редактора в перевірці фактичного матеріалу із врахуванням умов інформаційної війни та технічних засобів їх виявлення.

Важливою для розуміння проблеми протидії фейковій інформації, на мою думку, є дослідження доктора наук із соціальних комунікацій В. Шевченко, яка розглядає історію виникнення фактчекінгу (один з напрямків журналістського контролю), методи маніпуляції та інструменти для верифікації інформації [75].

Проблемами інформаційної безпеки, протидії впливу російської пропаганди та дезінформації, займався ще чимало українських дослідників: В. Горбулін, О. Литвиненко, Д. Дубов, В. Петров, М. Ожеван, Т. Черненко, В. Конах, В. Ліпкан, В. Остроухов, Я. Короход та інші, які в різні періоди аналізували інформаційний простір України, вказували на характерні риси інформаційної експансії Росії, яка використовує в своїх цілях вітчизняні ЗМІ для поширення неоімперіалістичних ідей. О. Саприкін, П. Шевчук, І. Костюк, О. Цуканова досліджували у різний спосіб проблеми інформаційних маніпуляцій, розкривали сутність інформаційних впливів на українське суспільство.

Для виявлення та ефективної протидії дезінформації та фейкам науковці виділяють фактчекінг та медіаосвіту. Українським експертом у галузі перевірки фактів є О. Гороховський автор практичного посібника «Фактчек як тренд розслідувань: можливості та перспективи». Автор досліджує перевірку фактів з точки зору нового тренду в сучасній журналістиці, описує головну концепцію формату фактчекінгу та проаналізував досвід країн Європи у цій сфері. Також автор виокремлює ознаки, які вказують на неправдивість інформації, аналізує контент сайтів для можливості уточнення формулювання поняття «фактчекінг» та «верифікація», наводить головні ознаки, які вказують на необхідність перевірки даних [41].

Не менш важливим питанням для є медіаосвіта, адже це дає можливість громадянам різного віку орієнтуватися в сучасному середовищі новин і приймати усвідомлені рішення. Тому варто відзначити, працю українських дослідників у галузі медіаосвіти В. Іванова, О. Волошенюк, Л.Кульчинської «Медіаосвіта та медіаграмотність: короткий огляд». У даному збірнику автори, подають аналіз термінології зарубіжних дослідників щодо медіаосвіти та медіаграмотності, а також описують досвід розвинених країн Європи у становленні медіаосвіти [47].

З огляду на те, що доробок українських дослідників з даної проблематики є досить невеликим, і поставлене питання не є вивченим у повній мірі, проведене дослідження враховує нароби зарубіжних науковців.

Особливо слід підкреслити внесок провідних західних аналітиків: Дж. Найя-молодшого, М. Галеотті, П. Померанцева, К. Пола, В. Метьюс та ін., доповіді яких стали підставою для прийняття важливих державних рішень у напрямі протидії російській «гібридній» інформаційній агресії.

Фундаментальною у сфері досліджень, присвячених боротьбі з інформаційними маніпуляціями є робота британської дослідниці соціальних мереж та дезінформації Клер Вордл (Claire Wardle) та ірано-канадського дослідника Хосейна Деракшан (Hossein Derakhshan) «Інформаційний розлад: до міждисциплінарних рамок для досліджень та формування політики» (Information disorder: toward an interdisciplinary framework for research and policy making). Цей звіт є спробою всебічно вивчити інформаційний розлад і пов'язані з ним проблеми. Хоча історичний вплив чуток і сфабрикованого вмісту добре задокументовано, дослідники стверджують, що сучасні соціальні технології означають, що нині спостерігається щось нове: забруднення інформації в глобальному масштабі; складна мережа мотивацій для створення, поширення та споживання цих «забруднених» повідомлень; безліч типів контенту та технік для посилення публікацій; незліченні платформи, які розміщують і відтворюють цей контент; шалену швидкість спілкування в мережі Інтернет. Автори утримуються від використання терміну «фейкові новини» тому, що цей термін почали

використовувати політики в усьому світі в негативному світлі і часто застосовують його як знаряддя боротьби. Таким чином, це стає механізмом, за допомогою якого сильні можуть притискати та обмежувати вільну пресу. Тому фахівці ввели нову концептуальну основу для дослідження інформаційного розладу, виокремлюючи три різні типи: неправильна інформація, дезінформація та шкідлива інформація, а також визначено їх основні елементи та фази [67].

Наступним важливим дослідженням є праця французьких науковців Жана Батиста Жонжена Вілмера (Jean-Baptiste Jeangène Vilmer) та Александра Ескорія (Alexandre Escorcía) «Інформаційні маніпуляції: виклик для наших демократій» (Information manipulation: A Challenge for Our Democracies). Дане дослідження є наслідком усвідомлення потенційної небезпеки, яку маніпулювання інформацією становить для наших демократій. Оскільки явище маніпулювання інформацією не є новим, але головним у сучасному світі, то важливість даного дослідження обумовлено двома наступними факторами:

- безпрецедентна здатність Інтернету та соціальних мереж швидко та «вірусно» поширювати інформацію;
- зростаюча криза довіри до демократії, яка знецінює публічне мовлення та принижує саме поняття істини.

Тому в цій доповіді на зміну терміну «фейкові новини» використовується більш точний термін «інформаційні маніпуляції». До того ж, основна увага зосереджується на конкретному виді маніпуляцій інформацією: тих, що організовані державами й чия мета полягає у тому, щоб ослабити або дестабілізувати демократичний лад в інших державах. Таким чином, у доповіді проаналізовано різноманітні маніпуляції з інформацією в країнах пострадянського простору, в Європі та Північній Америці, які є найвідомішими, акцентуючи увагу на кількох прикладах на Близькому Сході, Африці та Латинській Америці. Крім того, автори визначили майбутні технологічні виклики, тенденції російської «інформаційної війни» та можливі сценарії розвитку подій. Дослідники вважають, що маніпулювання інформацією залишатиметься проблемою в майбутньому і це буде довгостроковим викликом

для наших демократій, оскільки інформація все більше розглядається як загальне благо, захист якої стосується всіх громадян. Перш за все, громадянське суспільство має розвивати власну стійкість, а уряди можуть і повинні прийти їм на допомогу. Вони не повинні бути лідерами, але, тим не менш, їхня роль є вирішальною, оскільки вони не можуть дозволити собі ігнорувати загрозу, яка підриває основи демократії та національної безпеки.

Інституційні механізми боротьби з дезінформацією та пропагандою в ЄС розглядає професор стратегічних комунікацій Джеймс Паммент (James Pamment) автор дослідження «Майбутні загрози та рішення, які розглядаються в перспективі щодо протидії дезінформації в ЄС» (Future Threats, Future Solutions that looks into the future of the European Union's (EU) disinformation policy). Дане дослідження опубліковане в трьох статтях та виконане на замовлення Відділу стратегічних комунікацій Європейської служби зовнішніх дій (EEAS) [67].

У першій публікації «Роль ЄС у боротьбі з дезінформацією: повернення ініціативи» (The EU's Role in Fighting Disinformation: Taking Back the Initiative) Паммент акцентує увагу на майбутніх загрозах і мірі, в якій поточні інструменти ЄС щодо дезінформації можуть вирішити цю проблему. Слід зазначити, що дослідження даного питання співпадає з початком спалаху епідемії коронавірусу на п. 2020 р. Тому, у зв'язку з цим, спектр поточних інструментів боротьби з дезінформацією в ЄС був доповнений новим досвідом вирішення кризової ситуації громадського здоров'я.

У другій статті, «Роль ЄС у боротьбі з дезінформацією: посилення рамкових програм» (The EU's Role in Fighting Disinformation: Crafting an EU Disinformation) визначається основна термінологія та сфери організації дезінформаційної політики провідних інституцій ЄС.

У третій роботі «Роль ЄС у боротьбі з дезінформацією: розробка політичних заходів для 2020-х років» (The EU's Role in Fighting Disinformation: Developing Policy Interventions for the 2020s) детально описано три аспекти регулювання, які необхідні для розробки політики ЄС щодо дезінформації, здатної протистояти майбутнім загрозам.

Проблематику поширення фейкових новин в соціальних мережах активно досліджують американський журналіст і цифровий стратег Нік Ньюман, фізик і науковий письменник Марк Бьюкенен. Наприклад, у своїй аналітичній доповіді «Журналістика, медіа, тренди технологій та передбачення» Ньюман чітко охарактеризовує віртуальну реальність як головний засіб для розповсюдження фейкових новин та досліджує вплив неправдивої інформації на світові політичні процеси [67].

Оскільки дезінформаційні кампанії є серйозним викликом для Європи і вимагають скоординованої реакції країн-членів та інституцій ЄС, соціальних мереж, ЗМІ та громадян, левову частку джерельної бази магістерської роботи становить нормативно-правова база ЄС в сфері боротьби з дезінформацією та протидії гібридним загрозам. Серед основних документів варто виокремити наступні:

– «План дій зі стратегічних комунікацій» (EU Action Plan on Strategic Communication), в якому чітко були поставлені цілі щодо покращення можливостей ЄС у сфері ефективної комунікації та прогнозування, вирішення проблем та реагування на зовнішню дезінформаційну діяльність, а також зміцнення загального середовища ЗМІ в країнах Східного партнерства. Згідно цього плану, було створено Оперативну робочу групу зі стратегічних комунікацій ЄС (East StratCom Task Force) для виявлення та протидії дезінформації з боку Росії.

– «Спільні принципи протидії гібридним загрозам – відповідь Європейського Союзу» (Joint Framework on countering hybrid threats – a European Union response) у якому викладено дії, що спрямовані на протидію гібридним загрозам і сприяння стійкості суспільства до дезінформації як на рівні ЄС, так і на національному рівнях. Також пропонується активізувати співпрацю та координацію спільних зусиль ЄС і НАТО щодо протидії гібридним загрозам.

– Резолюція «Стратегічні комунікації ЄС як протидія пропаганді третіх сторін» (EU strategic communication to counteract propaganda against it by third parties), де визначаються проблеми стратегії ЄС з протидії пропаганді та

зазначено, що ворожа пропаганда проти ЄС має багато різних форм та інструментів, головною ціллю яких є спотворення істини, викликання сумнівів та створення стратегічного розколу між ЄС та північноамериканськими партнерами шляхом дискредитації інституцій ЄС, гальмування процесу прийняття рішень, які відіграють ключову роль у європейській безпеці [67].

Звіт Групи високого рівня (HLEG) «Багатовимірний підхід до дезінформації» (A multi-dimensional approach) значно вплинув на розвиток європейського підходу до регулювання протидії дезінформації. Завдяки цьому звіту ЄС отримав чітке окреслення проблеми дезінформації. Метою цього звіту є визначення ключових принципів і цілей для майбутніх дій, а також перетворення їх у конкретні, вимірні, досяжні, реалістичні та визначені у часі відповіді на дезінформацію в країнах Європи. Розглянуто заходи, які вже було вжито різними зацікавленими сторонами, та оцінено їхні переваги та можливі обмеження. Оскільки дезінформація є багатогранною проблемою, яку неможливо вирішити за допомогою одного заходу, запропоновані відповіді слід розглядати як набір взаємозалежних дій, що є частиною всеохоплюючого багатовимірного підходу.

Важливим кроком боротьби з дезінформацією в ЄС стало прийняття «Кодексу практики щодо протидії дезінформації» (Code of Practice on Disinformation), який підписали представники онлайн-платформ та рекламної індустрії (гугл, майкрософт), провідних соціальних мереж (фейсбук, твітер, тікток). Варто наголосити, що він є першим у світі саморегулюючим документом, а це означає, що підписанти на добровільній основі зобов'язалися впроваджувати широкий спектр заходів: покращувати контроль над прозорістю політичної реклами, закрити подроблені облікові записи і сприяти зменшенню доходів постачальників дезінформації.

Європейська Комісія затвердила «План дій проти дезінформації» (Action Plan against Disinformation), який залишається ключовим елементом політики ЄС у цій галузі. У цьому документі дезінформація розглядається в контексті гібридних загроз і підкреслюється роль стратегічних комунікацій Європейської

служби зовнішніх справ (EEAS). Також описуються чотири напрямки роботи: покращення спроможності інституцій ЄС виявляти та аналізувати дезінформацію; посилення скоординованої та спільної реакції на дезінформацію; мобілізація приватного сектора для боротьби з дезінформацією; і підвищення рівня обізнаності та підвищення стійкості суспільства до цієї загрози. У плані дій зображені рекомендації щодо розширення ресурсів і можливостей EEAS, а також створення системи швидкого оповіщення для посилення координації між інституціями ЄС, державами-членами та іншими відповідними міжнародними мережами [67].

Характерною особливістю поширення дезінформації є те, що чим серйозніша подія, тим більше про неї розповсюджується дезінформація, яка намагається спотворити реальність. Саме тому з метою запобігання великої кількості неправдивої та фальшивої інформації в період виборів до Європарламенту (травень 2019 р.) у березні того ж року було прийнято резолюцію «Про зовнішнє втручання у вибори та дезінформацію у національних і європейських демократичних процесах» (Foreign electoral interference and disinformation in national and European democratic processes). У ній рекомендується підвищити обізнаність європейських громадян про дезінформаційні кампанії Росії та інших ворожих суб'єктів. Наголошується, що іноземне втручання може мати безліч форм та окреслюються методи захисту виборчих процесів у країнах ЄС від такого втручання.

У 2020 р. спалахнула епідемія Covid-19, яка поширилася на весь світ. Відповідно значно активізувалося поширення дезінформації в мережі Інтернет та ЗМІ про даний вірус. У відповідь на це, інституції ЄС ухвалили документ «Боротьба з інфодемією COVID-19 – правильний виклад фактів» (Tackling the COVID-19 infodemic – getting the facts right). У документі йдеться про головні виклики, які спричинила дезінформація навколо коронавірусу. А також наголошується на посиленні стратегічних комунікацій як всередині ЄС, так і за його межами, покращенні співпраці в рамках ЄС, особлива увага зосереджується

на необхідній ефективній співпраці європейських інституцій із соціальними медіа та підтримка досліджень й діяльності у сфері перевірки фактів.

Ще одним визначальним документом є «Резолюція щодо медіаграмотності у цифровому світі» (European Parliament resolution on media literacy in a digital world), яку затвердив Європейський Парламент. У документі наголошується на необхідності розвитку медіаосвіти у країнах ЄС та подано рекомендації щодо визначених способів реалізації цього на різних освітніх рівнях [67].

Загалом, головною метою документів ЄС є визначення механізмів для протидії дезінформації, окреслення головних викликів і загроз для національного і міжнародного співтовариства в інформаційному та фізичному середовищах, а також шляхи виявлення та реагування на ці загрози.

Важливим джерелом для дослідження стали електронні ресурси, такі як офіційні сайти міжнародних організацій, офіційні сторінки інституцій ЄС та їх суміжних проєктів в галузі боротьби з дезінформацією та перевірки фактів. Зокрема, вебсайт EUvsDisinfo, який є флагманським проєктом Оперативної робочої групи зі стратегічних комунікацій (East StratCom Task Force) Європейської Служби зовнішніх справ (EEAS); а також офіційні сторінки: Європейського центру з протидії гібридним загрозам (Гельсінки), провідного фактчек-проєкту ЄС «FactcheckEU», Європейської обсерваторії цифрових медіа (Флоренція); Соціальної обсерваторії з дезінформації та аналізу соціальних мереж [67].

На основі аналітичних статей та доповідей, матеріалів монографій, які знаходяться у вільному доступі зазначених ресурсів, було проаналізовано структуру цих інституцій, а також визначено їх завдання, зокрема – аналіз основних загроз в інформаційному просторі, а також розробка рекомендацій з покращення механізмів протидії гібридній діяльності.

Аналіз наукових публікацій та нормативних документів засвідчив нагальну потребу проаналізувати досвід боротьби з дезінформацією та фейками у період воєнної агресії Росії проти України. Слід зазначити, що нині

фактологічний та інформаційний матеріал щодо боротьби з дезінформацією та фейками не висвітлений достатньо широко, а тому потребує аналізу та узагальнення.

1.2. Методи дослідження

На різних етапах роботи, відповідно до поставлених завдань у дослідженні були використані такі методи:

– спостереження, а саме у розробці моніторингового дослідження протидії дезінформації та фейкам в інформаційному просторі України на прикладі Центру протидії дезінформації та видання «Українська правда». Метод спостереження був використаний для моніторингу соцмережей, які українці найчастіше використовують для отримання новин, та виявленні в новинних матеріалах соціальних мереж і месенджерів дезінформації та фейків, наявності інформаційних маніпуляцій, перемішування фактів та суджень, відсутності достовірності, точності та повноти інформації, а також у виявленні технічного втручання у фото та відео з допомогою графічних редакторів, фотошопу, маніпуляцій у візуалізації статистичних та соціологічних даних.

– завдяки методу порівняння вдалося порівняти досвід України та Європейського Союзу в протидії інформаційним маніпуляціям в умовах інформаційної війни Росії проти України;

– історичний метод дав змогу простежити основні етапи розповсюдження дезінформації та формування інституційних механізмів для ефективної протидії цій загрози на теренах нашої держави та в межах Європейського Союзу;

– метод аналізу. Наукова доцільність використання методу обумовлена можливістю систематизувати великий обсяг емпіричного матеріалу та розглянути питання комплексно. Безпосередньо, завдяки методу аналізу розглянуто різні підходи до трактування термінів «дезінформація» та «фейк»,

виділено притаманні їм риси, схарактеризовано погляди різних науковців на них. Метод дозволив проаналізувати частоту висвітлення подій, пов'язаних з конфліктом, а також дослідити, як українські засоби масової інфомації висвітляють події. Також метод аналізу використано при опрацюванні нормативно-правової бази, що стосується поширення дезінформації та боротьби з нею;

– метод узагальнення використано для виявлення головних загроз та викликів в умовах війни Росії проти України.

Так, у кваліфікаційній роботі були використані вказані вище методи наукового дослідження, які зробили величезний внесок у розробку проблеми. Завдяки їх використанню мені вдалося вирішити завдання, які перед мною стояли, в ході дослідження та досягнула поставленої мети.

1.3. Сутність понять «дезінформація», «фейк»

Проблемою інформаційних маніпуляцій займалися видатні українські дослідники Почепцов Г., Карпенко Г., Ліпкан В., Остроухов В., Короход Я. та інші.

Зокрема, В. Карпенко аналізує інформаційний простір України, показує інформаційну експансію Росії (тобто поширення впливу однієї країни на одну або кілька сфер життя іншої країни), яка використовує в своїх цілях наші ЗМІ для поширення своїх ідей, подає форми російської експансії в інформаційному просторі України [51].

Такі дослідники, як О. Саприкін, П. Шевчук, І. Костюк, О. Цуканова досліджують проблеми інформаційних маніпуляцій, розкривають сутність процесів інформаційного впливу на суспільство [53], [65], [72], [74].

Типова інформаційна маніпуляція застосовується для досягнення таких цілей, як: запобігання можливого військовому конфлікту; ослаблення

морального духу особового складу збройних сил і цивільного населення супротивника; примус супротивника до відмови від участі у бойових діях; створення переваг на певних напрямках конфлікту. Г. Г. Почепцов зазначає, що інформаційні маніпуляції «будуються на стратегії резонансу, коли одна комунікативна складова починає функціонувати у такий спосіб, щоб замінити собою усі інші, коли одне повідомлення може викликати збудження усього суспільства» [61].

У вітчизняній науковій літературі недостатньо досліджені питання інформаційної маніпуляції. Поза увагою залишається виявлення причин захисту інформаційного поля України від інформаційних атак. Це явище існувало в тій чи іншій мірі з давніх часів. Здійснення інформаційних впливів з використанням інформаційної зброї (приховування інформації; подача її частково, у певному ракурсі; перебільшення наслідків) було зафіксовано літописцями на теренах України ще за Київської Русі. Так, загальновідомим є факт поїздки княгині Ольги до Константинополя, проте ні візантійські, ні руські джерела не висвітлюють причину та мету подолання такого довгого шляху. Войовничий князь Святослав заздалегідь повідомляв противника про свій похід, проте залишалися таємницею напрям та сили, котрі планувалося задіяти. Це давало можливість навести паніку у стані військ та швидко розгромити противника [42, с. 18].

Одним із перших у відкритому друці, хто написав про феномен інформаційних маніпуляцій був М. Маклюєн у 1960 рр. Уже тоді було відомо, що ця маніпуляція ведеться за допомогою інформаційних технологій, так як у всі часи війни велися з допомогою передових технологій. Дослідник відмітив, що в минулого використовували зброю, знищуючи ворогів одного за іншим, то інформаційна зброя за допомогою телебачення та кіно, навпаки, занурює все населення у певний світ уяви: «земна куля тепер – не більше, ніж село» [56, с. 7].

Дослідники П. Шпиґа та Р. Рудник повідомляють, що нині є 4 підходи до визначення даного поняття:

– перший підхід трактує їх як сукупність політико-правових, соціально-економічних, психологічних дій, що передбачають захоплення інформаційного

простору, витіснення ворога з інформаційної сфери, знищення його комунікацій, позбавлення засобів передачі повідомлень, а також інші подібні цілі;

– за другим підходом – це найгостріша форма протистояння в інформаційному просторі, де першочергового значення набувають такі якості взаємодії, як безкомпромісність, висока інтенсивність суперечки та короткотривалість гострого суперництва;

– за третім підходом це поняття інтерпретується як форма забезпечення та ведення військово-силових дій за допомогою найсучасніших електронних засобів (цифрових випромінювачів, супутникових передавачів та інших аналогічних засобів, які застосовуються для виконання військових завдань);

– четвертий підхід ототожнює це як протистояння між технічними системами [77, с. 328].

Українські дослідники Д. Богуш та О. Юдін зазначають, що про застосування інформаційної маніпуляції можна говорити лише в тому випадку, коли здійснюється комплексний вплив на інформаційну сферу противника, який передбачає створення умов для ведення бойових дій або виступає як самостійний чинник, який змушує конфронтуючу державу відмовитись від намічених політичних, економічних чи інших цілей. При цьому особливостями у будь-якому випадку є ризик і невизначеність її результатів [36, с. 85].

Зокрема, Р. Чирва стверджує, що головне завдання інформаційних маніпуляцій полягає в маніпулюванні масами, дезорієнтації та дезінформації громадян, залякуванні супротивника своєю могутністю [73, с. 9].

Є. Магда вважає, що інформаційні маніпуляції, які застосовує проти України Російська Федерація, спрямовані не лише на розхитування ситуації всередині держави, а і на створення негативного іміджу України в світі. Стартував цей процес ще 2005 р. під час першої газової війни і до сьогодні. Тоді Україну успішно представили в якості нечесного, а щонайменше сумнівного транзитера газу, незважаючи на те, що протягом десятиліть Україна ніколи не допускала зриву поставок природного газу до Європи через свою територію. Показово, що одночасно з цими звинуваченнями Росія наголошувала на

необхідності будівництва газопроводів, альтернативних українській системі (Північноєвропейський газопровід у Балтійському морі, друга нитка «Блакитного потоку» в Чорному морі та розширення газотранспортної системи в Білорусі, що тепер належить Газпрому). До того ж звинувачення у крадіжках газу не підкріплювалися конкретними фактами [55, с. 140].

За твердженням Р. Чирви, політичний бомонд Росії добре засвоїв уроки Геббельса: той, хто контролює інформаційне поле, має владу. Крім того, автор переконана, що інформаційна навала почалася задовго до Євромайдану, адже Кремль вважав, що доля України – це виключно Митний Союз та інтеграція до Росії. Деякі навіть відверто натякали, що губернія у складі Росії – це перспектива для України, а інакше буде беззаконня, розруха, кінець незалежності та крах держави [73, с. 8].

І дійсно видно, що Росія не шкодує фінанси на дезінформацію і фейки, направлені в сторону нашої держави, подає інформацію, що держава розвалюється, що Україною керують радикали, фашисти, бандерівці, нацисти, хунта, які чинять масовий безлад, вандалізм, найстрашніше – вбивають людей на вулицях, спалюють будинки комуністів, «регіоналів» та російськомовних громадян. Росія влаштовує своїм глядачам повноцінне шоу «про жахіття та беззаконня в Україні, на яке не шкодують великих грошей – захоплюючий сценарій, вишукана акторська гра, відповідна музика, спеціальні ефекти, шокуючий відеоряд.

Дослідниця І. Костюк має рацію, коли ствержує, що сьогодні російсько-українська інформаційна війна ведеться відкрито. Крім того, дослідниця вказує на те, що в Україні краща ситуація з погляду плюралізму в медіа і доступу громадян до інформації. У Росії не існує широковідомих опозиційних каналів інформації (окрім телеканалу «Дождь», який з початку повномасштабного вторгнення заборонили) [53, с. 58].

Український учений В. Карпенко повідомляє, що можна впевнено стверджувати, що Росія проводить по відношенню до України інформаційну експансію (система, що склалася в засобах інформації розвинених держав, і

методи, використані для пропагандистського забезпечення певних геополітичних цілей). Науковець впевнений, що українське телебачення та радіо і російське часто одну й ту ж подію висвітлюють по-різному. Він зауважує, що не потрібно дивуватися та обурюватися, адже чужоземний інформатор використовує наш національний простір в інтересах своєї держави [51].

Кандидат військових наук Ю. Радковець після аналізу розвитку ситуації навколо України стверджує, що є всі підстави стверджувати, що сьогодні наша держава зіткнулася саме із «гібридною» формою ведення воєнних дій. Використовуються нові, а точніше, брудні, методи та способи ведення цієї війни: підкуп, шантаж, залякування, викрадення людей, захоплення державних об'єктів, органів місцевої влади та об'єктів критичної інфраструктури, організація та проведення терористичних актів. Усе це супроводжується резонансними акціями насильства до непокірних та проявами мародерства. Водночас Росія, як держава-агресор, перекладає всю відповідальність за «брудну роботу» на недержавні формування (у тому числі збройні) [62, ст. 37-38].

Дезінформація та фейки є міжнародною проблемою та загрозою для суспільства, адже вони породжують плутанину та недовіру, а також зменшують віру людей в інституції, які мають вирішальне значення для функціонування здорової демократії, як-от уряд, ЗМІ тощо. Це підриває здатність громадян ефективно брати участь у житті суспільства та різноманітних громадських заходах.

Незважаючи на значну кількість досліджень зарубіжних та вітчизняних науковців у сфері протидії дезінформації та фейкам, сьогодні все ще не існує цілісного розуміння цих явищ. Проте, узагальнюючи розглянуті визначення, можна стверджувати, що дезінформацію розглядають в контексті розвитку цифрових медіа та їх впливу на сучасне суспільство.

Завдяки новим комунікаційним технологіям стало можливим легко створювати й розповсюджувати неправдиву та шкідливу інформацію, яка є замаскованою під новини заради завоювання довіри тієї чи іншої цільової аудиторії. Фальшиві чи частково спотворені новини в результаті мають

негативний вплив та є загрозовим явищем у медіапросторі. Вони розповсюджуються з чотирьох конкретних причин, таких, як прибуток, політичні та економічні мотиви, або внести корективи в демократичний устрій країн тощо.

Дезінформація – це проблема, яка перетинає кордони, як національні, так і дисциплінарні. Дедалі очевиднішим стає те, що вирішення проблеми неможливо знайти без істотної міжнародної та міждисциплінарної співпраці. Так, в умовах інформаційних війн та маніпуляцій зростає потреба в перевірці достовірності відомостей та фактів, які циркулюють в нашому інформаційному середовищі.

1.4. Нормативно-правові засади інформаційної безпеки України

Правову основу інформаційної безпеки становлять такі законодавчі та нормативно-правові документи:

– Конституція України. У ст. 10, 17, 31, 32, 34, 40, 50 регулюються загальні положення щодо свободи слова та висловлення думки, можливості отримання та розповсюдження інформації, міжособистого та міжгрупового спілкування та ін. [1];

– Закон України «Про національну безпеку України». Цей Закон визначає основні засади державної політики, спрямованої на захист національних інтересів і гарантування в Україні безпеки особи, суспільства і держави від зовнішніх і внутрішніх загроз в усіх сферах життєдіяльності [12];

– Закон України «Про інформацію». Базовими положеннями цього нормативно-правового акту закріплюється право громадян на інформацію, закладаються правові основи інформаційної діяльності. Ґрунтуючись на Декларації про державний суверенітет України та Акті проголошення

незалежності, Закон стверджує інформаційний суверенітет України і визначає правові норми міжнародного співробітництва в галузі інформації [2];

– Закон України «Про Державну службу спеціального зв'язку та захисту інформації України». Зазначений нормативно-правовий акт визначає правові основи організації та діяльності Державної служби спеціального зв'язку та захисту інформації в Україні. В Законі встановлюються правила, принципи підготовки повідомлення, зберігання передання інформації, системи доступу до певних типів інформації та умови зберігання пов'язаною з цим державної таємниці [8];

– Закон України «Про державну таємницю». Цей Закон регулює суспільні відносини, пов'язані з віднесенням інформації до державної таємниці, засекречуванням, розсекречуванням її матеріальних носіїв та охороною державної таємниці з метою захисту національної безпеки України [5];

– Закон України «Про доступ до публічної інформації». Цей Закон визначає порядок здійснення та забезпечення права кожного на доступ до інформації, що знаходиться у володінні суб'єктів владних повноважень, інших розпорядників публічної інформації, визначених цим Законом, та інформації, що становить суспільний інтерес [10];

– Закон України «Про захист інформації в інформаційно-телекомунікаційних системах». Цей Закон регулює відносини у сфері захисту інформації в інформаційних, телекомунікаційних та інформаційно-телекомунікаційних системах [6];

– Закон України «Про захист персональних даних». Зазначений Закон регулює правові відносини, пов'язані із захистом і обробкою персональних даних, і спрямований на захист основоположних прав та свобод людини і громадянина, зокрема права на невтручання в особисте життя, у зв'язку з обробкою персональних даних. Поширюється на діяльність з обробки персональних даних, яка здійснюється повністю або частково із застосуванням автоматизованих засобів, а також на обробку персональних даних, що містяться

в картотеці чи призначені до внесення до картотеки, із застосуванням неавтоматизованих засобів [9];

– Закон України «Про друковані засоби масової інформації (пресу) в Україні». Закон створює правові основи діяльності друкованих засобів масової інформації в Україні, встановлює державні гарантії їх свободи відповідно до Конституції України, Закону України «Про інформацію» та інших актів чинного законодавства і визнаних Україною міжнародно-правових документів [3];

– Закон України «Про телебачення та радіомовлення». Закон регулює діяльність телерадіоорганізацій та території України, визначає правові, економічні, соціальні, організаційні умови їх функціонування, спрямовані на реалізацію свободи слова, права громадян на отримання повної, достовірної та оперативної інформації, на відкрите і вільне обговорення суспільних питань [4];

– Закон України «Про Суспільне телебачення і радіомовлення України». Нормативно-правовий акт, що регулює питання створення та діяльності суспільних засобів масової інформації – телебачення та радіомовлення. Зазначені ЗМІ мають статус незалежних структур, діяльність яких контролюється Громадською радою, до її складу залучаються відомі та незалежні громадські діячі та профільні фахівці [11];

– Закон України «Про порядок висвітлення діяльності органів державної влади та органів місцевого самоврядування в Україні засобами масової інформації». Закон відповідно до Конституції України визначає порядок всебічного і об'єктивного висвітлення діяльності органів державної влади та органів місцевого самоврядування засобами масової інформації і захисту їх від монопольного впливу органів тієї чи іншої гілки органів державної влади або органів місцевого самоврядування, є складовою частиною законодавства України про інформацію [7];

– Указ Президента України Про рішення Ради національної безпеки і оборони України від 15 жовтня 2021 року «Про Стратегію інформаційної безпеки». Затверджена Стратегія визначає актуальні виклики та загрози національній безпеці України в інформаційній сфері, стратегічні цілі та завдання,

спрямовані на протидію таким загрозам, захист прав осіб на інформацію та захист персональних даних. Основними напрямками забезпечення інформаційної безпеки України є стійкість та взаємодія, для досягнення яких необхідним є виконання таких стратегічних цілей: протидія дезінформації та інформаційним операціям, насамперед держави-агресора, спрямованим, серед іншого, на ліквідацію незалежності України, повалення конституційного ладу, порушення суверенітету і територіальної цілісності держави, пропаганду війни, насильства, жорстокості, розпалювання національної, міжетнічної, расової, релігійної ворожнечі та ненависті, вчинення терористичних актів, посягання на права і свободи людини; забезпечення всебічного розвитку української культури та утвердження української громадянської ідентичності; підвищення рівня медіакультури та медіаграмотності суспільства; забезпечення дотримання прав особи на збирання, зберігання, використання та поширення інформації, свободу вираження своїх поглядів і переконань, захист приватного життя, доступ до об'єктивної та достовірної інформації; створення ефективної системи стратегічних комунікацій; розвиток інформаційного суспільства та підвищення рівня культури діалогу [15];

– Указ Президента України «Про рішення Ради національної безпеки і оборони України від 29 грудня 2016 року «Про Доктрину інформаційної безпеки України». Основною метою реалізації положень Доктрини інформаційної безпеки України є створення в Україні розвиненого національного інформаційного простору і захист її інформаційного суверенітету. Забезпечення інформаційної безпеки України має здійснюватися за такими принципами: свобода збирання, зберігання, використання та поширення інформації; достовірність, повнота та неупередженість інформації; обмеження доступу до інформації виключно на підставі закону; гармонізація особистих, суспільних і державних інтересів; запобігання правопорушенням в інформаційній сфері; економічна доцільність; гармонізація українського законодавства в інформаційній сфері з міжнародним; пріоритетність національної інформаційної продукції [13].

Насамперед, варто зауважити, що в Україні інформаційний простір досі залишається неврегульованим та не розроблено єдиної законодавчої практики у протидії дезінформації, що зумовлює неконтрольованість застосування маніпулятивних процесів та поширення недостовірної інформації.

Проте зазначені закони України не відповідають сучасним викликам, зокрема у них відсутній термін «дезінформація» та «фейк». Станом на 2022 р. в Україні розроблено два законопроекти «Про медіа» та «Про дезінформацію», що враховуватимуть попередні прогалини у законодавстві, проте окремі пункти досі залишаються дискусійними.

У законодавстві України питання поширення дезінформації у медіа розглядаються частково у низці згаданих вище законів, що регулюють діяльність засобів масової інформації. Проте вони не відповідають сучасним викликам, зокрема залишається неврегульованим інформаційний простір та не розроблено єдиної законодавчої практики у протидії дезінформації.

Отже, враховуючи динамічний характер розвитку та постійне удосконалення технологій впливів у маніпулюванні суспільною думкою, відсутність однозначності у визначеннях основної термінології та нерепрезентативність певної частки досліджень зумовлює подальше активне вивчення дослідниками та науковцями маніпулятивних процесів.

Таким чином, у першому розділі розглянуто походження та сутність понять «дезінформація», «фейк» та «інформаційні маніпуляції», розглянуто різні підходи до їх трактування, схарактеризовано погляди різних науковців на них, завдяки аналізу наукових джерел досліджено риси, притаманні цим поняттям; описано методи наукового дослідження, за допомогою яких вдалося вирішити завдання, які перед мною стояли, в ході дослідження та досягнути поставленої мети, а також було досліджено законодавчі та нормативно-правові документи, які становлять правову основу інформаційної безпеки України.

РОЗДІЛ 2

ДЕЗІНФОРМАЦІЯ ТА ФЕЙКИ ЯК ЗАСІБ ІНФОРМАЦІЙНИХ МАНІПУЛЯЦІЙ

2.1. Структура дезінформації та фейків в умовах війни Росії проти України, їх класифікація та канали поширення

Разом з розвитком інформаційного суспільства й сучасними досягненнями в галузі інформаційних технологій розвивається мережа «Інтернет». Інтернет, крім виконання функцій обміну думками й отримання інформації його користувачами в період інформаційного протистояння, стає об'єктом і засобом інформаційного керування. Серед користувачів мережі з'являються групи людей або окремі особи, які навмисно поширюють помилкову або спотворену інформацію.

У мережі з'являється дедалі більше фейків або вкидів – неправдивих повідомлень, які підкріплюються підробленими фото, свідченнями псевдоочевидців і відео. Найзручнішим місцем їх поширення є соціальні мережі. Популярність соцмереж зробила можливим не тільки миттєве поширення будь-якої інформації чи дезінформації, а й прямий доступ до політичної, військової та іншої еліти країни супротивника й лідерів думок через їхні акаунти. Якщо додати до цього, що соцмережі дають можливість майже ідеально маскувати проведення операцій психологічного впливу, то стає беззаперечно очевидним: соцмережі є надзвичайно ефективним інструментом ведення інформаційної війни [68].

Дезінформація – це спосіб психологічного впливу, що полягає в намірі подання об'єктові такої інформації, яка вводить його в оману стосовно справжнього стану справ та створює викривлену реальність. Поширення перекручених, неповних або свідомо неправдивих відомостей для досягнення

пропагандистських, військових (введення противника в оману), комерційних або інших цілей.

Фейк – це різновид дезінформації, навмисне подання неправдивої інформації. Фейк можна сприймати як жарт – навмисне перекручення фактів, аби викликати позитивні емоції, сміх тощо, проте все частіше фейк перетворюється на справжню дезінформацію, яка вводить в оману.

Тему фейку в новинах досі не було ретельно вивчено та описано дослідниками у галузі журналістики. Її актуальність сьогодні, в умовах інформаційної війни з Росією, є безперечною – адже фейкові новини, спрямовані на дестабілізацію ситуації в нашій країні, російські ЗМІ продукують мало не щодня [44].

Дезінформація розповсюджується дуже швидко саме тому, що її автори намагаються скористатися нашими емоціями та упередженнями.

І йдеться не лише про негативні емоції – інколи обнадійливі історії також можуть стати вірусними. Вони підіймають бойовий дух, але ускладнюють розуміння того, що відбувається насправді, й сприяють хаосу.

Дезінформація породжує плутанину та недовіру, а також зменшує віру людей в інституції, які мають вирішальне значення для функціонування здорової демократії, як-от уряд, ЗМІ тощо. Це підриває здатність громадян ефективно брати участь у житті суспільства за допомогою голосування та інших громадських заходів. Дезінформація також може спонукати людей приймати рішення, які негативно впливають на особисте здоров'я, безпеку та фінансове становище суспільства [76].

Дезінформація – це передусім процес маніпулювання інформацією з метою введення певної цільової аудиторії, перед тим як ця аудиторія прийматиме певне важливе рішення, в оману шляхом надання їй неповної інформації, викривлення контексту цієї інформації або певної частини інформації. Мета такого інформаційного впливу завжди зводиться до намагання нав'язати цільовій аудиторії проєкт рішення, вигідний маніпулятору. Хоча може йтися й

про відмову від прийняття невігідного для маніпулятора рішення. У будь-якому разі кінцева мета – це дія або бездіяльність цільової аудиторії [59].

Отже, поняття дезінформації та фейк мають як спільні, так і відмінні риси. Спільною рисою, яка притаманна цим поняттям є те, що вони цілеспрямовано поширюють інформацію з конкретною метою. Відмінними рисами є те, що дезінформація спрямована виключно на деструктивні наслідки, в той час як фейк може все-таки бути конструктивним.

Фейки стосуються не лише соціальних мереж. Це битва, яку ведуть уряди як України, так і Росії. Тому треба розуміти, чому те чи інше джерело щось говорить та чи підтверджується це доказами.

В Україні слово «фейк» звучить з екранів телевізорів, у ЗМІ. Термін «фейк» (англ. fake – підробка) має багато значень. Часто фейком називають недостовірну, неправдиву інформацію. Але таке визначення не відображає суті фейку. Адже фейк – це підробка, фальшивка, яка поширюється спеціально для того, щоб дезінформувати аудиторію [44].

Для того, щоб якась інформація потрапила в інтернет, не треба бути журналістом чи власником якогось медіа. Варто лише запостити цю інформацію у соцмережі, на твіттері, у блозі тощо та позначити правильним тегом, щоб пост дістався до цільової аудиторії. Зробити це може будь-хто і саме тому в Інтернет потрапляє неймовірно багато інформації, яка є неправдою. Так, часто люди помиляються. Проте, все частіше неправдиву інформацію пишуть з певною метою.

Відповідаючи на запитання “для чого поширювати брехню?”, можна виділили декілька типів фейків залежності від їхнього завдання, зокрема які:

- сіють паніку серед людей;
- розпалюють міжнаціональну (расову, релігійну тощо) ворожнечу;
- поширюють хибні думки для того, щоб заплутати нас, відволікти від правди;
- маніпулюють свідомістю;
- рекламують когось або щось;

- приносять прибуток ЗМІ, що його поширює («жовта преса»);
- плямують чиюсь репутацію (найчастіше це фото, добре опрацьовані у Photoshop);
- мають розважальний характер (трохи детальніше про них поінформуємо пізніше).

Неправдивою інформацією засмічують інформаційне поле за допомогою коментарів (найчастіше з тих самих, фейкових, акаунтів), хештегів (особливо в години, коли цей хештег є найпопулярніший, і люди шукають інформацію за темою хештега, спамери починають свою інформаційну атаку).

Велика кількість дослідників феномену «фейкові новини» намагались класифікувати та виокремити фейки за типами. Враховуючи це, у нашому дослідженні здійснено аналіз чотирьох класифікацій, які найширше та найповніше охоплюють спектр фальшивих новин. У 2018 р. група вчених з Наньянського технологічного університету дослідила 34 наукові статті про фейкові новини за 2003-2017 рр.

У своїй роботі «Defining Fake News: A typology of scholarly definitions» Едсон Тандок виділяє шість типів фейків відповідно до їх змісту:

- новинна сатира;
- пародія на новину;
- фальсифікація;
- маніпуляція;
- реклама;
- пропаганда [67].

Через іншу призму розглядає поділ фейкових новин Д. Лавникевич. Дослідник класифікує продукування фальшивих матеріалів відповідно до мотивів, зокрема виділяє такі:

- фейки, що створені випадково. Джерела їх походження – неуважність редактора, поспіх у роботі редакції, одрук, некомпетентність журналіста. Вони створюються або в наслідок поспіху редакції випустити номер, матеріал, або внаслідок родруківки, некомпетентності журналіста;

– фейки, що продукуються в межах інформаційної війни. Приклад цьому російсько-український конфлікт, який посилюється зокрема і через продукування недостовірної інформації;

– фейки, що створені комерційними структурами. Цю групу складають псевдонаукові розробки торгових марок задля ефектних слоганів бренди часто вдаються до «досліджень», за результатами яких запускається лінійка продукту, що завдяки неправдивому опису набув популярності завдяки своїм неперевершеним властивостям. До цієї групи можна також відносити PR технології;

– фейки, що створені з метою залучення читацької аудиторії. До таких фейків відносять неправдиві гумористичні матеріали з лихим умислом. Для досягнення цієї мети ЗМІ публікують завідома неправдиву інформацію, посиляючись на власні надійні джерела;

– фейки, що створені з невідомою метою. До цього класу відноситься «жовту пресу», зокрема неточну, перефразовану або неправдиву інформацію, яка частіше за все розповсюджується з розважальною метою [54].

Остання класифікація, на яку варто звернути увагу, належить директору проекту First Draft News К. Уордл. В своєму дослідженні Клер Улодл взяла тип контенту за основу розподілу фейкових новин, в якому їх використовують, мотиви особи, яка їх створює, а також засоби поширення таких новин [67]. Відповідно до класифікації дослідниці виокремлено сім видів фейкових новин, а саме:

- фейкові ролики розважального характеру (пародія або сатира);
- фейкові публікації з оманливим зв'язком. До цієї групи належать заголовки, матеріали, текст і зображення які не пов'язані між собою);
- фейковий контент. До цієї групи належать неповна, перекручена або хибна інформація, яку використовують з метою дискредитації факту, події, особи;
- контент «самозванця». Дійсні достовірні джерела інформації спеціально видають себе за фейкові;

- фейкова ситуація. Такі фейки відображають реальний контент, який наповнений брехливою контекстуальною інформацією;
- сфальсифікований контент. Це класичні фейкові новини – повністю хибна інформація, мета якої – ввести в оману реципієнта або нашкодити йому;
- маніпулятивний контент. Інформація (правдива або сфальсифікована), що має на меті маніпуляцію. Такий контент може бути підкріплений фейковими фото або відео [67].

Здійснивши глибинний аналіз кількості фейкових новин в українському інтернет-просторі вважаємо, що варто розрізняти фейкові новини за масштабністю описаних подій. Саме тому доцільно поділити фейкові новини на:

- місцеві (які стосуються певного – населеного пункту, міста, району або області);
- регіональні (пов’язані з окремим регіоном в межах однієї країни);
- всеукраїнські (або такі що створюються в масштабах будь-якої іншої країни);
- світові (стосуються кількох країн).

За сферою поширення фейкові новини також поділяють на:

- політичні фейки;
- соціальні фейки;
- культурні фейки;
- спортивні фейки;
- економічні фейки;
- наукові фейки та ін.

Отже, враховуючи вищезазначене можна з впевненістю стверджувати, що фейкові новини розповсюджуються на всі сфери людської життєдіяльності. Для кожної сфери такі неякісні новини можуть мати згубний вплив та незворотні наслідки.

Варто зауважити, що фейкові новини можна розглядати з точки зору їх тривалості, а саме:

– короткотривалі фейки (вони, як правило, публікуються в інтернет мережі, живуть від кількох годин до кількох днів, а потім швидко розвінчуються);

– довготривалі фейки (такі можуть існувати від року до десятків років)

Відповідно до вищезазначеного фейки можна поділити на вербальні (тексти та заголовки до них) та полікодовані (ті, що містять невербальні засоби

– фото, зображення, малюнки, карикатури, тощо).

Якщо класифікувати фейкові новини за метою створення, то можна виокремити:

– фейки, що створені з метою привернення уваги громадян до події (можливо, вигаданої), факту або явища;

– фейки, що створені з метою піару .

До такого брудного піару часто вдаються політики та зірки шоубізнесу. Вони розповсюджують завідома неправдиву інформацію, щоб підняти рейтинги своєї популярності та привернути увагу людей. Як правило, рано, чи пізно правда стає відомою, а особа, яка розпустила фейк – отримала безкоштовний піар свого прізвища у ЗМІ.

Отже, не існує уніфікованої класифікації фейкових новин. Медіа-експертами (як вітчизняними, так і іноземними) запропоновано чимало моделей поділу фейкових новин, проте наразі така класифікація відсутня.

Розмаїття фальшивих новин та їх постійні модифікації дозволяють запропонувати чимало нових критеріїв, за якими можна розподілити фейковий контент, а саме: за часом існування, метою створення, тематикою та масштабом.

Український інформаційний простір сьогодні зазнає значного впливу, так як війна триває не тільки на території країни, але й в її інформаційному полі.

Кремлівську риторику, фейки можуть підхоплювати і інші ЗМІ, сприймаючи таку інформацію як «альтернативну точку зору», чи таку інформацію, яка підвищить клікабельність.

Найголовнішою перемогою тих, хто поширює дезінформацію та фейки, є саме підхоплення цих матеріалів найбільш популярними, головними масмедіа,

навіть, якщо це згадування відбувається у формі спростування. Посилення й поширення нарративу є одними з основних цілей пропагандистів.

Процес розповсюдження фейків має властивості інформаційних операцій:

– високий ступінь подібності текстів, не будучи повними дублікатами;

– невеликий інтервал часу, в який відбувається їх опублікування. Це дозволяє імітувати появу нової значущої події;

– джерела, які опублікували їх, є маловідомими, регіональними або спеціалізованими ЗМІ. Поява повідомлень у великих інформаційних агентствах можлива тільки під час пасивної фази.

Поширення фейків – це один із видів інформаційних операцій – взаємопов’язаних послідовностей інформаційних впливів для досягнення поставленої мети. Вони дозволяють приховати факт їх проведення, але при цьому отримати цільовий ефект, мають низку вартість проведення, ефект від їх проведення реальний (зміна курсу акцій компанії, активні дії частини населення, втрата довіри до політичного або громадського діяча). Фейкова новина спонукає до різкої розбіжності думок, різного роду конфліктів, включаючи політичні.

Сьогодні, мало не кожен день на екранах телевізорів, у стрічках новин можна зустріти слово «фейк». Цей термін увібрав в себе різноманіття інтерпретацій. Зазвичай, під терміном «фейк» розуміють перекручену неправдиву інформацію. Втім слід зрозуміти правильний сенс цього слова, фейк – це брехня, підробка, фальсифікація, яка розповсюджується цілеспрямовано для того, щоб дезінформувати та ввести в оману певну аудиторію.

Термін «фейкові новини» є як повністю або частково вигаданою інформацією про суспільні події, явища, певних осіб, яка подається в ЗМІ під виглядом справжніх журналістських матеріалів. Часто носять гумористичний або сатиричний характер і створюються з метою висміювання або привернення уваги до важливих суспільних проблем чи тенденцій. Тобто таке визначення фейкової інформації має позитивний і розважальний характер. Проте в сучасних українських соціальних медіа фейкова інформація спрямована на

дезінформацію, введення в оману аудиторії, що в результаті викликає не позитивні, а, навпаки, негативні емоції.

Зараз фейком може бути будь-що, відредаговані фото, штучно змонтовані відеоролики, написані або вигадані неправдиві новини, які важко відрізнити від правдивих. Ще фейками вважають заведені акаунти неіснуючих людей у соціальних мережах, через які поширюється недостовірна інформація.

Основною метою фейкових повідомлень як інструмента інформаційної війни – це змусити людей сумніватися, запевнити аудиторію в правдивості поданої інформації. Задача стоїть в дезінформуванні аудиторії; сприянні розвитку власного бачення, політики або позиції; спричиненні агресію; похитнути позицію індивіда та вимусити його сумніватися; розповсюдженні паніки; редагування мислення аудиторії; індукування певної дії; підвищення увагу й зацікавленості аудиторії; запевнення аудиторії використанням вигаданих фактів; залякуванні аудиторії тощо.

Враховуючи вище сказане слід зробити наступне визначення фейку. Фейк – це навмисно змінена новина, подія чи журналістська публікація, що включає в себе неправдиву або спотворену інформацію, що дискримінує певну особу чи групу людей в очах аудиторії.

Отже, як вже зазначено, фейками можуть бути фото, відео, новини, сторінки в соціальних мережах, створені від імені неіснуючої/іншої людини, програми, сайти, створені під виглядом відомих ресурсів з метою фішингу тощо. Виявити брехливість інформації, яку несе в собі фейк, набагато легше, якщо дотримуватися принципу обов'язкової перевірки і повторної перевірки інформації, що надходить в конкретне медіа за принципом «точність важливіше швидкості». Істотним фактором оцінки достовірності інформації є той канал комунікації, за допомогою якого вона надійшла до редакції.

Найбільш надійним засобом боротьби із інформаційними атаками є створення тотального ментального бар'єру, який може витримати будь-які несподіванки. При цьому отримувачі інформації будуть знаходитися на певних ідеологічних позиціях, що дозволить їм критично сприймати або взагалі не

сприймати шкідливу інформацію. Створення такого механізму є довготривалим процесом та передбачає налагодження системного інформування на основі мультимедійного ефекту та багатократного повторення певних попереджень, розкриття механізмів можливих маніпуляцій та типових фейків, з якими можуть стикнутися основна маса населення.

Формування такого роду захисту є комплексною роботою, до якої необхідно залучати зусилля та ресурси суспільства, держави та окремих громадських лідерів.

Найкращим форматом боротьби із інформаційними атаками є розвінчання фейку із тлумаченням характеру та реального змісту повідомлення.

Зважаючи на той факт, що переважна більшість інформаційних атак у форматі сьогочасних інформаційно-психологічних війн є анонімними, одним з ключових механізмів розвінчання є з'ясування та доведення до відома широкої громадськості авторів агресії або тих, на чию користь вона працює.

У залежності від характеру та специфіки інформаційної атаки до справи розвінчання необхідно залучати різного роду ресурси. Найбільш ефективними в цьому плані є неформальні або такі, що є авторитетними для відповідних цільових груп. До процесу розвінчання мають залучатися всі можливі ресурси – державні, громадські, індивідуальні.

Російська війна проти України призвела до появи в інтернеті чисельних фейкових відео і фото, які активно розповсюджують користувачі соціальних мереж. Інколи відрізнити їх від справжніх доволі важко, але є певні ознаки, на які варто звернути увагу, перш ніж повірити тому чи іншому фото чи відео:

1. Перше і найголовніше, щоб не стати жертвою в інформаційних маніпуляцій, слід довіряти лише офіційній інформації. Перелік офіційних джерел інформації:

- президент України Володимир Зеленський – в телеграмі, фейсбуці, твіттері;
- Офіс президента України – на сайті, в телеграмі, фейсбуці, твіттері;
- Генеральний штаб ЗСУ – в телеграмі, фейсбуці, твіттері;

- Кабінет Міністрів України – на сайті, у фейсбуці, твіттері;
- Міністерство оборони України – на сайті, у фейсбуці, твіттері;
- МВС України – на вебсайті, в телеграмі, фейсбуці, твіттері;
- Національна поліція України – на сайті, в телеграмі, фейсбуці, твіттері;
- Служба безпеки України – на сайті, в телеграмі, фейсбуці, твіттері;
- ДСНС України – на сайті, в телеграмі, фейсбуці, твіттері;
- Центр стратегічних комунікацій та інформаційної безпеки – на сайті, в телеграмі, фейсбуці;
- Державна служба спеціального зв'язку та захисту інформації України – на сайті, в телеграмі, фейсбуці, твіттері;

– тощо;

Перелік офіційних джерел інформації по Києву:

- мер Києва Віталій Кличко – в телеграмі, фейсбуці, твіттері;
- КМДА – на сайті, в телеграмі, фейсбуці, твіттері;
- Київська обласна військова адміністрація – на сайті, в телеграмі, фейсбуці;
- поліція Києва – на сайті, у фейсбуці, твіттері;
- ДСНС по Києву – у фейсбуці.

2. Перевірте, коли саме зняли те чи інше відео.

Автори багатьох фейкових роликів намагаються видати за нові ті відео, що були зроблені під час інших конфліктів. Часом подібні матеріали розповсюджують та «шерять» прості користувачі, які шоковані тим, що бачать, або хочуть допомогти

Завжди перевіряйте, чи є ознаки того, що відео старе. Наприклад, яка на ньому погода? Якою мовою говорять люди, які там знаки дорожнього руху?

Гугл карти допоможуть з'ясувати, чи дійсно відео зняли там, де каже автор. А за допомогою зворотного пошуку зображень, які є на низці вебсайтів, можна побачити, чи публікували це відео/фото раніше в інтернеті. Якщо так, це точна ознака того, що його переробили з попередньої події.

3. Завжди звертайте увагу на те, хто публікує той чи інший контент, і чи можна вважати це джерело авторитетним й таким, якому можна довіряти.

Деякі фейкові відео розповсюджують ті, хто прагне отримати якомога більше «шерів» і «лайків». Інші намагаються у такий спосіб просунути свої власні політичні погляди або сіяти сумніви і тривогу. Є також акаунти, де раніше поширювали фейки про пандемію Covid, а тепер сконцентрувалися на теоріях змови про війну.

4. Думайте перед тим, як натиснути на «поділитись». Відео та фото, що розповідають про війну, часто дуже страшні й викликають у людей емоційну реакцію, яка примушує їх одразу ділитися ними, навіть без додаткових перевірок [70].

Враховуючи вищенаведене, можна зробити висновок, що дезінформація та пропаганда є міжнародною проблемою та загрозою для суспільства. Дезінформація породжує плутанину та недовіру, а також зменшує віру людей в інституції, які мають вирішальне значення для функціонування здорової демократії, як-от уряд, ЗМІ тощо. Це підриває здатність громадян ефективно брати участь у житті суспільства за допомогою голосування та інших громадських заходів. Дезінформація також може спонукати людей приймати рішення, які негативно впливають на особисте здоров'я, безпеку та фінансове становище суспільства. А основна мета фейкових новин – не інформувати, на відміну від традиційних новин, а ввести в оману шляхом розповсюдження завідома неправдивої інформації.

2.2. Соціальні мережі та месенджери як канали поширення фейкової інформації (на прикладі тікток та вайбер).

Сервіс «Тікток» для створення і перегляду коротких відео став однією з основних платформ, де фейкові відео про війну в Україні збирають мільйони переглядів. Щомісячна кількість активних користувачів тіктоку сягнула мільярда, більша її частина молодше 30 років. Вони заходять на сервіс, щоб дізнатись новини про російсько-український конфлікт, тож платформа щосили намагається зупинити потік фейків.

Згідно з дослідженням NewsGuard, вебсайту, що відстежує дезінформацію в інтернеті, новим користувачам можуть рекомендувати неправдивий контент про Україну протягом 40 хвилин після приєднання до мережі. Тож сумнівний контент не потрібно навіть шукати [80].

Однак, якщо фейсбук, інстаграм і твітер позначають фейкові відео про війну, то тікток, схоже, не дуже за цим встигає. Тим не менш, компанія наполягає, що активізувала свої зусилля з боротьби з дезінформацією.

Ось деякі з найбільш поширених категорій фейкового контенту:

– фейкові прямі трансляції. З перших днів війни фейкові стріми збирали величезну кількість переглядів у тікток. Рецепт простий: користувач знаходить драматичне відео старого конфлікту чи якихось військових навчань, додає фейковий звук потужного вибуху чи інтенсивної перестрілки, запускає пряму трансляцію і, щойно збереться значна аудиторія, просить пожертвування на свій канал [80].

До середини березня один з таких акаунтів набрав майже 30 мільйонів переглядів. Усі, крім трьох прямих трансляцій, були короткими кліпами, взятими з відео на ютубі про старі українські військові навчання, датовані 2017 р. Приклад подібного фейкового акаунту представлено у додатку А;

– старі відео. Відео старих конфліктів зазвичай використовують, коли спалахує новий. ВВС бачила відео бойових дій у Лівії, Сирії та Чечні, які

видавали за конфлікт в Україні. Відео запеклого бою між російськими та українськими військами біля багатоквартирного будинку набрало 7,7 млн переглядів. Але насправді ці кадри були записані у 2014 р. у столиці Чечні Грозному під час смертоносного нападу джихадистів. Щоб приховати справжнє джерело, на оригінальні кадри наклали фейкові позначки екстрених новин та субтитри нібито прямого ефіру, що продемонстровано у додатку Б [80].

Відео колони українських танків у центрі Києва представили так, ніби вони прямують захищати столицю від російського наступу. Ролик отримав дев'ять мільйонів переглядів. Насправді ж його зняли кілька років тому під час військового параду до Дня незалежності України. Знімки екрану фейкового відео представлено у додатках В-Г [80].

Що стосується фейсбука та інстаграму, то вони в більшості випадків роблять відмітку, яка позначає, що це фейковий контент про Україну (прикладом цього є знімки екрану інстаграму наведені у додатках Д-Е), а в подальшому і зовсім видаляє публікацію, в тікток таке маркування зустрічається рідко, тому відповідальність лягає на кожного з нас, чи поширювати нам цю фейкову новину чи сісти проаналізувати спочатку її достовірність.

За результатами відповідних досліджень було встановлено, що станом на квітень 2022 р. найбільш поширеним серед населення додатком для обміну інформацією став вайбер, яким користуються майже 66% респондентів. Він лідирує серед усіх вікових груп. На вказаній позиції перебуває з 2018 р.

Друге місце посідає фейсбук месенджер, який використовують майже 35% опитаних. Проте лідирує додаток не скрізь. У віковій категорії «18-29 років» друге місце займає телеграм, який використовують 45% користувачів. Також у віковій групі «70 років і старші» опитані більше користуються вотсапом, ніж фейсбук месенджером.

Третє місце за кількістю користувачів займає телеграм – йому довіряють 24,2% користувачів.

Четверте та п'яте місце займають вотсап та твітер відповідно .

Зважаючи на об'єм доповіді та поширеність серед користувачів, вважаємо за доцільне більш детально зупинитися на характеристиці саме месенджеру вайбер. Отже, вайбер є додатком для дзвінків і обміну повідомленнями, який дозволяє створювати чат-боти та спільноти тощо.

Незважаючи на те, що вказаний додаток є для значного відсотку українців джерелом новинної інформації, за своїми ознаками він є аналогом смс-повідомлень (більш «прогресивна» версія).

Його поширеність та популярність обумовлена тим, що він став одним із перших каналів комунікації, який почали масово використовувати українці після стандартних текстових смс-повідомлень. Зважаючи на те, що першочергово ми писали рідним, близьким людям, друзям у вайбер, на підсвідомому рівні, сформувалося коло людей, яким ми довіряємо (т.зв. «коло довіри»). Разом з тим, в умовах сьогодення, месенджер перестав використовуватися виключно як «інструмент для спілкування», а став платформою для «викривлення інформаційного поля».

Наразі, вказане «коло» значно розширилося. У більшості користувачів в додатку є значна кількість чатів (спільнот) з тисячами учасників. Зважаючи на вказане, фізично відсутня можливість ідентифікувати осіб, які розміщують відповідні дописи. При цьому, психологічно, ми продовжуємо сприймати вайбер як «зону безпеки». Вказана підсвідома реакція людського мозку активно використовувалася з метою оперативного поширення тенденційної інформації задля впливу на вільне волевиявлення громадян.

Доведено, що з метою швидкого розповсюдження вказаної інформації та штучного підняття інтересу до неї активно застосовувалися технічні можливості ботоферм, в тому числі й тих, які розміщувалися на території Російської Федерації.

Отже, проаналізувавши психологічні та технічні прийоми, які використовуються зловмисниками при підготовці та поширенні у додатку фейкового чи деструктивного контенту, можна зробити висновок, що вони, в першу чергу, використовують властивість людської психіки обумовлену

бажанням вберегти від небезпеки своїх близьких та рідних (як вже зазначалося: на підсвідомому рівні вайбер = «коло довіри»).

Таким чином, у другому розділі проаналізовано структуру дезінформації та фейків в умовах війни Росії проти України, їх класифікацію; описано канали їх поширення; визначено ознаки, на які варто звернути увагу, перш ніж повірити тій чи іншій новині; виділено соцмережі та месенджери, які українці найчастіше використовують для отримання новин, проаналізовано контент, який висвітлюється в цих засобах отримання інформації та показано приклади фейкової інформації у зазначених соціальних мережах та месенджерах.

РОЗДІЛ 3

МЕТОДИ ПРОТИДІЇ ІНФОРМАЦІЙНИМ МАНІПУЛЯЦІЯМ

3.1. Моніторингове дослідження протидії дезінформації та фейкам в інформаційному просторі України на прикладі Центру протидії дезінформації та видання «Українська правда» (лютий – листопад 2022 р.)

Для боротьби з фейковою інформацією та маніпуляціями держава створила відповідні інституції. Одним з них є саме Центр протидії дезінформації.

Центр протидії дезінформації (АНГЛ. CENTER for Countering Disinformation) – робочий орган Ради національної безпеки і оборони України, утворений відповідно до рішення Ради національної безпеки і оборони України від 11 березня 2021 р. «Про створення Центру протидії дезінформації», уведеного в дію Указом Президента України від 19 березня 2021 р. № 106 [14].

Центр забезпечує здійснення заходів щодо протидії поточним і прогнозованим загрозам національній безпеці та національним інтересам України в інформаційній сфері, забезпечення інформаційної безпеки України, виявлення та протидії дезінформації, ефективної протидії пропаганді, деструктивним інформаційним впливам і кампаніям, запобігання спробам маніпулювання громадською думкою [63].

Робота Центру протидії дезінформації охоплює такі сфери, як воєнний напрям, боротьбу зі злочинністю та корупцією, зовнішню та внутрішню політику, економіку, інфраструктуру, екологію, охорону здоров'я, соціальну сферу та науково-технологічний напрям. Але основна увага зосереджена на протидії поширенню неправдивої інформації в інтернеті та фейків у медіа. Центр не має каральних функцій за дезінформацію і не зможе застосовувати санкції, але може вносити подання до РНБО щодо певних порушень [37].

Основними завданнями Центру є:

1. Проведення аналізу та моніторингу подій і явищ в інформаційному просторі України, стану інформаційної безпеки та присутності України у світовому інформаційному просторі.

2. Виявлення та вивчення поточних і прогнозованих загроз інформаційній безпеці України, чинників, які впливають на їх формування, прогнозування та оцінка наслідків для безпеки національних інтересів України.

3. Забезпечення Ради національної безпеки і оборони України, Голови Ради національної безпеки і оборони України інформаційно-аналітичними матеріалами з питань забезпечення інформаційної безпеки України, виявлення та протидії дезінформації, ефективної протидії пропаганді, деструктивним інформаційним впливам і кампаніям, запобігання спробам маніпулювання громадською думкою.

4. Підготовка та внесення Раді національної безпеки і оборони України, Голові Ради національної безпеки і оборони України пропозицій щодо:

– визначення концептуальних підходів у сфері протидії дезінформації та деструктивним інформаційним впливам і кампаніям;

– координації діяльності та взаємодії органів виконавчої влади з питань національної безпеки в інформаційній сфері, забезпечення інформаційної безпеки, виявлення та протидії дезінформації, ефективної протидії пропаганді, деструктивним інформаційним впливам і кампаніям, запобігання спробам маніпулювання громадською думкою;

– здійснення системних заходів, спрямованих на посилення спроможностей суб'єктів сектору безпеки та оборони, інших державних органів задля забезпечення інформаційної безпеки, виявлення та протидії дезінформації, ефективної протидії пропаганді, деструктивним інформаційним впливам і кампаніям, запобігання спробам маніпулювання громадською думкою, розвитку національної інфраструктури у відповідній сфері;

– удосконалення системи правового та наукового забезпечення інформаційної безпеки, виявлення та протидії дезінформації, ефективної

протидії пропаганді, деструктивним інформаційним впливам і кампаніям, запобігання спробам маніпулювання громадською думкою.

5. Участь у розбудові системи стратегічних комунікацій, організації та координації заходів щодо її розвитку.

6. Участь у розробленні та реалізації Стратегії інформаційної безпеки України, здійсненні аналізу стану її реалізації, зокрема з питань ефективності заходів щодо протидії дезінформації.

7. Участь у створенні інтегрованої системи оцінки інформаційних загроз та оперативного реагування на них.

8. Розроблення методології виявлення загрозливих інформаційних матеріалів маніпулятивного та дезінформаційного характеру.

9. Сприяння взаємодії держави та інституцій громадянського суспільства щодо протидії дезінформації та деструктивним інформаційним впливам і кампаніям, організація та участь в інформаційно-просвітницьких заходах з питань підвищення медіа-грамотності суспільства.

10. Вивчення, узагальнення й аналіз досвіду інших держав і міжнародних організацій з протидії дезінформації та підготовка пропозицій щодо його використання в Україні.

11. Визначення пріоритетів залучення міжнародної технічної допомоги з питань забезпечення інформаційної безпеки, виявлення та протидії дезінформації, ефективної протидії пропаганді, деструктивним інформаційним впливам і кампаніям, запобігання спробам маніпулювання громадською думкою [32], [71].

Другим джерелом інформації, який я моніорила стало видання «Українська правда» – українське суспільно-політичне інтернет-ЗМІ, яке заснував Георгій Гонгадзе у квітні 2000 р. Після смерті Гонгадзе у вересні 2000 р. редакцію очолила співзасновниця видання Олена Притула, яка залишалась головним редактором «Української правди» до 2014 р., поки не передала посаду Севгіль Мусаєвій. У травні 2021 р. новим власником видання став генеральний директор Dragon Capital Томаш Фіала [31].

Видання відіграло важливу роль у наданні інформації громадськості під час Помаранчевої революції 2004 р. та було форпостом української розслідувальної журналістики у 2007–2010 рр.

Інститут масової інформації у 2015–2017 рр. визначав «Українську правду» як одного з лідерів з дотримання журналістських стандартів серед всеукраїнських інтернет-видань.

Згідно з Інститутом масової інформації 2020 р. «Українська правда» увійшла до «білого списку» українських медіа. Цей список включає медіа, які мають рівень якісної інформації понад 95 % [49].

В українському антирейтингу новин, за версією Інституту масової інформації та порталу Texty.org.ua, «Українська правда» посіла 44 місце з 50. В аналізі виявлено 98 вірогідних новин, одна новина з ненадійними джерелами інформації та одна невірогідна новина. Дослідження проводилось у межах проекту «Розвиток відповідальних інтернет-ЗМІ» за підтримки Міністерства іноземних справ Чеської республіки у червні-серпні 2018 р.

У вересні 2019 р. «Українська правда» потрапила до рейтингу Інституту масової інформації як популярний новинний сайт, що демонструє середній рівень прозорості. Дослідження проводилось за підтримки Фонду розвитку ЗМІ Посольства США в Україні та охопило 50 найпопулярніших новинних сайтів українського сегмента інтернету (за даними SimilarWeb).

У квітні 2020 р. «Українська правда» потрапила на друге місце у списку найякісніших ЗМІ щодо дотримання професійних стандартів, за результатами аналізу, проведеного Інститутом масової інформації. Згідно з даними дослідження, на сайті УП рівень дотримання професійних стандартів становив 97,5 %. Переважну більшість новин на ресурсі було написано без жодних порушень професійних стандартів журналістики. Так, стандарт балансу та відокремлення фактів від коментарів на сайті було дотримано в 99 % матеріалів. Рівень дотримання вірогідності ще вищий і становить 99,5 % [45].

У березні 2022 р. ІМІ рекомендував інтернет-ЗМІ «Українська правда», як достовірне медіа, якому можна довіряти [48].

Загальна кількість фейків, виявлених Центром протидії дезінформації та виданням «Українська правда», наведено на рисунку 3.1.1 [31], [34].

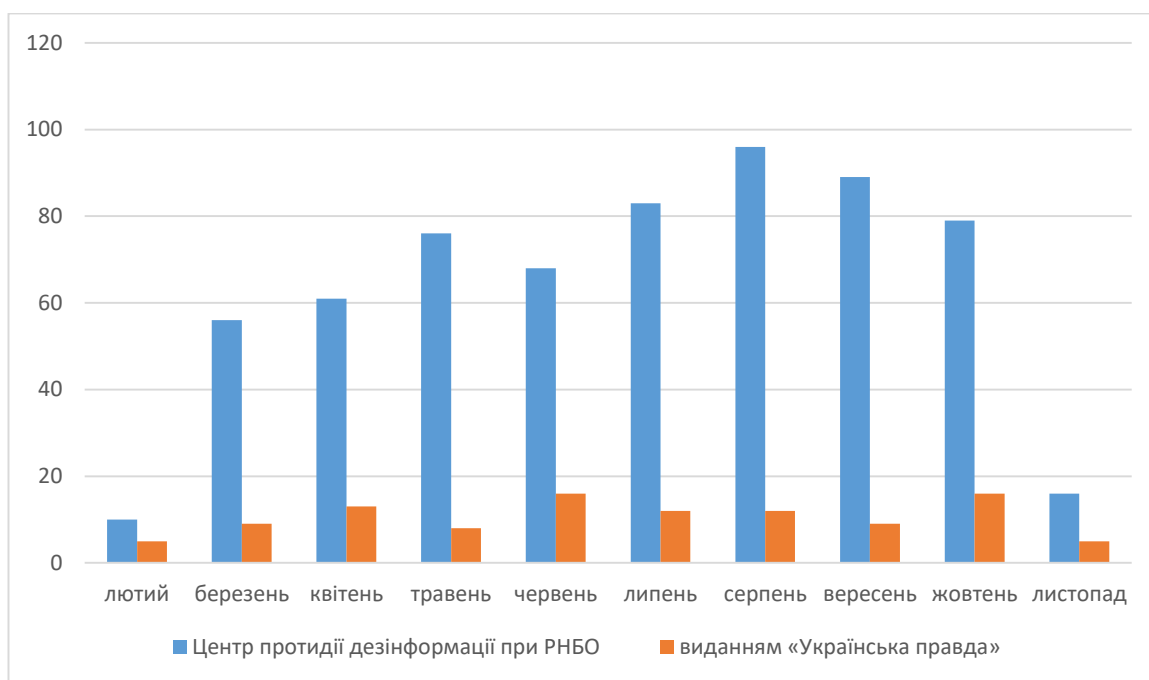


Рисунок 3.1.1– Загальна кількість фейків, виявлених Центром протидії дезінформації та виданням «Українська правда» за лютий–листопад 2022 р.

Отже, лідером у виявленні і представленні фейкової інформації є, звісно, Центр протидії дезінформації при РНБО, так як він, відповідно, цим займається, але не розвінчує фейки, а просто констатує факт, що та чи інша інформація є неправдивою. Центром протидії дезінформації при РНБО було виявлено 632 фейкові новини. Щодо видання «Українська правда», то ним було виявлено всього 105 фейків, але, варто зазначити, що окрім новин, які публікуються, вони пропонують статті, які раніше публікувалися на цю тему, в кожній статті зазначається передісторія питання, для того щоб допомогти читачеві розібратися в цьому матеріалі, вдаються в деталі, пояснюють новину, розвінчують фейкову інформацію, в кінці статей вони зазначають джерело, звідки взялась ця інформація для того, щоб читач міг сам в іншому джерелі перевірити точність цієї інформації, також, цитуючи людину, яка інформує про щось, зазначають її

ім'я і посаду, для того, щоб запевнитись, що це сказала людина, яка має на це повноваження.

3.2. Досвід України з протидії інформаційним маніпуляціям в умовах інформаційної війни Росії проти України

Гібридна війна відбувається, як мінімум, у чотирьох зонах – зоні прямого збройного протистояння, зоні ворожого тилового населення, зоні власного населення, зоні міжнародної спільноти.

Застосування Російською Федерацією технологій гібридної війни проти України перетворило інформаційну сферу на ключову арену протиборства. Саме проти України Російська Федерація використовує найновіші інформаційні технології впливу на свідомість громадян, спрямовані на розпалювання національної і релігійної ворожнечі, пропаганду агресивної війни, зміну конституційного ладу насильницьким шляхом або порушення суверенітету і територіальної цілісності України [13].

Одним із проявів інформаційної складової гібридної війни сьогодні є здійснення масових «вкидів» у вітчизняний інфопростір, що мають на меті викривлення реалій українського життя, підрив довіри до управлінських структур, а також переконання у безперспективності української державності тощо.

Специфіка цієї складової гібридної війни РФ проти України полягає в:

- інтенсивності та широті охоплення аудиторії інформаційним впливом, яка набула глобального масштабу;
- систематичному й комплексному застосуванні медійних та новомедійних засобів;
- створенні нового дискурсу війни, спрямованого на руйнування існуючих і формування нових інтерпретаційних та смислових механізмів сприйняття дійсності [40].

Слід зауважити, що інновацією сучасної інформаційної складової гібридної війни є дедалі ефективніше і всеохоплююче проникнення в інфопростір об'єкта агресії за допомогою сучасних технологій і, як результат – підвищення ефективності інформаційного впливу на його населення.

Очевидно, що в умовах триваючого гібридного протистояння забезпечення інформаційної безпеки України має включати не лише захист вітчизняного інформаційного простору від негативних впливів, а й створення та використання власних інформаційно-аналітичних продуктів, які виявлятимуть недоліки та прорахунки у суспільному житті противника.

Розглядаючи РФ як об'єкт інформаційних впливів в рамках гібридної війни останньої проти України, варто мати на увазі такі її особливості – до її істотних проблем можна віднести відсутність чіткої перспективи розвитку та орієнтирів у майбутньому, а також фактичне обмеження розвитку економіки Росії інтересами її олігархічних монополій, зацікавлених здебільшого у використанні багатих сировинних ресурсів країни, також сучасна Росія є однією з найбільших мультинаціональних держав, на території якої проживає понад 190 народів. Крім росіян до їх числа входять не лише малочисельні корінні народи, а й представники багатьох інших національностей, які раніше входили до складу СРСР, і чи не найбільша кількість – вихідці з України. Хоча їх вважають росіянами вже не одне покоління, проте в їхній самосвідомості все ще може зберігатися український етнічний елемент. Цю обставину слід враховувати при підготовці інформаційних продуктів, що орієнтовані на регіони, населені, ментально близькими нам мешканцями РФ, а також при підготовці інформаційноаналітичних матеріалів, спрямованих на нейтралізацію зарубіжних інформаційних впливів на населення України.

Таким чином, варто правильно зосередити зусилля на здійсненні інформаційного впливу на найбільш податливу частину аудиторії противника. Крім того, доцільно висвітлювати проблеми та слабкі сторони РФ з метою створення об'єктивної «картини світу» в свідомості її населення.

Основні інструменти, що активно використовуються РФ для пропаганди, є такими:

1. Російська система медійного впливу:

– всеросійська державна телевізійна і радіомовна компанія (телеканали «Россия-1», «Россия-2», «Россия-24», «РТР-планета», EuroNews; інтернет-проекти «Россия», «Вести.ru», «Страна друзей», Digitalrussia.tv, «Страна.ru» та інші);

– міжнародне інформаційне агентство «Россия сегодня» (телеканал Russia Today, новинне відеоагентство Ruptly, міжнародна інтернет-студія Sputnik, РІА «Новости», сайт Ria.ru та інші);

– перший канал Росії («Первый канал. Всемирная Сеть»), на базі якого запущений «Первый Балтийский канал», мовлення якого поширене на Латвію («ПБК Латвия»), Естонію («ПБК Эстония»), Литву («ПБК Литва»).

– медіа «Газпрому» (телеканали «НТВ», «ГНТ»; супутникова телекомпанія «НТВПЛЮС»; радіостанції СІТІ-FM, «Эхо Москвы», «Авторадіо», «101.ru»; видавництво «Семь дней»; кіностудії «НТВкіно», «Централ Партнершип»; інтернет-портали Rutube і Now.ru та інші);

– Національна Медіа Група (НМГ), яка позиціонує себе як приватний медіахолдинг (телеканали «Пятый канал», «РЕН ТВ», LifeNews TV; газета «Вести», сайт LifeNews.ru; студія «Российская служба новостей»);

– Russia Beyond the Headlines – міжнародний видавничий проєкт «Российской газеты», який періодично виходить безкоштовним друкованим і електронним додатком до найвідоміших видань світу 16 мовами (The Washington Post (США), The New York Times (США), The Daily Telegraph (Велика Британія), Le Figaro (Франція), Zuddeutsche Zeitung (Німеччина), The Economic Times (Індія), Folha de Sao Paulo (Бразилія), La Repubblica (Італія), JoongAng Ilbo (Південна Корея), China Business News (Китай) та інші).

2. Російські засоби мережевої комунікації:

– соціальні мережі «Одноклассники», «ВКонтакте» і «Мой Мир»,

– інстант-месенджер «Агент Mail.Ru» з поштовим сервісом ICQ, які з 2014 року повністю зосереджені в руках російської інтернеткомпанії Mail.Ru Group.

3. Програмно-комп'ютерні і мережеві елементи впливу:

– «Лаборатория Касперского»;
– проєкт «Киберберкут»;
– спеціальні підрозділи кібербезпеки ФСБ, МВС, МО РФ та інших структур;

– організації інтернет-тролів (селище Ольгіно (Санкт-Петербург), селище Яблоновське (Республіка Адигея), селище Перекат (Республіка Адигея), селище Зелений Город (Нижегородська обл.), м. Белгород, м. Рязань, м. Хабаровськ, м. Калінінград та інші. Найвідомішою з-поміж цих організацій є ТОВ «Интернет-исследования» (м. Санкт-Петербург).

4. Російська система соціального формування громадської думки:

– Всеросійський центр вивчення громадської думки (ВЦИОМ),
– дослідне агентство «Евразийский монитор»,
– соціологічна служба Фонд «Общественное мнение»,
– аналітичний центр «Левада-центр» та ін.

5. Федеральне агентство у справах СНД і співвітчизників, які проживають за кордоном, – «Россотрудничество», у складі якого функціонують представництва в 80 країнах світу, у т.ч. в Україні.

6. Інститути громадянського суспільства – урядові та неурядові фонди, які виступають як громадські організації:

– громадська організація «Фонд «Русский мир» ;
– неурядова організація «Фонд поддержки публичной дипломатии имени А. М. Горчакова»;

– некомерційна організація «Российский совет международных дел в сфере внешней политики и международных отношений», заснована Міністерством закордонних справ РФ і Міністерством освіти і науки РФ,

Російською академією наук, Російським союзом промисловців і підприємців та інформаційним агентством «Интерфакс»;

– неурядова організація «Фонд исторической перспективы», створена для фінансування європейської (Париж) і американської (НьюЙорк) філій Інституту демократії і співпраці.

7. Окремі європейські суспільно-політичні організації націоналістичного і ультрарадикального штибу, що фінансуються керівництвом Кремля:

- Front National (Франція), UKIP (Велика Британія),
- BNP (Велика Британія),
- AfD (Німеччина),
- Jobbik (Угорщина),
- Latvijas Krievu savienība (Латвія),
- Атака (Болгарія),
- Forza Italia (Італія) та інші.

8. Російська православна церква, духовенство якої відіграє особливу роль в інформаційній підтримці дій РФ щодо України, пропаганді теорії «русского мира» під прикриттям ідей православної єдності.

9. Проросійські партії, рухи та суспільні організації, фінансовані та керовані з Москви, які відіграли значну роль на підготовчому етапі гібридної війни («Русский мир», «Русская община Крыма», «Русское единство», «Русский блок», «Славянская партия», «Авангард», «Оплот», «Юго-Восток», «Великая Русь» та ін.) [69, с. 105-106].

Інтенсивність і використання пропаганди з боку Російської Федерації на телебаченні, інтернет-ЗМІ, у соціальних мережах зумовлено зумисним дезінформаційним впливом на аудиторію для розпалу і загострення гібридної війни. Завдання сучасної антиукраїнської пропаганди – підірвати довіру, дискредитувати українську владу, політику, економіку, культуру та інше через навмисне та масове поширення неправдивих, упереджених новин з ворожою політичною метою. Крім цього, внести хаос у суспільну свідомість закликами до порушення державного суверенітету, територіальної цілісності України.

Для сучасної пропаганди в засобах масової інформації властиві такі ознаки: зумисне свідоме поширення викривленої інформації з деструктивними намірами, спрямованими на дестабілізацію ситуації в Україні та дискредитацію її міжнародного авторитету.

Для захисту від дезінформації та боротьби із російською пропагандою важливо забезпечити обізнаність населення з цього питання. Перевірка отриманої інформації, уточнення відомостей через інші джерела, обізнаність у сфері методів пропагандистського впливу дають змогу виявити маніпулятивні прийоми та технології.

Актуальним завданням для багатьох країн, в тому числі і України, є переоцінка своїх власних зовнішніх та внутрішніх пріоритетів, що зумовлено необхідністю забезпечення національної безпеки в умовах різкого загострення безпекової ситуації в світі.

Стаття 1 Закону України «Про національну безпеку України» визначає загрози національній безпеці України як явища, тенденції і чинники, що унеможливають чи ускладнюють або можуть унеможливити чи ускладнити реалізацію національних інтересів та збереження національних цінностей України.

Стратегічні документи в галузі безпеки та оборони визначені в статті 3 Закону України «Про національну безпеку України». Так, зокрема, про загрози національній безпеці України та відповідні пріоритети державної політики у сферах національної безпеки і оборони йде мова у Стратегії національної безпеки України, Стратегії воєнної безпеки України, Стратегії кібербезпеки України, інших документах з питань національної безпеки і оборони, які схвалюються Радою національної безпеки і оборони України і затверджуються указами Президента України [12].

Основним документом щодо національної безпеки є Стратегія національної безпеки України. В цьому стратегічному документі визначені основні напрями державної політики у сфері національної безпеки. Стратегія визначає поточні та прогнозовані загрози національній безпеці та національним

інтересам України з урахуванням зовнішньополітичних та внутрішніх умов. Зазначається, зокрема, що Російська Федерація як держава-агресор залишається джерелом довгострокових системних загроз національній безпеці України [15].

Основним джерелом загроз національній безпеці України є і впродовж найближчих років залишатиметься обраний керівництвом Росії курс на закріплення за Росією статусу глобального гравця та визнання так званих «російських інтересів», зроблено фахівцями Служби зовнішньої розвідки України. В інформаційному бюлетені Служби зовнішньої розвідки України «Біла книга» зазначається, що Росія гнучко змінює тактику дій на українському напрямі, проте стратегічна мета залишається незмінною – не допустити успішної західно-орієнтованої України. Гарантією національної безпеки держави в умовах зростання гібридних загроз є забезпечення високого рівня політичної, військової, інформаційної та економічної безпеки [35].

25 березня 2021 р. Президент України своїм Указом № 121/2021 затвердив рішення Ради національної безпеки і оборони України «Про Стратегію воєнної безпеки України». Таким чином, один із головних документів системи планування в сфері національної безпеки і оборони введено в дію. Фактично вперше в Україні підготовлено такий стратегічний документ, який передбачає запровадження комплексного всеосяжного підходу до оборони України в умовах воєнної загрози національній безпеці, пов'язаної з використанням гібридних методів. Положення Стратегії воєнної безпеки України ґрунтуються на тому, що захист суверенітету і територіальної цілісності України є найважливішою функцією держави, справою всього українського народу [1]. Зазначається, що реалізація цієї норми Конституції України в умовах екзистенційної воєнної загрози національній безпеці, зростання дефіциту фінансових ресурсів та дисбалансу воєнних потенціалів України та Російської Федерації обумовлює необхідність розроблення нової стратегії воєнної безпеки, яка базується на всеохоплюючій обороні України [15].

«Гібридна» агресія Росії розглядається військовими фахівцями різних країн як така, що має глобальний характер. А точкою відліку для формування

«гібридного» світоустрою стала агресія РФ проти України, яка спричинила руйнівні наслідки для європейської та глобальної безпеки. На думку експертів, Україні необхідно формувати комплексні стратегічні підходи у протидії російській «гібридній» агресії, створювати гнучкі та ефективні механізми реагування та протистоянням загрозам [38].

Незважаючи на різноманіття підходів до визначення сутності, більшість експертів називають одним із елементів гібридної війни – інформаційне протистояння. Особливо чітко це можна спостерігати на прикладі діяльності РФ проти України: інформаційний вплив спрямований в кількох напрямках: на суспільство України, при цьому особливо потужно на жителів тимчасово окупованих територій, на російське суспільство та на світову громадськість.

РФ використовує проти нашої країни найновіші інформаційні технології впливу на свідомість громадян, спрямовані на розпалювання національної та релігійної ворожнечі, пропаганду агресивної війни, зміну конституційного ладу насильницьким шляхом або порушення суверенітету та територіальної цілісності України. При чому інформаційна війна з Україною почалася задовго до збройного вторгнення у Крим. Однією з численних цілей інформаційної війни було формування громадської думки та світогляду населення, в основу якої лягла ідеологія «руського міру», який на думку його розробників охоплює населення по всій колишній царській та радянській імперіях, які пов'язані з РФ російською мовою, а також спільною релігією, історією та культурою.

В загальних рисах – «руський мір» – це російська неоімперська геополітична та ідеологічна доктрина, розроблена з метою орієнтації російського населення стосовно ідейних основ існування та розвитку російського суспільства, яка полягає в об'єднанні народу, навколо таких елементів як єдина культура, російська мова, православна віра, а також «спільна історична пам'ять», та використовується з метою впливу на масову свідомість російськомовного населення, вигідному РФ. При цьому Україна бачиться невід'ємною складовою «руського міру», що зіграло вирішальну роль у рішенні уряду РФ про вторгнення в Україну та сприяло високому рівню підтримки серед проросійських громадян,

які надавали допомогу в окупації Криму та Донбасу та їх консолідації навколо зазначеної ідеології. Використання ідеї «руського міру» також сприяла вербуванню громадян РФ, які в перші роки війни бажали «захистити російськомовних братів» на Донбасі.

При поширенні ідеології «руського міру» агресор використав несформованість світоглядно-ціннісних орієнтацій українського суспільства та певний ідеологічний вакуум, який утворився у більшості громадян після розпаду СРСР. Концепція «руського міру» формувалася П. Щедровицьким, Г. Павловським, В. Тишковим, О. Дугіним. Президент РФ В. Путін у своїх виступах теж неодноразово використовував термін «руський мір», визнавши його елементом російської зовнішньої політики. В останні своїй статті «Про історичну єдність росіян та українців» В.Путін чітко викладає своє бачення, яке повністю збігається із зазначеною ідеологією і підтверджує, що сьогодні ідеологія «руського міру» виведена на рівень державної політики РФ, що потребує врахування на загальнодержавному рівні.

Використовуючи ідеологію «руського міра» представники спецслужб РФ намагались також імплементувати сценарії створення т.зв. «Запорізької Народної Республіки», «Херсонської Народної Республіки», «Харківської Народної Республіки» та ін. Таким чином зазначена ідеологія активно використовується російськими спецслужбами та російськими ЗМІ для виправдання російської агресії щодо України і спрямована на дестабілізацію соціально-політичної обстановки в Україні, розпалювання сепаратистських настроїв, провокування діяльності з метою посягання на територіальну цілісність, що вимагає розробки та реалізації комплексу заходів з протидії зазначеній ідеології.

Протидія поширенню зазначеної ідеології повинна здійснюватися на кількох рівнях: на міжнародному, загальнодержавному та спеціальному. На спеціальному рівні – протидія СБ України поширенню ідеології «руського міру» в ЗМІ та соціальних мережах, виявлення «ботоферм», створених з метою поширення фейків та виправдання ідеології агресора. На загальнодержавному

рівні повинні вживатися такі заходи як вдосконалення нормативно-правової бази в галузі інформаційної політики, розробка системи захисту від інформаційного домінування іноземних країн, особливо країни-агресора, розвиток національної інформаційної інфраструктури, що надасть можливості Україні ефективно протидіяти інформаційній агресії та практично діяти в інформаційній сфері, підвищення рівня медіакультури суспільства.

Відомий дослідник М. Головатий вважає, що впровадження державотворчої ідеології є одним із засобів подальшого гарантування державотворчої безпеки і покликане «сприяти цілісності держави та її зміцненню, подолання загроз сепаратизму, зміцнення консолідації суспільства та міжетнічного миру» [39, с. 14]. Вона має бути заснована на цінностях, що поділяються більшістю українського суспільства. В Карлова також визнає необхідність створення і впровадження «загальнонаціональної ідеології в Україні, що має включати культурноісторичну, політичну, економічну і соціогуманітарну складові» [50, с. 24].

Водночас ст. 15 Конституції України стверджує, що «жодна ідеологія не може визнаватися державою як обов'язкова» [1]. Державою все ж повинні вживатися певні заходи заповнення ідеологічного вакууму, в якому опинилися українці після розпаду СРСР. Тому важливим є формування на державному рівні ціннісних орієнтирів розвитку сучасного українського суспільства, які зможуть об'єднати та мотивувати український народ успішно долати виклики, спровоковані в тому числі гібридною війною РФ та спробами поширення вигідної агресору ідеології.

Служба безпеки України веде активну діяльність по протидії пропагандистським впливам Російської Федерації. У 2020 р., за матеріалами Служби безпеки України вдалося притягнути до кримінальної відповідальності 40 осіб, які поширювали деструктивну антиукраїнську пропаганду та здійснювали підривну діяльність в інформаційній сфері, 32 особи засуджено, 158 іноземцям, причетним до пропаганди сепаратизму в інтернеті, заборонено в'їзд

в Україні. Загалом порушено понад 50 кримінальних проваджень за різними статтями Кримінального кодексу України (109, 110, 111, 161 ККУ) [30].

У 2020 р. СБУ заблокувала понад 2,5 тисячі спільнот у соцмережах з мільйонною аудиторією та понад 20 бот-мереж потужністю більше ніж 60 тисяч акаунтів; нейтралізувала понад 600 кіберінцидентів та кібератак на інформаційні ресурси органів державної влади; припинила діяльність 20 хакерських угруповань, причетних до таких атак.

З лютого 2022 р. СБУ офіційно звернулася до адміністрації телеграму з вимогами заблокувати певні канали, які поширюють фейкові новини щодо України. З початку війни вони передали на блокування понад 1500 телеграм-каналів, більш як 1500 акаунтів в інстаграм, фейсбук і тікток [66].

Цього року СБУ вже припинила діяльність 35 ботоферм потужністю близько 1,5 млн фейкових акаунтів і заблокувала майже 500 проросійських YouTube-каналів з аудиторією більше ніж 15 млн підписників.

Також, за даними, які відомі на сьогодні, Служба безпеки України з початку повномасштабного вторгнення Росії в Україну викрила близько 700 колаборантів, 50 із них вже засудили, але це не остаточні цифри, адже війна ще триває [30].

Зараз Україна ефективно протидіє російській дезінформації, перемагає на інформаційному фронті, який не менш важливий, ніж поле бою, та набирається досвіду. Успіхом України в сфері протидії дезінформації вважаю, те що:

– враховуючи пряму військову агресію з боку Російської Федерації, активне поширення державою-агресором дезінформації, викривлення відомостей, а також виправдовування або заперечення збройної агресії Російської Федерації проти України, з метою донесення правди про війну, забезпечення єдиної інформаційної політики в період дії в Україні правового режиму воєнного стану, було створено єдину інформаційну платформу стратегічної комунікації "Єдині новини #UАразом" за запитом Кабміну для забезпечення щоденного інформування населення про стан ситуації з безпекою та діяльність державних органів, тому що в умовах воєнного стану реалізація

єдиної інформаційної політики є пріоритетним питанням національної безпеки, забезпечення якої реалізується шляхом об'єднання усіх загальнонаціональних телеканалів, програмне наповнення яких складається переважно з інформаційних та/або інформаційно-аналітичних передач на єдиній інформаційній платформі стратегічної комунікації;

– парламентом за основу був схвалений законопроект про медіа, покликаний оновити законодавство, яке регулювало індустрію ще в 1990-х. За задумом авторів, він має регулювати діяльність телебачення, радіо, преси, онлайн-медіа, стримінгових сервісів і платформ загального доступу до інформації. За словами спікера парламенту України Руслана Стефанчука, оновити законодавство в галузі аудіовізуальних послуг – один із кроків, необхідних для початку переговорів про вступ України до ЄС, тож він входить до пакету євроінтеграційних законопроектів, які Верховна Рада планує розглянути до кінця року. Нині документ оцінюють експерти з Ради Європи та Єврокомісії. Його мета, як зазначено в пояснювальній записці, – створити єдину та взаємоузгоджену систему правових норм, спрямованих на регулювання правовідносин у сфері медіа, виконання Україною зобов'язань перед європейськими партнерами та впровадження норм законодавства ЄС у національне. Цей законопроект – серед кроків, необхідних, щоб безпосередньо почати переговори про вступ до ЄС [64].

Велика частина документа присвячена протидії державі-агресору. Нацрада матиме більше повноважень вплинути на медіа з проросійським контентом, а надто – в режимі воєнного часу. Поправок до документа нині – понад дві тисячі, попередньо його планують схвалити до кінця року. На той час запланована і попередня оцінка Єврокомісією виконання завдань, які отримала Україна разом зі статусом кандидата в країни-члени ЄС;

– у березні 2021 р. був створений Центр стратегічних комунікацій та інформаційної безпеки. Робота Центру сфокусована на протидії зовнішнім загрозам, об'єднанні зусиль держави та громадських організацій у боротьбі з дезінформацією, оперативному реагуванні на фейки, а також на встановлення

українських нарративів. Ключовими завданнями Центру є: розбудова стратегічних комунікацій (розробка контрнарративів РФ, проведення інформкампаній, включення українських нарративів у щоденну комунікацію Уряду); протидія дезінформації та формування стійкості до неї. Постійне сповіщення про інформаційні атаки проти України на ресурсах Центру; підвищення обізнаності про гібридні загрози (розробка та проведення тренінгів для державних службовців, зокрема для представників комунікаційних підрозділів); регулярне інформування про гібридну агресію з боку Росії на міжнародному рівні, напрацювання механізмів протидії дезінформації спільно з міжнародними партнерами [33], [79];

– Координаційний штаб з питань поводження з військовополоненими запустили цілодобову гарячу телефонну лінію для військовослужбовців Російської Федерації, які бажають безпечно здатись у полон. Проєкт «Хочу жити» покликаний допомогти військовослужбовцям РФ безпечно здатися в полон українським Збройним силам. Росіянам та білорусам, які безпосередньо теж беруть участь в збройному конфлікті, гарантують утримання згідно з нормами Женевських конвенцій. В свою чергу, Україна потребує поповнення обмінного фонду, аби повернути своїх захисників додому. Дана можливість призначена інформувати російських військових про можливості скласти зброю та зберегти своє здоров'я та життя. Бійці Збройних Сил України неодноразово зверталися до військовослужбовців об'єднаного угруповання військ Білорусі та Росії. У роликах українські військові закликають у жодному разі не виконувати злочинні накази їхнього командування. Але якщо вже не виконати наказ не вийде, військових закликають заглушити мотори техніки, розрядити зброю, та підняти білі прапори. Їх відмову від вбивства українців наша бійці приймуть як акт вияву дружніх та сусідських відносин і будуть вдячні за це. Натомість ЗСУ гарантують білорусам або повернення додому, або гідне перебування в Україні до закінчення війни у спеціально обладнаних військових містечках [43], [46].

На міжнародному рівні Україна повинна вживати усіх заходів з використанням інструментів міжнародного права, зарубіжних змі та інших

засобів з метою протидії поширенню та розвінчанню ідеології «руського міру» як серед світової громадськості, так і серед населення РФ.

Отже, для успішного протистояння гібридній агресії Росії вкрай необхідне перш за все, внутрішнє зміцнення держави. Цього можна досягти шляхом вдосконалення демократичного врядування, нормативно-правової бази та системи політичних і спеціальних інститутів забезпечення безпеки; подолання корупції і забезпечення умов для функціонування організацій громадянського суспільства. Необхідне проведення збалансованої міжетнічної і міжконфесійної політики, широке інформування суспільства про чутливі теми, в тому числі історичні, які використовуються або можуть використовуватись агресором для досягнення своїх цілей. Такий комплексний всеохоплюючий підхід дозволить консолідувати суспільство і забезпечити для інших країн, які потерпають від гібридних загроз.

Ми стикнулись з найбільшою війною авторитарної диктатури проти ліберальних демократій після Другої світової війни. Вся російська міжнародна інформаційна політика – політика окупації. Світ сьогодні, без перебільшення, живе в інформаційній російській окупації. Тому разом з Україною світ має вивільнитися від спотвореної інформації та боротися і відстоювати свої свободи.

3.3. Європейський досвід протидії російській дезінформації

З кожним роком створення та розповсюдження дезінформації в Інтернеті набуває все більших масштабів, що здійснює серйозний вплив на європейські країни. Сьогодні Європа та Захід є об'єктами дезінформації та іноземного втручання. В більшості країн Європи реагування та відповіді на ці загрози були повільними через правові обмеження та нерозуміння масштабів проблеми з боку політиків.

Європейська Комісія визначила дезінформаційні кампанії Росії та Китаю найбільшою загрозою для ЄС, оскільки вони систематичні, добре забезпечені ресурсами та здійснюються у великих масштабах. Тому постає нагальна потреба у побудові потужних механізмів захисту від оманливої та неправдивої інформації, особливо в мережі Інтернет. З одного боку, Інтернет містить величезну кількість інформації у вільному доступі, а з іншого боку він несе цілу низку загроз, серед яких наявні дезінформація та пропаганда. Тому за останні кілька років було зроблено велику кількість офіційних кроків задля вирішення цієї проблеми.

Після анексії Криму в лютому 2014 р. Росія продемонструвала світові, що дезінформація є невід'ємною складовою гібридної війни. Починаючи з 2015 р. Росія веде активну кампанію з розповсюдження дезінформації та фейків спрямовану на країни ЄС. Тоді ж виникла гостра необхідність протистояти цим маніпулятивним впливам.

Саме тому 22 червня 2015 р. ухвалено «План дій зі стратегічних комунікацій» (EU Action Plan on Strategic Communication), в якому чітко були поставлені цілі щодо покращення можливостей ЄС у сфері ефективної комунікації та прогнозування, вирішення проблем та реагування на зовнішню дезінформаційну діяльність, а також зміцнення загального середовища ЗМІ в країнах Східного партнерства. Згідно цього плану, було створено Оперативну робочу групу зі стратегічних комунікацій ЄС (East StratCom Task Force) для виявлення та протидії дезінформації з боку Росії [21].

Наступним важливим кроком у напрямку протидії маніпулятивним впливам стало прийняття Європейською Комісією та Верховним представником ЄС з питань закордонних справ та політики безпеки документу «Спільні принципи протидії гібридним загрозам – відповідь Європейського Союзу» (Joint Framework on countering hybrid threats a European Union response). Цей документ було підписано в квітні 2016 р. і фактично він став основним з погляду структурування зусиль ЄС у боротьбі з дезінформацією та гібридним загрозам. У документі зазначається, що ЄС і НАТО мають об'єднати свої зусилля

для більш ефективної й швидкої реакції на гібридні загрози та дезінформаційні кампанії. Також наголошується на необхідності створення нових механізмів для протидії дезінформації, стверджується, що дезінформація може поширюватись в рамках цілеспрямованих кампаній в соціальних мережах з метою дестабілізації суспільства. Перш за все, за підтримки Єврокомісії та Верховного представника ЄС, державам-членам пропонується розпочати дослідження гібридних загроз для визначення вразливих місць, які істотно впливають на національні та загальноєвропейські державні структури та мережі. Наступним важливим кроком є створення центру «EU Hybrid Fusion Cell» в рамках існуючої структури Центру розвідки та ситуацій ЄС (EU Intelligence and situation centre – EU INTCEN), який буде відповідальний за отримання та аналіз секретної інформації про гібридні загрози [27].

У листопаді 2016 р. Європейський Парламент затвердив Резолюцію «Стратегічні комунікації ЄС як протидія пропаганді третіх сторін» (EU strategic communication to counteract propaganda against it by third parties). Зокрема, в цьому документі зазначається, що дезінформація та пропаганда є характерними складовими частинами гібридної війни. Більше того, стратегія пропаганди та дезінформації, яка спрямована проти ЄС з боку третіх країн може набувати різних форм і передбачає залучення різних засобів комунікації, а саме традиційних засобів інформації, соціальних мереж тощо. Саме тому Європейський Парламент закликає інституції ЄС уважно стежити за фінансуванням антиєвропейської пропаганди, а також підкреслює, що необхідно збільшити фінансування для підтримки свободи ЗМІ в країнах-сусідах ЄС [22].

Великим проривом у протидії розповсюдженню дезінформації стало прийняття «Кодексу практики щодо протидії дезінформації» (Code of Practice on Disinformation), який підписано у жовтні 2018 р. Цей документ було визнано першим саморегулюючим документом у світі, який стосується боротьби з дезінформацією, адже він встановлює основні принципи й зобов'язання щодо онлайн-платформ та рекламного сектора для боротьби з дезінформацією в Європейському Союзі. До того ж, Кодекс підписали такі представники онлайн-

платформ, як гугл, фейсбук, твіттер, майкрософт, тікток. Цим самим онлайн-платформи зобов'язалися звітувати і виробити механізми протидії розповсюдженню дезінформації та пропаганди в мережі. Дані зобов'язання діляться на п'ять основних напрямів: перевірка розміщення реклами; політична та тематична реклама; чесність у наданні послуг; розширення можливостей для користувачів; збільшення можливостей для дослідницької спільноти.

В першу чергу платформи мають посилити контроль за розміщенням реклами, видаляти підроблені облікові записи та позначати дії ботів, а також забезпечити прозорість за допомогою показників достовірності джерел контенту. Отже, головними цілями Кодексу є забезпечення прозорості щодо спонсорованого вмісту, зокрема політичної реклами та зменшення доходів розповсюджувачів дезінформації; вжиття заходів щодо виявлення та закриття фейкових акаунтів; можливість постійно моніторингу онлайн-дезінформації дослідниками, факт-чекерами та органами влади [18].

В грудні 2018 р., в рамках підготовки до виборів Європарламенту у 2019 р., у Євросоюзі представили «План дій проти дезінформації» (Action Plan against Disinformation), який передбачає підвищення прозорості щодо походження інформації та способів її отримання, підвищення обізнаності громадськості та розвиток медіаграмотності населення для формування критичного мислення, контроль вмісту реклами, а саме прозорість політичної реклами та запровадження чітких правил для виявлення ботів [17]. Крім того, для посилення реакції ЄС на дезінформацію, у Плані основний акцент робиться на чотирьох напрямках: покращення можливостей установ Європейського Союзу з виявлення, аналізу та викриття дезінформації; посилення скоординованих та спільних заходів реагування установ ЄС та держав-членів на дезінформацію; залучення приватного сектору для боротьби з дезінформацією; підвищення обізнаності про дезінформацію та підвищення стійкості суспільства.

До того ж, у даному Плані описуються заходи, які спрямовані на більш ефективну боротьбу з дезінформаційними кампаніями, а саме створення системи швидкого реагування (Rapid Alert System), контроль за виконанням Кодексу та

збільшення механізмів для вчасного виявлення загроз дезінформації. Таким чином, пропонується комплекс заходів, які в подальшому повинні забезпечити спільний та скоординований підхід ЄС до боротьби з дезінформаційними кампаніями [17].

У січні 2019 р. онлайн-платформи представили перший звіт, в якому викладені перші результати виконання заходів прийнятих відповідно до «Кодексу практики щодо протидії дезінформації». Моніторинг Кодексу є частиною «Плану дій проти дезінформації» для зміцнення співпраці та нарощення потенціалу між державами-членами та інституціями ЄС з метою активної протидії загрозам, спричинених дезінформацією. Зокрема, фейсбук реалізовує заходи проти фейкових облікових записів та шкідливих автоматизованих систем, які поширюють неправдиву інформацію в мережі, а також заохочує дослідження дезінформації та створює відповідні інструменти, які допоможуть користувачам мережі виявляти фейкову інформацію. У роботі гугл спостерігається прогрес щодо контролю за розміщенням реклами через мережу «AdSense», ведеться активна боротьба з підробленими сайтами, а також було вжито заходи для надання користувачам інформації, інструментів та підтримки для розширення їх можливостей в мережі: його алгоритми ранжування визначають пріоритетність релевантної та достовірної інформації в результатах пошуку, а мітка перевірки фактів доступна користувачам у всіх державах-членах ЄС. Твіттер приділяє значну увагу новим заходам, що спрямовані на боротьбу зі зловмисниками, які використовують вразливості сервісу для розповсюдження дезінформації та пропаганди в даній соціальній мережі. Зокрема, йдеться про закриття фейкових або підозрілих облікових записів та виявлення автоматизованих систем (ботів), які за допомогою спаму поширювали недостовірний контент. Отже, з січня по травень 2019 р. Європейська Комісія провела цілеспрямований моніторинг виконання зобов'язань гугл, фейсбук та твіттер, акцентуючи увагу на чесності виборів до Європарламенту [19].

З метою попередження великих масивів дезінформації в період виборів до Європарламенту (травень 2019 р.), напередодні, у березні 2019 р. парламент затвердив Резолюцію «Про зовнішнє втручання у вибори та дезінформацію у національних та європейських демократичних процесах» (Foreign electoral interference and disinformation in national and European democratic processes). У резолюції зазначалося, що РФ є «основним джерелом дезінформації в Європі», тому рекомендується підвищити обізнаність про дезінформаційні кампанії Росії та інших ворожих суб'єктів. Наголошується, що іноземне втручання може мати безліч форм, включаючи дезінформацію в соціальних мережах для формування громадської думки, кібератаки, які націлені на критичну інфраструктуру, пов'язану з виборами, пряму та непряму фінансову підтримку політичних суб'єктів. Також пропонується розробити юридичні рамки, які б регулювали процес протидії цим гібридним загрозам, зокрема у питаннях відповідальності та санкцій за організацію та проведення таких дій. У документі, окрема увага приділяється захисту виборчих процесів у країнах ЄС від зовнішнього втручання. Наголошується на тому, що держави-члени ЄС повинні стежити за тим, щоб їх виборчі закони враховували потенційні загрози демократичності виборів, які спричиняють дезінформаційні кампанії. Крім того, наголошується на необхідності покращення медіаграмотності населення [25].

Впродовж 2020 р. високопоставлені чиновники ЄС, зокрема Урсула фон дер Ляєн (чинний президент Європейської Комісії), наголошували на небезпеці дезінформації, пов'язаної з епідемією Covid-19. Тому європейські інституції ухвалили документ «Боротьба з інфодемією COVID-19 – правильний виклад фактів» (Tackling the COVID-19 infodemic – getting the facts right). У документі йдеться про головні виклики, які спричинила дезінформація навколо коронавірусу. Зокрема, це розповсюдження медичної інформації, яка вводить людей в оману; поява різноманітних «теорій змови», що можуть поставити під загрозу здоров'я громадян (наприклад, міфи про установки 5G, що поширюють коронавірус, або про те, що джерелом коронавірусу є певна етнічна або релігійна група людей, тощо); зростання кількості кіберзлочинів таких, як хакінг або

фішинг, з використанням посилань, пов'язаних з COVID-19 для поширення шкідливих програм тощо. А також наголошується на підсиленні стратегічних комунікацій як всередині ЄС, так і за його межами, покращенні співпраці в рамках ЄС, особлива увага зосереджується на необхідній співпраці європейських інституцій із соціальними медіа та підтримка досліджень й діяльності у сфері фактчекінгу [29].

З метою протидії дезінформації, яка пов'язана з пандемією було створено «Програму моніторингу та звітності про Covid-19» (Covid-19 disinformation monitoring programme), яка є мірою прозорості для забезпечення підзвітності громадськості за зусилля, що вживаються онлайнплатформами і відповідними галузевими асоціаціями з обмеження дезінформації про вірус в мережі Інтернет. Платформи, які підписали Кодекс щомісяця звітують про: дії щодо підвищення обізнаності про авторитетні джерела, такі як Всесвітня Організація Охорони Здоров'я (ВООЗ); інструменти для полегшення доступу до достовірної інформації, що представляє суспільний інтерес; публікації, що містять оманливу інформацію; зусилля з надання точної інформації про вакцини.

До того ж, онлайн-платформи виявили велику кількість публікацій, які містили неправдиву інформацію, пов'язану з Covid-19, проте у своїх сервісах вони не виявили чітко скоординованих операцій з дезінформації з особливим акцентом на пандемію [20].

4 травня 2020 р. «Європейська група регуляторів аудіовізуальних медіапослуг» (European Regulators Group for Audiovisual Media Services – ERGA) здійснила моніторинг «Кодексу практики щодо протидії дезінформації» (2018 р.) та дала свою оцінку, виявила недоліки й надала рекомендації з покращення цього документу, тим самим, відобразили цю інформацію в звіті «Звіт ERGA про дезінформацію: оцінка виконання Кодексу практики» (ERGA Report on disinformation: Assessment of the implementation of the Code of Practice). Відповідно до проведеного моніторингу за 2019 р. було встановлено, що Кодекс є унікальним та інноваційним інструментом боротьби з дезінформацією в Інтернеті. Також він встановлює умови й зобов'язання співпраці між

соціальними платформами та Єврокомісією. У такий спосіб платформи зобов'язалися співпрацювати з ЄС для покращення своїх внутрішніх правил та процедур. Проте, з іншого боку, виявили недоліки суттєві недоліки Кодексу, зокрема: заходи з протидії дезінформації є занадто загальними і тому важко оцінити їхню ефективність; платформи впроваджують дуже мало заходів, а саме, не всі політичні оголошення маркуються належним чином, бракує інформації про діяльність платформ на національному рівні та вилучені облікові профілі; Кодекс не має єдиного механізму за допомогою якого, інформацію у звітах соціальних платформ можна було б незалежно перевірити. ERGA (European Regulators Group for Audiovisual Media Services) у своєму звіті надала рекомендації для покращення Кодексу, які поділяються на три напрямки:

- покращення моніторингу чинних зобов'язань – необхідно розробити набір відповідних визначень (політична реклама, фейкові новини, маніпуляція тощо) для забезпечення послідовного підходу до цих питань у всьому ЄС; покращити надання інформації онлайн-платформами; удосконалити співпрацю між фактчекінговими організаціями та соціальними медіа;

- розширення існуючих зобов'язань – двічі на рік платформи мають звітувати про впровадження заходів, які описані в Кодексі; збільшити кількість підписантів Кодексу;

- пошук та впровадження нових більш ефективних інструментів для протидії дезінформації в мережі [67].

У грудні 2020 р. Єврокомісія представила «Європейський план дій щодо демократії» (European Democracy Action Plan), який передбачає запровадження конкретних заходів для сприяння вільним й справедливим виборам та активної демократичної участі, підтримки вільних і незалежних засобів масової інформації. Також даний План передбачає боротьбу з дезінформацією шляхом розробки інструментарію ЄС для протидії впливу іноземних втручань; посилення Кодексу, шляхом надання онлайн-платформам чітких вказівок про те, як активізувати їхні заходи по боротьбі з дезінформацією і створення надійної бази для її моніторингу; збільшення фінансування, що спрямовуватиметься на

підтримку нових інноваційних проектів у галузі протидії дезінформації та підвищенню медіаграмотності населення в рамках різних програм ЄС. Для виконання цих дій будуть задіяні інституції ЄС, національні уряди, які несуть відповідальність за забезпечення надійного функціонування демократії, а також інші національні органи влади, політичні партії, ЗМІ та онлайн-платформи [23], [24].

А вже у травні 2021 р. Європейська Комісія представила «Керівництво з посилення Кодексу практики щодо протидії дезінформації» (Guidance on Strengthening the Code of Practice on Disinformation), що спрямоване на усунення недоліків і прогалин для створення більш надійного та безпечного онлайн-середовища [26].

Отже, ЄС постійно вдосконалює свої нормативно-правові документи, щоб протистояти дезінформаційним кампаніям та маніпуляціям, особливо з 2014 р., коли посилися гібридні загрози з боку Росії. На законодавчому рівні було прийнято велику кількість правових актів, резолюцій, кодексів, але зважаючи на динамічність поширення цих маніпуляцій і постійну зміну форми подачі такої інформації, необхідно мати здатність оперативно реагувати на виникаючі загрози.

Крім того, в ЄС намагаються комплексно вибудовувати нові механізми та стратегії для запобігання поширенню деструктивної пропаганди та дезінформації. Тому необхідно проаналізувати діяльність інституцій та організацій, які відповідають за боротьбу з неправдивою та оманливою інформацією, що поширюється не тільки на теренах Інтернету, а й в традиційних засобах масової інформації.

Однією з головних інституцій в Європейському Союзі, яка займається вирішенням проблем, пов'язаних з дезінформацією являється Європейська служба зовнішніх справ (EEAS). Дана служба була офіційно створена 1 січня 2011 р., відповідно до Лісабонського договору, який набув чинності в кінці 2009 р. EEAS звітує про свою діяльність, за допомогою щорічних звітів про свою

діяльність з питань зовнішньої політики, діяльності в галузі безпеки й оборони ЄС та дотримання прав людини [67].

У Європейській служби зовнішніх справ створено два відділи комунікацій:

Перший – «Відділ комунікаційної політики та публічної дипломатії» (The Communication Policy and Public Diplomacy), який просуває діяльність Верховного представника ЄС та інформує про політику ЄС у сфері закордонних справ, безпеки та оборони.

Другий – «Відділ стратегічних комунікацій» (The Strategic Communications), який сприяє ефективній комунікації, протидії дезінформації, покращенню загального середовища засобів масової інформації та суспільства у відповідних регіонах [67].

У розпорядженні цього відділу функціонує три групи.

Перша – була створена у 2015 р. за ініціативою Європейської Ради, що звернулася до Верховного представника ЄС з проханням розробити чіткий план дій щодо стратегічних комунікацій, у зв'язку зі збільшенням масивів поширення дезінформації з боку Росії. Ці дії призвели до створення Оперативної робочої групи зі стратегічних комунікацій ЄС «East StratCom Task Force» при Європейській службі зовнішніх справ (EEAS). Оперативна група була створена для ефективної комунікації та просування політики ЄС щодо Східного партнерства, зміцнення загального середовища ЗМІ, шляхом підтримки свободи ЗМІ, покращення можливостей ЄС у здатності прогнозувати та швидко реагувати на дезінформаційну діяльність Росії. Група працює в рамках існуючого бюджету ЄС на стратегічні комунікації. У 2018 р. в рамках боротьби з кремлівською дезінформацією група отримала 1.1 млн \$ [67].

Зазначена група випускає щотижневий огляд прокремлівської дезінформації, яка скерована на Захід, в якості лідируючого продукту на вебплатформі EUvsDisinfo. Ця платформа створена у 2015 р. для кращого прогнозування, виявлення та реагування на російські дезінформаційні кампанії, які часто спрямовуються на країни-члени ЄС. Основна мета – підвищити

обізнаність громадськості та розуміння дезінформаційних кампаній Кремля, а також допомогти суспільству в Європі виробити стійкість до різноманітних маніпуляцій. До прикладу, на початку червня 2020 р. веб-платформа EUvsDisinfo виявила близько 570 випадків поширення дезінформації, яка стосується вірусу Covid-19 і таку дезінформацію поширювали саме прокремлівські ЗМІ.

Друга група – оперативна група «Південь», яка створена у 2015 р. і працює над протидією пропаганди джихадизму.

Третьою є цільова група «Західні Балкани», що була створена у 2017 р. і займається захистом іміджу ЄС в регіоні.

Отже, для відділу стратегічних комунікацій пріоритетним завданням є протидіяти кремлівській дезінформації та пропаганді. Для його виконання у 2021 р. було виділено 11 млн \$. Цей бюджет забезпечує професійний моніторинг ЗМІ, аналіз дезінформації, розробку та впровадження комунікаційних кампаній, а також проведення тренінгів й створення симуляцій щодо реагування на дезінформацію.

Оскільки в XXI ст. гібридні загрози є справжнім викликом для безпеки ЄС. Важливим кроком у протидії цьому стало створення Центру гібридного синтезу (EU Hybrid Fusion Cell) у рамках Центру розвідки та ситуацій ЄС (EU INTCEN) Європейської служби зовнішніх справ (EEAS) для аналізу зовнішніх аспектів гібридних загроз ЄС. Діяльність центру зосереджується на отриманні, аналізу та обміну секретною інформацією від різних зацікавлених сторін в EEAS, зокрема щодо показників та попереджень про гібридні загрози на теренах ЄС, для того, щоб швидко аналізувати відповідні інциденти та інформувати про процеси прийняття стратегічних рішень ЄС [27].

У січні 2018 р. Європейська Комісія створила Групу експертів високого рівня «HLEG» для консультування комісії з питань дезінформації та фейкових новин в мережі Інтернет. Дана група складається з 39 експертів з фінансової сфери, представників ЗМІ та соціальних медіа, наукових кіл та спостерігачів від європейських та міжнародних установ. Основним результатом діяльності даної групи є звіт, який починається із загального розуміння поняття дезінформації. У

ньому зазначається, що «дезінформація містить всі форми неправдивої, оманливої інформації, яка була створена та розповсюджена з метою заподіяння суспільної шкоди або отримання прибутку». Також у звіті Група експертів високого рівня надає рекомендації для Єврокомісії і закликає її утриматись від спрощених рішень. Рекомендації «HLEG» спрямовані на впровадження не тільки короткострокових заходів реагування на найбільш нагальні проблеми, але й довгострокових дій спрямованих на підвищення стійкості суспільства до дезінформації та для забезпечення постійної оцінки ефективності цієї діяльності [67].

Підхід, який рекомендує група експертів високого рівня базується на низці взаємопов'язаних і взаємодоповнюючих принципах, які націлені на:

- підвищення прозорості онлайн-новин, адже саме прозорість є ключовим елементом реагування на дезінформацію в мережі Інтернет. В даному випадку, йдеться про те, що інформація про власників цих медіа не має бути прихованою від читачів;

- підвищення рівня медійної та інформаційної грамотності суспільства для протидії дезінформації та допомагати користувачам орієнтуватися в середовищі цифрових медіа. В інформаційну епоху медіаграмотність стала необхідною навичкою, адже вона сприяє розвитку критичного мислення;

- сприяння продовженню досліджень впливу дезінформації на європейське суспільство.

Для поглиблення співпраці між НАТО та ЄС щодо протидії гібридним загрозам, за ініціативою уряду Фінляндії в Хельсінкі 2018 р. було створено міжнародний, незалежний «Європейський центр протидії гібридним загрозам» (European Centre of Excellence for Countering of Hybrid Threats). Країнами-засновниками центру виступають США, Велика Британія, Німеччина, Франція, Швеція, Польща, Фінляндія, Латвія та Литва. Головною діяльністю є проведення досліджень та аналізу із протидії гібридним загрозам, а саме дезінформації, пропаганди, кібератак. Варто звернути увагу на те, що центр носить суто дослідницький характер.

Метою діяльності центру є ведення комунікації про гібридні загрози через публікування звітів, різних видань та співпраці з партнерами у цій галузі. До структури центру входять:

- керівна рада є головним органом, складається з представників держав-учасниць та відповідає за прийняття внутрішніх правил, затверджує програму роботи, бюджет і залучення нових держав-учасниць;

- три активні мережі, так звані спільноти інтересів, які спрямовані на: гібридний вплив (очолюється Великою Британією), вразливість і стійкість (очолюється Фінляндією) та стратегія й оборона (очолюється Німеччиною). Цими мережами керує Секретаріат;

- дослідницька група займається поглибленням розуміння наукових досліджень та дискусій з відповідних тем. Дослідження забезпечують аналіз, що необхідний для визначення пріоритетних проблем;

- група з тренування та навчання виступає в якості ініціатора та виконавця, планує та виконує експериментальні вправи з різними сценаріями гібридних загроз. Мета тренувань полягає в навчанні учасників та вдосконаленні механізмів реагування на різні інциденти стосовно гібридних загроз;

- секретаріат займається адміністративними функціями та забезпечує належне виконання загальних обов'язків центру. Крім того, він відповідальний за підготовку та організацію засідань Керівної ради та співпрацю й підтримку зв'язків з державами-учасниками, а також відповідає за створення й підтримку мереж [67].

Таким чином, центр виступає як платформа між ЄС та НАТО, яка забезпечує площину для стратегічних дискусій, спільних навчань та тренувань.

У березні 2019 р. Європейська служба зовнішніх справ запустила «Систему швидкого оповіщення» (Rapid Alert System) для забезпечення загальної обізнаності про ситуацію, яка пов'язана з поширенням дезінформації в державах-членах ЄС. Даний інструмент є ключовим елементом «Плану дій ЄС щодо боротьби з дезінформацією» (2018 р.). Система складається з елементарної платформи для обміну інформацією, а також мережі пунктів зв'язку в різних

державо-членах ЄС. Крім того, усі країни-члени ЄС призначили національний контактний відділ для моніторингу фейкових новин, а також узгодили конкретний поріг для активації системи.

Система швидкого оповіщення призначена для підключення до існуючих можливостей моніторингу в режимі реального часу, наприклад до таких, як Координаційний центр реагування на надзвичайні ситуації та ситуаційна кімната Європейської служби зовнішніх справ [67].

Якою б неправдоподібною не була новина, російським медіа вдається її зробити популярною за допомогою армії інтернет-тролів, проплачених експертів та потужного фінансування, розповідають експерти. За словами британського журналіста та письменника Пітера Померанцева, ця інформаційна війна кардинально відрізняється від усіх відомих донині протистоянь: «Це нова ідея війни. Війна у традиційному розумінні – це продовження політики. Тобто політика закінчується, починається війна, далі війна закінчується і настає мир. Зараз ми говоримо про безкінечну інформаційно-психологічну війну. Це постійна дестабілізація, це абсолютне неприйняття ідеї глобалізації. Ви запитаете, чого Путін хоче. XXI століття він бачить саме таким: безкінечна підривна діяльність, дезінформація, економічні маніпуляції. І, можливо, він правий, можливо, в інформаційний вік, у 21-му столітті війну виграє не той, хто переміг на полі бою, а чий новині більше повірили» [78]. Можливо, раніше я б погодилася з цією думкою, так як в інформаційному полі ми, м'яко кажучи, відставали, але не зараз. В даний момент ми сильні та міцні, даємо відсіч ворогові і на полі бою, і на інформаційному полі теж, адже правда завжди перемагає.

За словами Померанцева, протидіяти такій потужній машині пропаганди потрібно масштабними методами: «Чого російському суспільству не вистачає – це не просто іншої точки зору, іншого телеканалу. У них немає того центрального стержня, освіти, розуміння, вміння думати раціонально, критично оцінювати докази».

На думку європейських експертів, російська пропаганда виявилася надзвичайно гнучкою, і саме тому вона може орієнтуватися на всіх. Росія дуже

добре визначає як атакувати держави-члени ЄС через дезінформацію: для Німеччини вони зосереджувались на міграції, для Литви – на меншинах, для Великобританії – на Brexit, для Іспанії – на сепаратистських питаннях. ЄС має конкретно визначити, де загроза для кожної держави-члена.

Дезінформаційну кампанію Росія проводить за допомогою різноманітних методів, адаптуючи меседжі під різні цільові аудиторії. Вона сіє дезінформацію, але водночас намагається, щоб її «брехня» була розважальною та емоційно привабливою, прилаштовує неправду до риторики, щоб та відповідала упередженням та установкам аудиторії. Щоб привернути увагу до свого контенту, Росія готова повністю фабрикувати «історії» з використанням фото- й відеоматеріалів для своїх потреб. Ціла низка ЗМІ – від кіно до новин, ток-шоу, друкованих медіа та соціальних мереж – займається просуванням комплексу офіційних російських установок.

Отже, боротьба із дезінформацією та пропагандою здійснюється не тільки на рівні Європейського Союзу, а й безпосередньо в країнах Європи. Протидія розповсюдженню дезінформації та пропаганді – це постійний, нескінченний процес, що вимагає розвитку стійкості суспільства та уряду. Ці загрози постійно змінюються та вдосконалюються, а це означає, що відповідь на них теж повинна постійно розвиватися. На законодавчому рівні ЄС було розроблено чималу кількість документів, які засвідчують, що необхідно розробляти нові інструменти протидії неправдивій інформації, покращити обізнаність європейського населення щодо інформаційної грамотності та надалі проводити дослідження впливу дезінформації на громадськість. В Європі експерти вважають Росію основним розповсюджувачем дезінформації, адже саме РФ досягла широкого проникнення своїх наративів у ЄС та інших країнах світу.

Враховуючи вище викладене, аналіз європейського законодавства та досвіду організаційних й практичних заходів, спрямованих на боротьбу з прокремлівською пропагандою та дезінформацією, створює належні підстави для імплементації відповідного досвіду Україною, дасть змогу обґрунтовано, з урахуванням інтересів громадян та держави, вдосконалити вітчизняну

нормативно-правову базу й практику стратегічних комунікацій. Запозичення закордонного досвіду не повинно відбуватися шляхом автоматичного копіювання документів (нормативних актів, рекомендацій). Подібна імплементація має відбуватися з урахуванням особливостей менталітету українського народу та особливостей української державності на даному конкретному етапі її становлення та розвитку, конкретних обставин, у яких знаходиться Українська Держава на даному етапі її збройного протиборства з Росією.

Таким чином, у третьому розділі було проведено моніторингове дослідження протидії дезінформації та фейкам в інформаційному просторі України на прикладі Центру протидії дезінформації при РНБО України та виданні «Українська правда» (лютий – листопад 2022 р.), яке показало, що лідером у виявленні і представленні фейкової інформації є, звісно, Центр протидії дезінформації при РНБО, так як він, відповідно, цим займається, але не розвінчує фейки, а просто констатує факт, що та чи інша інформація є неправдивою. Центром протидії дезінформації при РНБО було виявлено 632 фейкові новини. Щодо видання «Українська правда», то ним було виявлено всього 105 фейків, але, варто зазначити, що окрім новин, які публікуються, вони пропонують статті, які раніше публікувалися на цю тему, в кожній статті зазначається передісторія питання, для того щоб допомогти читачеві розібратися в цьому матеріалі, вдаються в деталі, пояснюють новину, розвінчують фейкову інформацію, в кінці статей вони зазначають джерело, звідки взялась ця інформація для того, щоб читач міг сам в іншому джерелі перевірити точність цієї інформації, також, цитуючи людину, яка інформує про щось, зазначають її ім'я і посаду, для того, щоб запевнитись, що це сказала людина, яка має на це повноваження. Також було визначено досвід України в протидії інформаційним маніпуляціям в умовах інформаційної війни Росії проти України і проаналізовано європейський досвід протидії російській дезінформації.

ВИСНОВКИ

В інформаційному просторі України йде безперервна боротьба за управління ресурсами, вплив і контроль на території нашої держави.

Інформація – глобальний ресурс сьогодення, за допомогою якого збільшується ефективність керування в усіх сферах життя. Практично в усіх збройних конфліктах за останні десятиліття ефективно використовувалися методи та засоби інформаційної боротьби, які можуть призвести до таких трагічних наслідків, як: зміна суспільного ладу та політичного устрою; розпад держави; втрата армії; розвал економічної системи в країні; страта національної ідеї та духовних цінностей; загибель людей тощо.

Дезінформація – це проблема, яка перетинає кордони, як національні, так і дисциплінарні. Дедалі очевиднішим стає те, що вирішення проблеми неможливо знайти без істотної міжнародної та міждисциплінарної співпраці. Так, в умовах інформаційних війн та маніпуляцій зростає потреба в перевірці достовірності відомостей та фактів, які циркулюють в нашому інформаційному середовищі.

Дезінформація є міжнародною проблемою та загрозою для суспільства, адже вони породжують плутанину та недовіру, а також зменшують віру людей в інституції, які мають вирішальне значення для функціонування здорової демократії, як-от уряд, ЗМІ тощо. Це підриває здатність громадян ефективно брати участь у житті суспільства та різноманітних громадських заходах.

Завдяки новим комунікаційним технологіям стало можливим легко створювати й розповсюджувати неправдиву та шкідливу інформацію, яка є замаскованою під новини заради завоювання довіри тієї чи іншої цільової аудиторії. Фальшиві чи частково спотворені новини в результаті мають негативний вплив та є загрозливим явищем у медіапросторі. Вони розповсюджуються з чотирьох конкретних причин, таких, як прибуток,

політичні та економічні мотиви, або внести корективи в демократичний устрій країн тощо.

У системі сучасних економічних, політичних та військових протистоянь інформаційні маніпуляції посідають провідне місце, як один з ключових супроводжувальних процесів. Головне призначення таких процесів – шляхом концентрації зусиль на певних ключових ланках, забезпечувати суттєві переваги в рамках комплексного протиборства сторін. Інформаційна зброя такого типу здатна знищувати чи, як мінімум, блокувати системи координації, поширення інформації та інші відповідні управлінські процеси, а також перешкоджати роботі відповідних центрів керування. Спектр інструментів при цьому доволі широкий – від кібератак до організації акцій протесту, терористичних актів та організованого збройного опору.

Інформаційно-психологічні операції є сьогодні невід'ємною частиною систем управління військами, політичними та економічними процесами. У зв'язку з активною віртуалізацією людства, такі конфлікти переносяться у інтернет-простір і набувають формату мережевих онлайн протистоянь.

Останнє викликає необхідність налагодження системної роботи за двома напрямками. Перший – розробка та впровадження стандартів і алгоритмів ведення мережевих інформаційних війн, які допомагатимуть швидко реагувати на певні виклики та компенсувати в певних обставинах відсутність досвіду та власних інструментів. Другий напрямок – налагодження системної роботи із підготовки відповідних фахівців, що спиратиметься на чітку методологічну базу та практичні методики навчання.

Важливість роботи за двома зазначеними вище напрямками полягає в тому, що інформаційні маніпуляції, на відміну від, наприклад, торгово-економічних, політичних та збройних протистоянь, ніколи не закінчуються. Тому питання державної інформаційної безпеки в зазначеному контексті є завжди актуальним.

СПИСОК ВИКОРИСТАНИХ ДЖЕРЕЛ

Законодавчі та нормативно-правові акти

1. Конституція України : Закон України від 28.06.1996. Поточна редакція 01.01.2020. База даних «Законодавство України». URL: <https://zakon.rada.gov.ua/laws/show/254к/96> (дата звернення: 02.09.2022).
2. Про інформацію : Закон України від 2 жовт. 1992 р. Поточна редакція 15.06.2022. База даних «Законодавство України». URL: <https://zakon.rada.gov.ua/laws/show/2657-12> (дата звернення: 21.10.2022).
3. Про друковані засоби масової інформації (пресу) в Україні : Закон України від 16 лист. 1992 р. Поточна редакція 12.06.2022. База даних «Законодавство України». URL: <https://zakon.rada.gov.ua/laws/show/2782-12> (дата звернення: 15.10.2022).
4. Про телебачення та радіомовлення: Закон України від 21.12. 1993 р. Поточна редакція 07.10.2022. База даних «Законодавство України». URL: <https://zakon.rada.gov.ua/laws/show/3759-12> (дата звернення: 15.10.2022).
5. Про державну таємницю : Закон України від 21 січ. 1994 р. Поточна редакція 15.03.2022. База даних «Законодавство України». URL: <https://zakon.rada.gov.ua/laws/show/3855-12> (дата звернення: 28.10.2022).
6. Про захист інформації в інформаційно-телекомунікаційних системах : Закон України від 02.08.1994 р. Поточна редакція 01.07.2022. База даних «Законодавство України». URL: <https://zakon.rada.gov.ua/laws/show/80/94-вр> (дата звернення: 07.11.2022).
7. Про порядок висвітлення діяльності органів державної влади та органів місцевого самоврядування в Україні засобами масової інформації : Закон України від 23.09.1997р. Поточна редакція 16.07.2019. База даних «Законодавство України». URL: <https://zakon.rada.gov.ua/laws/show/539/97-вр> (дата звернення: 01.11.2022).

8. Про Державну службу спеціального зв'язку та захисту інформації України : Закон України від 23.02.2006 р. Поточна редакція 30.10.2022. База даних «Законодавство України». URL: <https://zakon.rada.gov.ua/laws/show/3475-15> (дата звернення: 01.11.2022).

9. Про захист персональних даних : Закон України від 1 черв. 2010 р. Поточна редакція 27.10.2022. База даних «Законодавство України». URL: <https://zakon.rada.gov.ua/laws/show/2297-17> (дата звернення: 07.11.2022).

10. Про доступ до публічної інформації : Закон України від 13.01.2011 р. Поточна редакція 19.02.2022. База даних «Законодавство України». URL: <https://zakon.rada.gov.ua/laws/show/2939-17> (дата звернення: 28.10.2022).

11. Про Суспільне телебачення і радіомовлення України : Закон України від 17.04.2014 р. Поточна редакція 12.02.2021. База даних «Законодавство України». URL: <https://zakon.rada.gov.ua/laws/show/1227-18> (дата звернення: 15.10.2022).

12. Про національну безпеку України: Закон України від 21.06.2018 р. Поточна редакція від 15.06.2022. База даних «Законодавство України». URL: <https://zakon.rada.gov.ua/laws/show/964-15> (дата звернення: 20.09.2022).

13. Указ Президента України Про рішення Ради національної безпеки і оборони України від 29.12.2016 року «Про Доктрину інформаційної безпеки України». Поточна редакція 30.12.2021. База даних «Законодавство України». URL: <https://zakon.rada.gov.ua/laws/show/47/2017> (дата звернення: 10.10.2022).

14. Указ Президента України Про рішення Ради національної безпеки і оборони України від 11.03.2021 року «Про створення Центру протидії дезінформації». Поточна редакція 19.03.2021. База даних «Законодавство України». URL: <https://zakon.rada.gov.ua/laws/show/106/2021> (дата звернення: 18.10.2022).

15. Указ Президента України Про рішення Ради національної безпеки і оборони України від 15.10.2021 року «Про Стратегію інформаційної безпеки». Поточна редакція 28.12.2021. База даних «Законодавство України». URL: <https://zakon.rada.gov.ua/laws/show/685/2021> (дата звернення: 15.10.2022).

16. Рішення Ради національної безпеки і оборони України «Щодо реалізації єдиної інформаційної політики в умовах воєнного стану» від 18.03.2022 р. База даних «Законодавство України». URL: <https://zakon.rada.gov.ua/laws/show/n0004525-22> (дата звернення: 05.11.2022).

17. Action Plan against Disinformation. *European Commission contribution to the European Council*. 2018. P. 30. URL: https://ec.europa.eu/info/publications/actionplan-disinformation-commission-contribution-european-council-13-14-december2018_en (дата звернення: 25.08.2022).

18. Code of Practice on Disinformation. *European Commission. Shaping Europe's digital future*. 2018. P. 12. URL: <https://digitalstrategy.ec.europa.eu/en/policies/code-practice-disinformation> (дата звернення: 17.08.2022).

19. Code of Practice on Disinformation – Intermediate targeted monitoring: January reports. European Commission. 2019. P. 3. URL: https://ec.europa.eu/newsroom/dae/document.cfm?doc_id=57596 (дата звернення: 13.09.2022).

20. COVID-19 disinformation monitoring programme. European Commission. *Shaping Europe's digital future*. 2020. URL: <https://digitalstrategy.ec.europa.eu/en/policies/covid-19-disinformation-monitoring> (дата звернення: 13.09.2022).

21. EU Action Plan on Strategic Communication. 2015. URL: <https://www.europeansources.info/record/eu-launches-reaction-to-russian-campaigns-of-disinformation/> (дата звернення: 23.08.2022).

22. EU strategic communication to counteract propaganda against it by third parties. *European Parliament*. 2016. P. 22. URL: <https://eur-lex.europa.eu/legalcontent/EN/TXT/?uri=CELEX%3A52016IP0441> (дата звернення: 19.08.2022).

23. European Democracy Action Plan. European Commission. 2020. URL: https://ec.europa.eu/commission/presscorner/detail/en/ip_20_2250 (дата звернення: 13.09.2022).

24. European Parliament resolution of 16 December 2008 on media literacy in a digital world (2008/2129(INI)). *European Parliament*. 2008. URL: https://www.europarl.europa.eu/doceo/document/TA-6-2008-0598_EN.html (дата звернення: 13.10.2022).

25. Foreign electoral interference and disinformation in national and European democratic processes. *European Parliament*. 2019. P.8. URL: https://www.europarl.europa.eu/doceo/document/TA-9-2019-0031_EN.pdf (дата звернення: 07.09.2022).

26. Guidance on Strengthening the Code of Practice on Disinformation. *European Commission. Shaping Europe's digital future*. 2021. URL: <https://digitalstrategy.ec.europa.eu/en/library/guidance-strengthening-code-practicedisinformation> (дата звернення: 04.10.2022).

27. Joint Framework on countering hybrid threats a European Union response. *European Commission*. 2016. P.18. URL: <http://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:52016JC0018&rid=1> (дата звернення: 09.09.2022).

28. Recommendation for Media Education. *Parliamentary Assembly*. 2000. URL: <http://www.assembly.coe.int/nw/xml/xref/xrefxml2htmlen.asp?fileid=16811&lang=en> (дата звернення: 15.10.2022).

29. Tackling COVID-19 infodemic - Getting the facts right. *European Commission*. 2020. URL: <https://eur-lex.europa.eu/legalcontent/EN/TXT/?uri=CELEX%3A52020JC0008> (дата звернення: 01.09.2022).

Офіційні вебсайти/портали підприємств, установ, організацій та їхні офіційні сторінки/блоги у соціальних мережах

30. Офіційний сайт Служби безпеки України. URL: <https://ssu.gov.ua/> (дата звернення: 06.10.2022).
31. Офіційний сайт інтернет-видання «Українська правда». URL: <https://www.pravda.com.ua> (дата звернення: 09.10.2022).
32. Офіційний сайт Центру протидії дезінформації. URL: <https://cpd.gov.ua/> (дата звернення: 25.10.2022).
33. Офіційний сайт Центру стратегічних комунікацій та інформаційної безпеки. URL: <https://spravdi.gov.ua/> (дата звернення: 09.11.2022).
34. Офіційна сторінка Центру протидії дезінформації у соціальній мережі «Інстаграм». URL: <https://instagram.com/cpd.gov.ua> (дата звернення: 13.09.2022).

Наукові, довідкові, навчальні видання

35. «Біла книга» Служби зовнішньої розвідки України. *Служба зовнішньої розвідки України*. 2021. URL: <https://bit.ly/3fQ5uvm> (дата звернення: 19.10.2022).
36. Богуш В. М. Інформаційна безпека держави. Київ: МК-Прес, 2005. 432 с.
37. В Україні запрацював Центр протидії дезінформації. *Радіо Свобода*. 06.04.2021. URL: <https://www.radiosvoboda.org/a/news-tsentr-protydiya-dezinformatsiya/31189623.html> (дата звернення: 26.09.2022).
38. «Гібридна» війна Росії – виклик і загроза для Європи. *Центр Разумкова*. 2016 р. С. 88.
39. Головатий М. Ф. Соціологія політики: навч. посіб. Київ: МАУП, 2003. 504 с.

40. Горбуліна В. П. Світова гібридна війна: український фронт: монографія . Київ: НІСД, 2017.
41. Гороховський О. Фактчек як тренд розслідувань: можливості та перспективи. Дніпро: *ЛІРА*. 2017. 133 с.
42. Гуз А.М. Історія захисту інформації в Україні та провідних країнах світу: навч. посібник. Київ: *КНТ*, 2007. 260 с.
43. Для росіян, які хочуть здатись у полон, запустили гарячу телефонну лінію. *Укрінформ*. 18.09.2022. URL: <https://www.ukrinform.ua/rubric-ato/3574055-dla-rosian-aki-hocut-zdatis-u-polon-zapustili-garacu-telefonnu-liniu.html> (дата звернення: 09.10.2022).
44. Дубова Д. В. Фейки, пропаганда, дезінформація та виборчий процес: як нам захистити демократичні практики? Київ: *ТОВ «Видавництво Сталь»*, 2019. 254 с.
45. Звіт з моніторингу дотримання профстандартів в онлайн-медіа. Друга хвиля моніторингу у 2020 році. *Інститут масової інформації*. 14.05.2020. URL: <https://imi.org.ua/monitorings/zvit-z-monitoryngu-dotrymannya-profstandartiv-v-onlajn-media-druga-hvylya-monitoryngu-u-2020-rotsi-i33089> (дата звернення: 09.10.2022).
46. ЗСУ записали звернення до білоруських та російських військових. *Аналітичний портал Слово і Діло*. 11.11.2022. URL: <https://www.slovoidilo.ua/2022/11/11/novyna/suspilstvo/zsu-zapysaly-zvernennya-biloruskyx-ta-rosijskyx-vijskovyx> (дата звернення: 09.10.2022).
47. Іванов В. Медіаосвіта та медіаграмотність: короткий огляд. *Академія української преси*. 2011. 58 с.
48. ІМІ рекомендує читати новини з достовірних джерел. *Інститут масової інформації*. 15.03.2022. URL: <https://imi.org.ua/news/imi-rekomenduyechytaty-novyny-z-dostovirnyh-media-spysok-i44370> (дата звернення: 14.10.2022).
49. ІМІ склав список 10 сайтів з якісною інформацією. *Інститут масової інформації*. 21.01.2021. URL: <https://imi.org.ua/news/imi-sklav-spysok-10-sajtiv-z-yakisnoyu-informatsiyeyu-i37201> (дата звернення: 09.11.2022).

50. Карлова В. Проблема формування загальнонаціональної ідеології в Україні. *Вісник національної академії державного управління при Президентові України*. 2010. № 42. С. 17-24.
51. Карпенко В. Інформаційний простір як чинник національної безпеки: науковий громадсько-політичний культурно-мистецький релігійно-філософський педагогічний журнал. *Українознавство*, 2005. № 3. 182-192 с.
52. Кіца М. Особливості та методи виявлення фейкової інформації в українських ЗМІ. *Національний університет «Львівська політехніка»*. 2017. С. 30-35.
53. Костюк І.А. Інформаційні війни в контексті революційних подій в Україні. *Актуальні проблеми соціальних комунікацій: матеріали студентської наукової конференції*. Київ, 2014. 57-60 с.
54. Лавникевич Д. Фейки як нова медіареальність. 2016. URL: <http://mediakritika.by/article/3573/feyki-kak-novaya-media-realnost> (дата звернення: 12.09.2022).
55. Магда Є. Виклики гібридної війни: інформаційний вимір. *Наукові записки Інституту законодавства Верховної Ради України*. 2014. № 5. С. 138-142.
56. Маклюен М. Розуміння медіа: Зовнішнє розширення людини. Переклад, с англ. В. Ніколайова. КАНОН-пресс-Ц. 2003. 464 с.
57. Мартинюк. В. Гібридні загрози Україні і суспільна безпека. *Досвід ЄС і Східного партнерства*. 2018. С. 105.
58. Мудра І. Поняття «фейк» та його види у ЗМІ. *Теле- та радіожурналістика, № 15*. 2016. С. 184 – 188.
59. Ожеван М.А. Маніпулятивні стратегії. *Підприємництво в Україні*. 2001. №9. 27 с.
60. Почепцов Г. (Дез)інформація. *Детектор Медіа*. 2019. 248 с.
61. Почепцов Г. Сучасні інформаційні війни. Київ: Києво-Могилянська акад., 2015. 498 с.

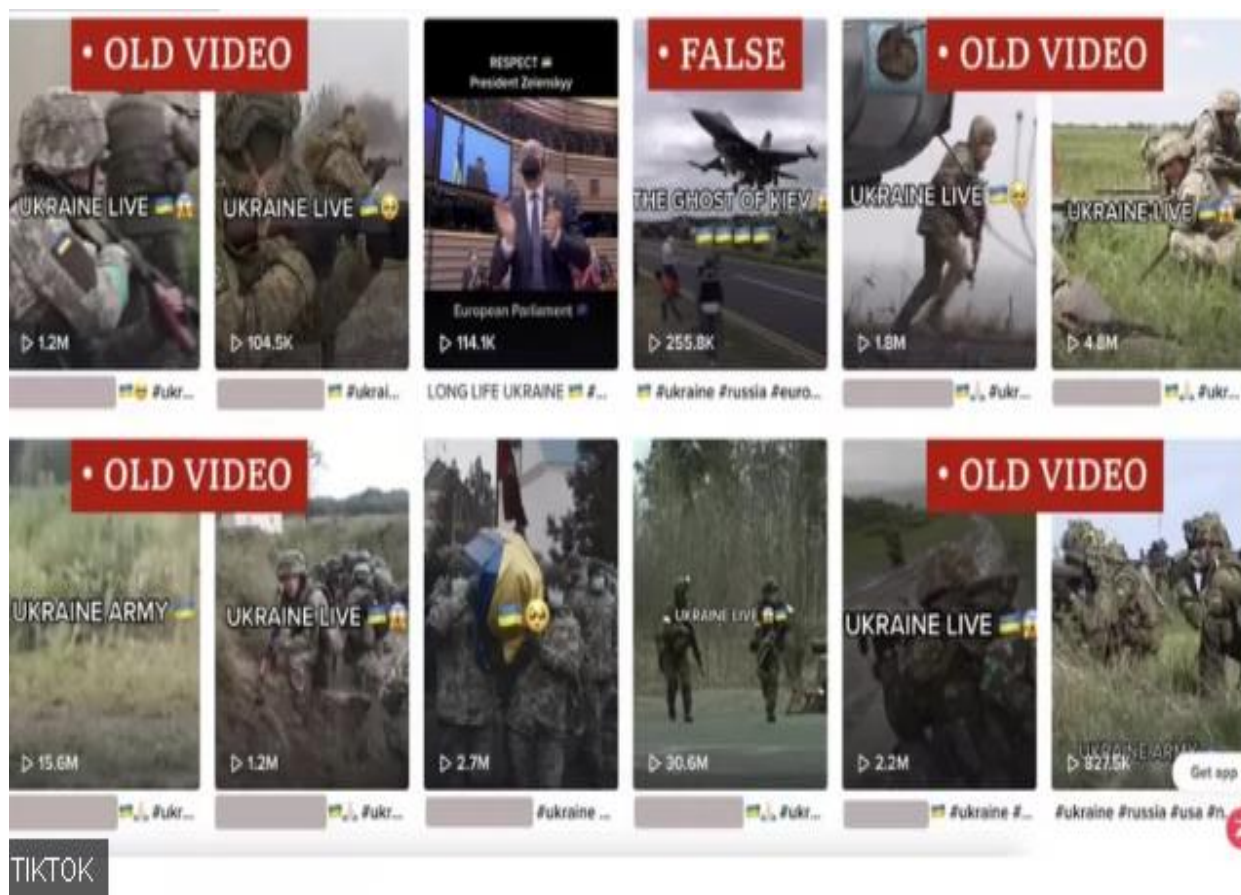
62. Радковець Ю. І. Ознаки технологій «гібридної війни» в агресивних діях Росії проти України. *Наука і оборона*. 2014. № 3. С. 36-42.
63. РНБО створила Центр протидії дезінформації. *Офіційний вебсайт Укрінформ*. 11.03.2021. URL: <https://www.ukrinform.ua/rubric-politics/3206454-rnbo-stvorila-centr-protidii-dezinformacii.html> (дата звернення: 21.10.2022).
64. Реформа медіапростору: Україна наближається до ЄС чи навпаки обмежує свободу слова? *Радіо Свобода*. 08.10.2022. URL: <https://www.radiosvoboda.org/a/reforma-mediaprostoru-ukrayina-yes/32071332.html> (дата звернення: 24.10.2022).
65. Саприкін О. Інформаційна експансія, інформаційна війна та інформаційна атака у засобах масової інформації. *Вісник Книжкової палати*. 2013. № 1. 40-43 с.
66. СБУ від початку війни просила Telegram заблокувати понад 1,5 тисячі анонімних каналів. *Українська правда*. 09.11.2022. URL: <https://www.pravda.com.ua/news/2022/11/9/7375618/> (дата звернення: 09.10.2022).
67. Середа М. О. Проблеми протидії поширенню деструктивної пропаганди та дезінформації в Європейському Союзі. Чернівці. 2021. С. 96.
68. Соціальні мережі як інструмент сучасної інформаційно-психологічної війни. *Army UA*. 2016. URL: <http://www.armyua.com.ua/socialni-merezhi-yak-instrument-suchas> (дата звернення: 17.10.2022).
69. Ткач В. Ф. Спецпропаганда як інформаційний складник гібридної війни Росії проти України. *Стратегічні пріоритети*. Серія: «Політика». 2016. № 1. С. 99-109.
70. Удовиченко К. Методи та засоби перевірки фактажу в умовах інформаційної війни. *Молодий вчений*. 2017. № 11. С. 773-776.
71. Центр протидії дезінформації розпочав роботу. *Офіційний вебсайт Укрінформ*. 2021. URL: <https://www.ukrinform.ua/rubric-politics/3222362-centr-protidii-dezinformacii-rozposav-robotu.html> (дата звернення: 29.09.2022).
72. Цуканова О. В. Інформаційні війни: вплив на суспільство. Київ. 2014. С. 6.

73. Чирва Р. Інформаційна війна – зброя, страшніша за ядерну. *Профспілкові вісті*, 2014. № 13. С. 8-9.
74. Шевчук П. Інформаційно-психологічна війна Росії проти України: як їй протидіяти. *Демократичне врядування*. 2014. Вип. 13.
75. Шевченко В. Е. Фактчекінг і верифікація в журналістській роботі. *Образ: науковий журнал*. Вип. 1. 2018. С.140-153.
76. Шлапаченко В. Дезінформація як спосіб інформаційно-психологічного впливу. *Інформаційна безпека людини, суспільства, держави*. № 2. 2013. С. 78-86.
77. Шпига П. С. Основні технології та закономірності інформаційної війни. *Проблеми міжнародних відносин*. 2014. Вип. 8. С. 326-339.
78. Як протидіяти російській пропаганді розказали медіа-експерти. *Центр міжнародної безпеки та партнерства*. URL: <https://www.ispc.org.ua/archives/1274> (дата звернення: 09.10.2022).
79. Як стратегічні комунікації допомагають Україні налагодити міжнародну співпрацю з протидії ворожій дезінформації. 2021. URL: <https://armyinform.com.ua/2021/12/09/yak-strategichni-komunikacziyi-dopomagayut-ukrayini-nalagodyty-mizhнародnu-spivpraczyu-z-protydiyi-vorozhij-dezinformacziyi/>. (дата звернення: 29.09.2022).
80. Як фейки про війну в Україні збирають мільйони переглядів у TikTok. *BBC*. 26.04.2022. URL: <https://www.bbc.com/ukrainian/features-61220423> (дата звернення: 09.10.2022).

ДОДАТКИ

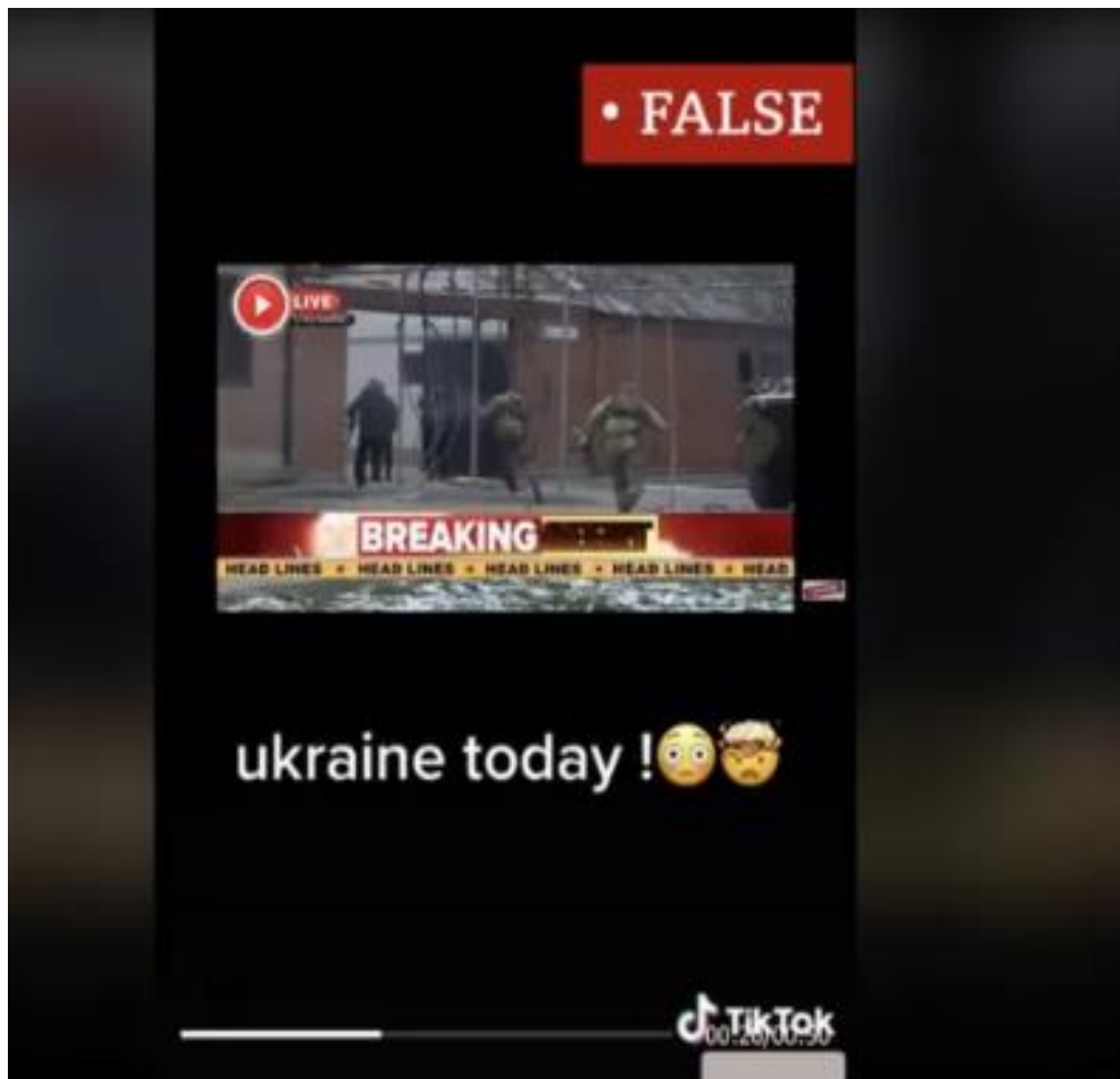
ДОДАТОК А

ЗНІМОК ЕКРАНУ АКАУНТУ КОРИСТУВАЧА ТІКТОКУ, ЯКИЙ ПОШИРЮЄ НЕПРАВДИВУ ІНФОРМАЦІЮ ЩОДО ВІЙНИ РОСІЇ ПРОТИ УКРАЇНИ [80]



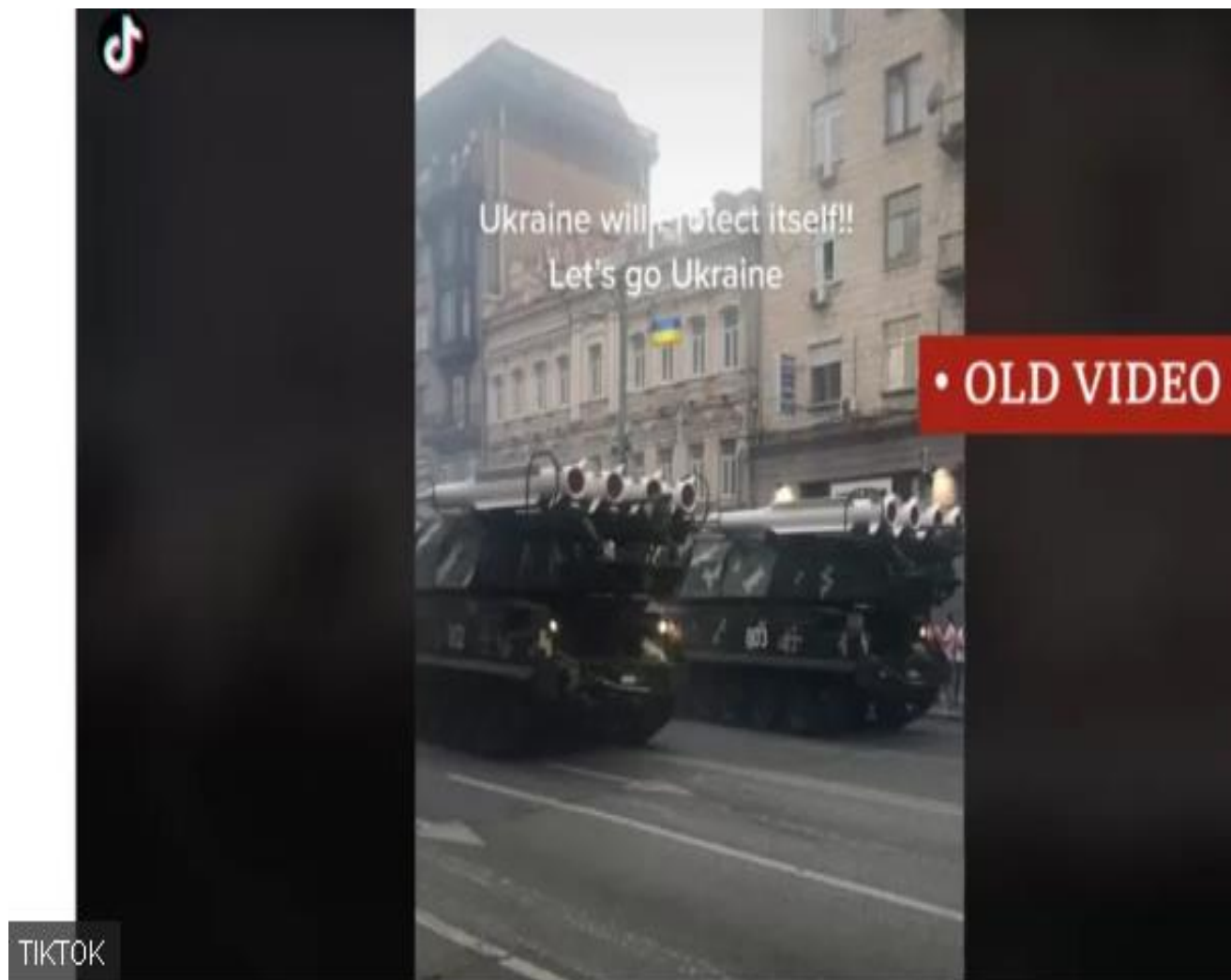
ДОДАТОК Б

ЗНІМОК ЕКРАНУ ВІДЕО З АКАУНТУ КОРИСТУВАЧА ТІКТОКУ,
ЯКИЙ ПОШИРЮЄ НЕПРАВДИВУ ІНФОРМАЦІЮ ЩОДО ВІЙНИ РОСІЇ
ПРОТИ УКРАЇНИ [80]

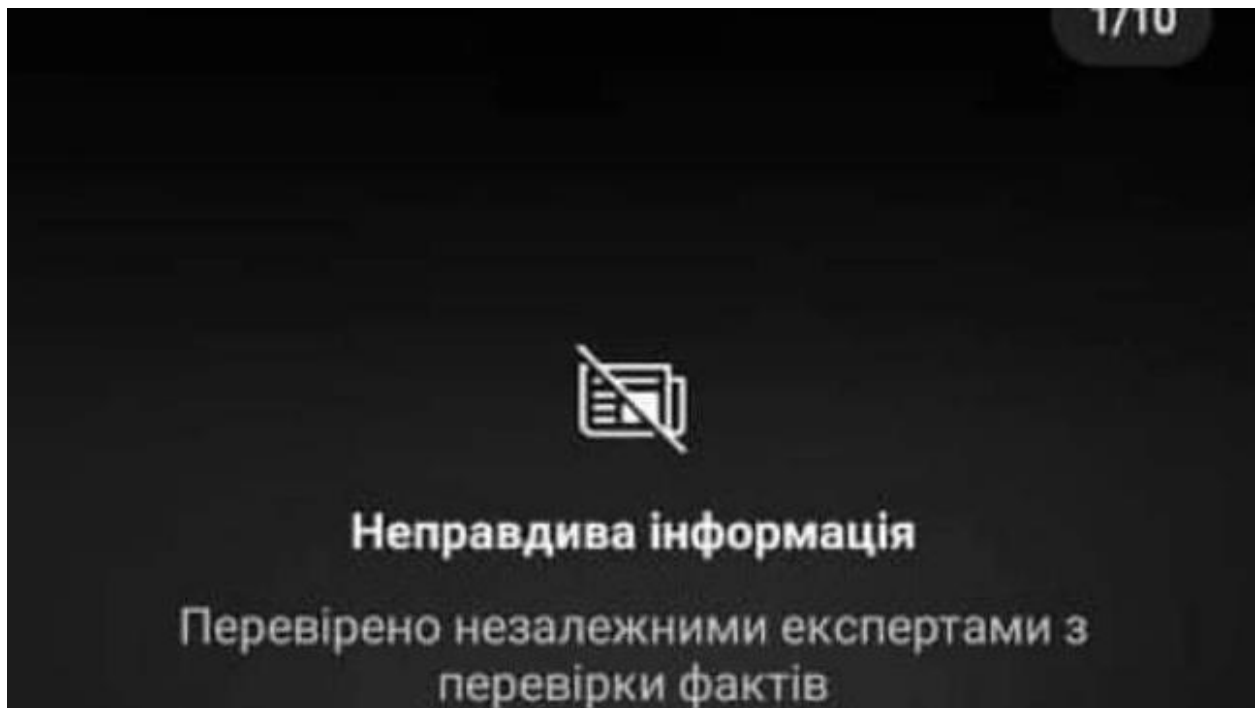


ДОДАТОК В

ЗНІМОК ЕКРАНУ ВІДЕО З АКАУНТУ КОРИСТУВАЧА ТІКТОКУ,
ЯКИЙ ПОШИРЮЄ НЕПРАВДИВУ ІНФОРМАЦІЮ ЩОДО ВІЙНИ РОСІЇ
ПРОТИ УКРАЇНИ [80]

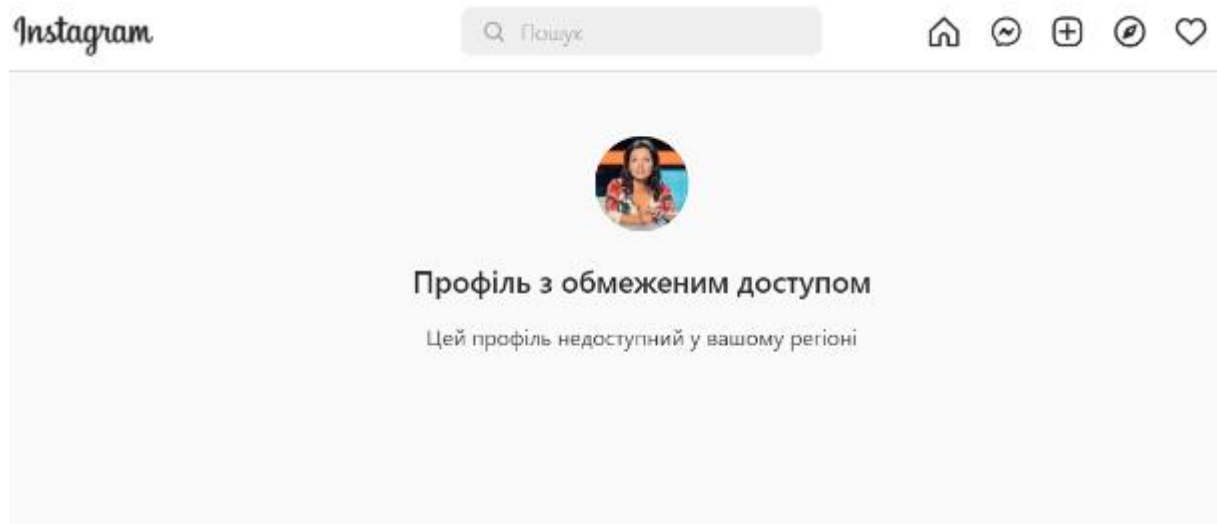


ДОДАТОК Г
СКРІН ВІДМІТКИ ПУБЛІКАЦІЇ В ІНСТАГРАМІ, ЯКА ПОЗНАЧАЄ,
ЩО ЦЕ ФЕЙКОВИЙ КОНТЕНТ ПРО УКРАЇНУ [80]



ДОДАТОК Д

СКРІН ВІДМІТКИ НА АКАУНТІ В ІНСТАГРАМІ, ЯКА ПОЗНАЧАЄ,
ЩО ЦЕЙ АКАУНТ РОЗРАХОВАНИЙ ЛИШЕ ДЛЯ РОСІЙСЬКОГО
ГЛЯДАЧА І МОЖЕ МІСТИТИ НЕПРАВДИВИЙ КОНТЕНТ [80]



ДОДАТОК Е

МОНІТОРИНГ КІЛЬКОСТІ ФЕЙКІВ, ПРЕДСТАВЛЕНИХ НА
ОФІЦІЙНОМУ ВЕБСАЙТІ ЦЕНТРУ ПРОТИДІЇ ДЕЗІНФОРМАЦІЇ ПРИ РНБО
ТА ОФІЦІЙНОМУ ВЕБСАЙТІ ВИДАННЯ «УКРАЇНСЬКА ПРАВДА»

[31], [34]



Рисунок 1 – Результати моніторингу за лютий 2022 р.

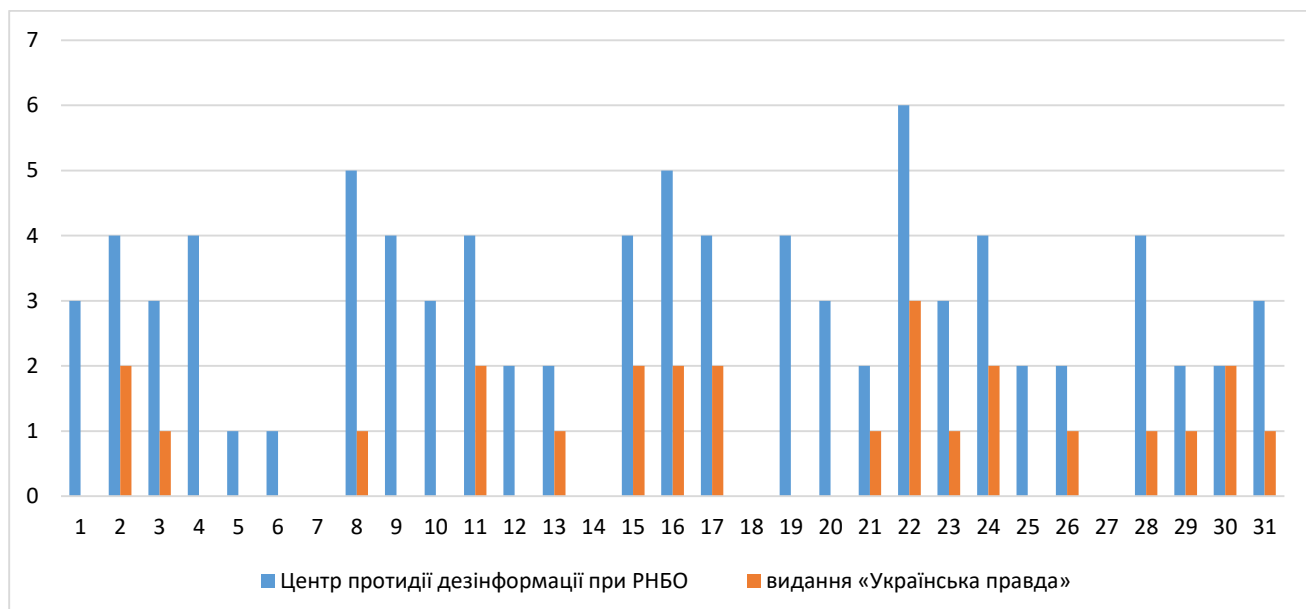


Рисунок 2 – Результати моніторингу за березень 2022 р.

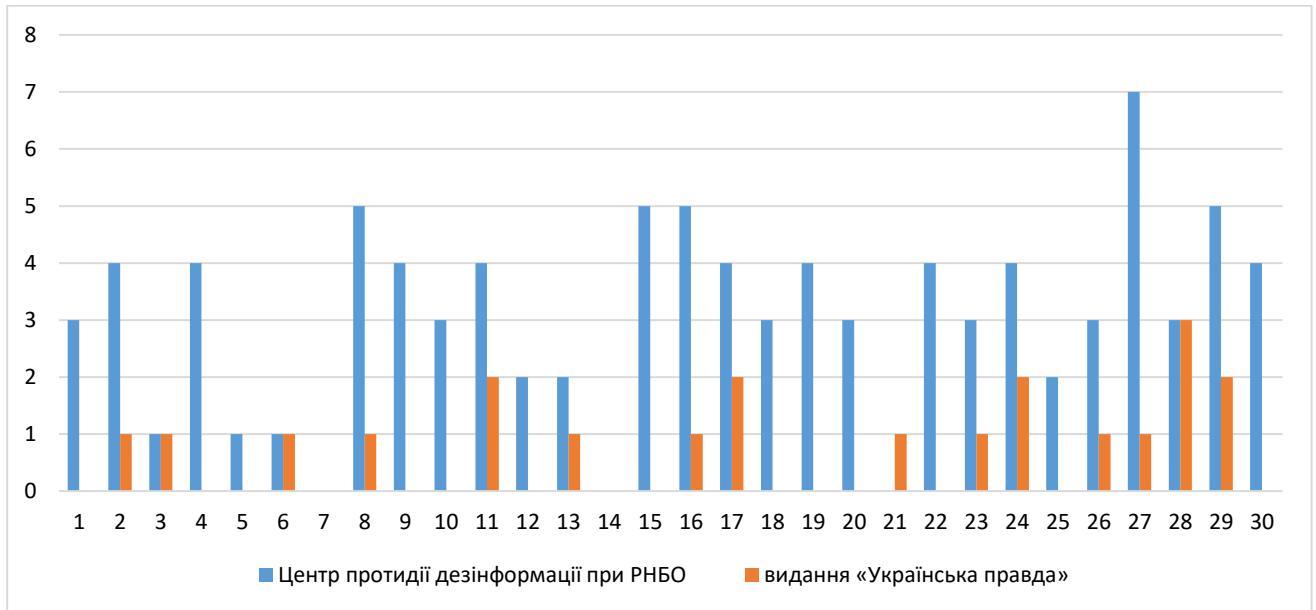


Рисунок 3 – Результати моніторингу за квітень 2022 р.

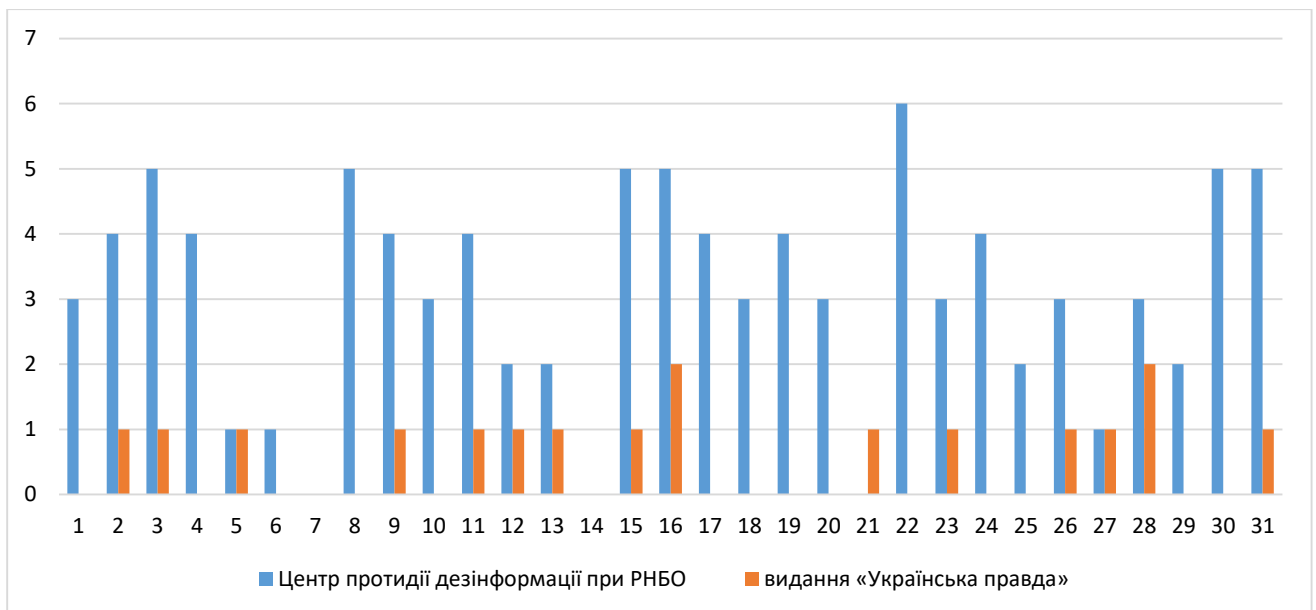


Рисунок 4 – Результати моніторингу за травень 2022 р.

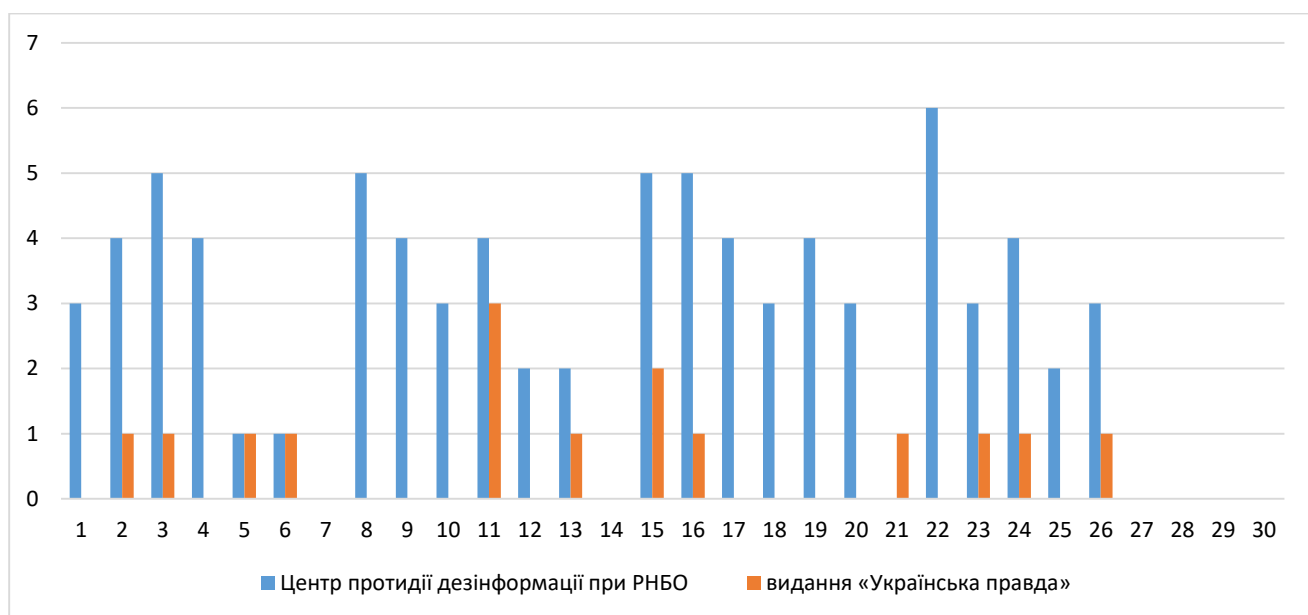


Рисунок 5 – Результати моніторингу за червень 2022 р.

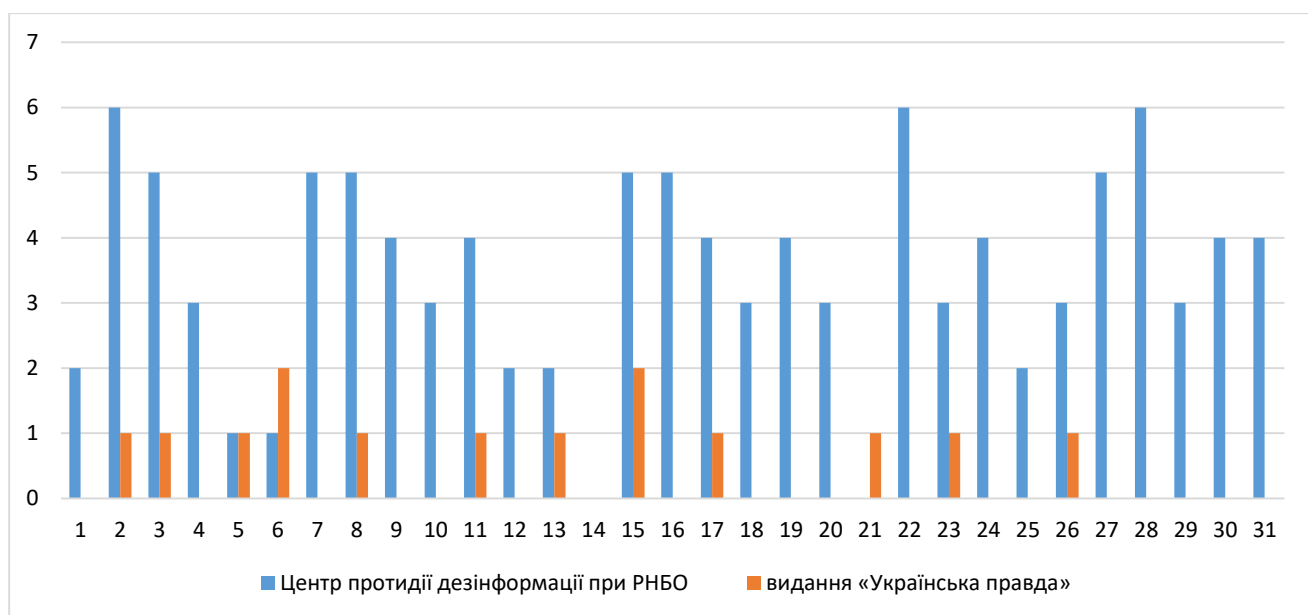


Рисунок 6 – Результати моніторингу за липень 2022 р.

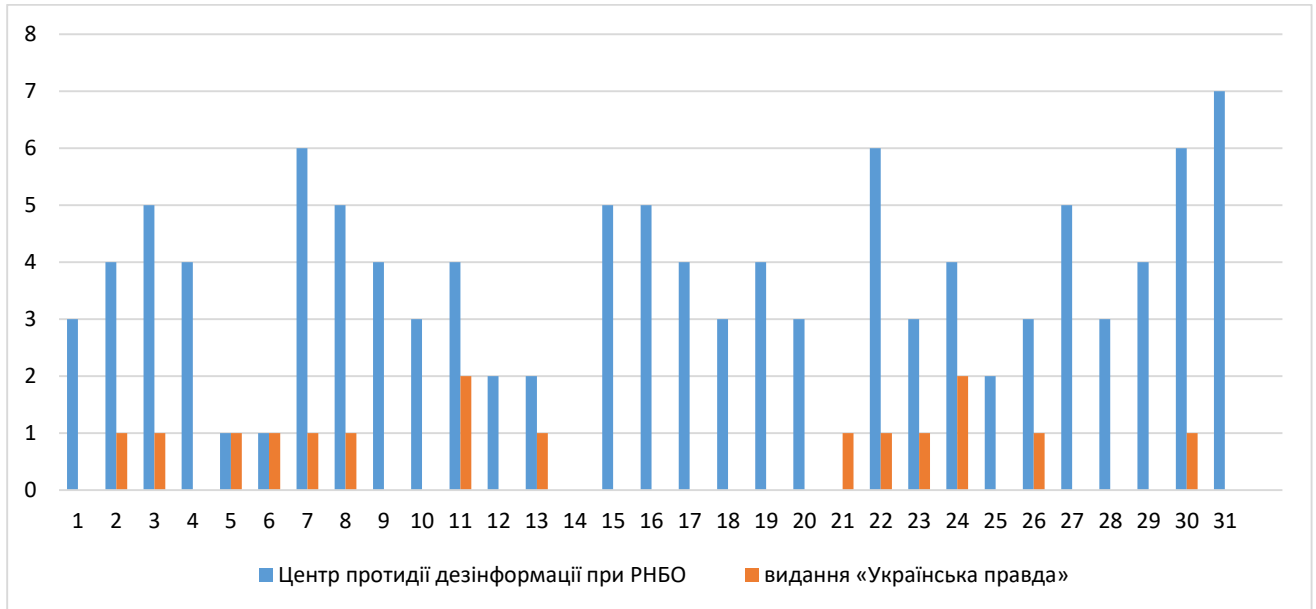


Рисунок 7 – Результати моніторингу за серпень 2022 р.

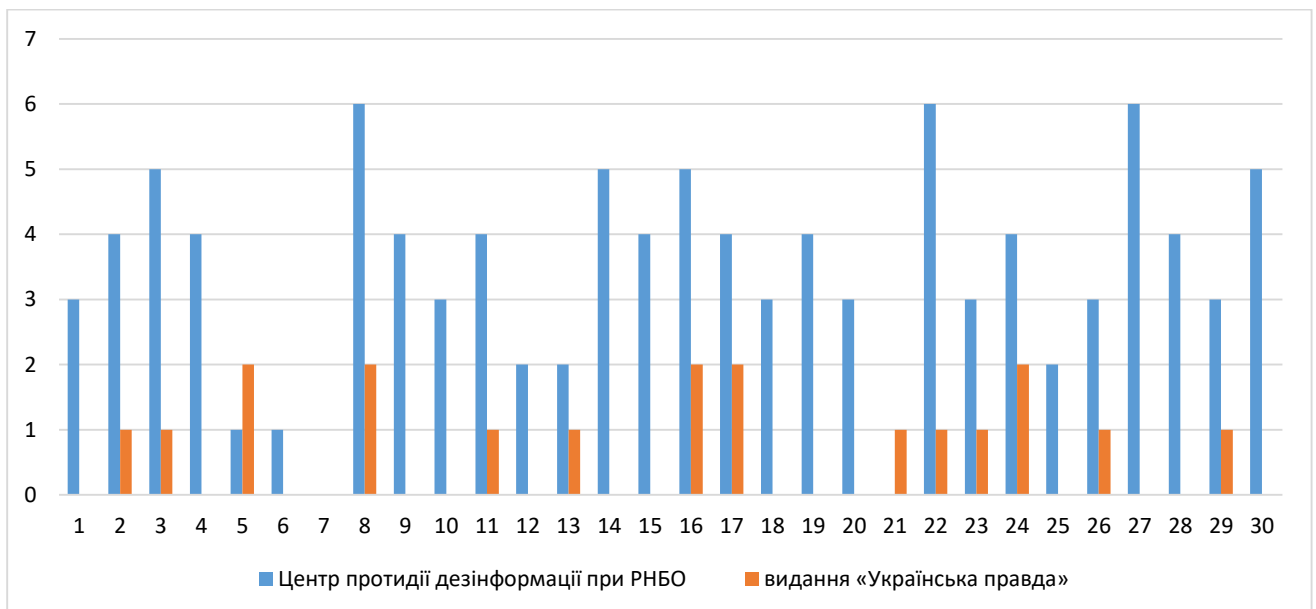


Рисунок 8 – Результати моніторингу за вересень 2022 р.

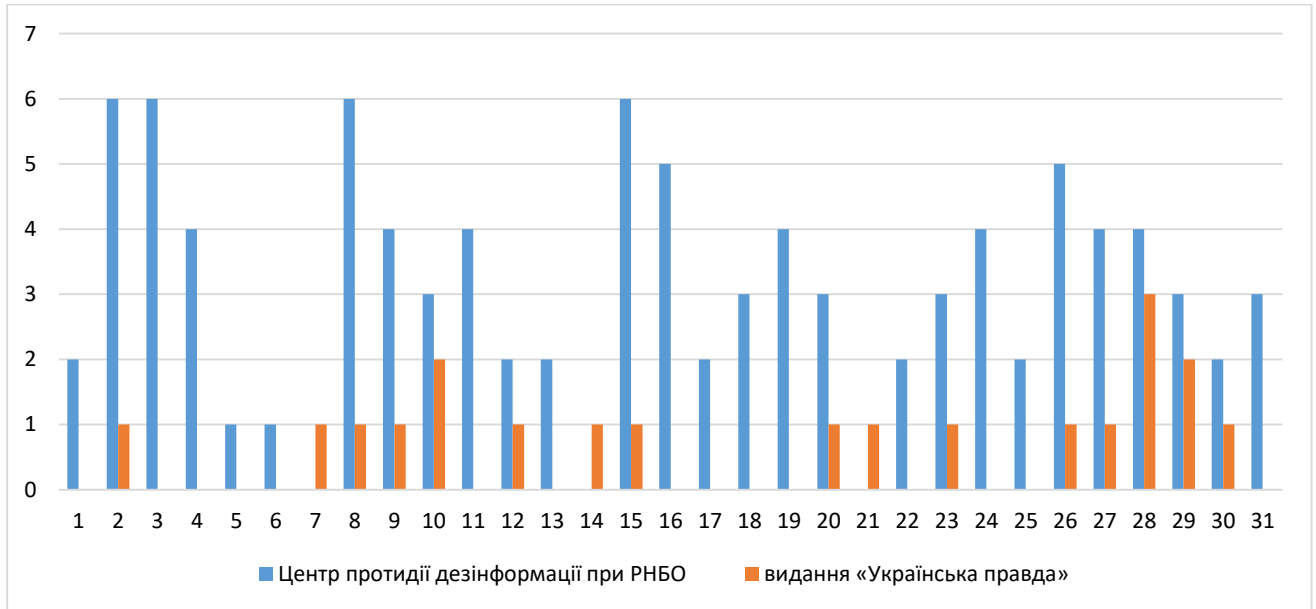


Рисунок 9 – Результати моніторингу за жовтень 2022 р.

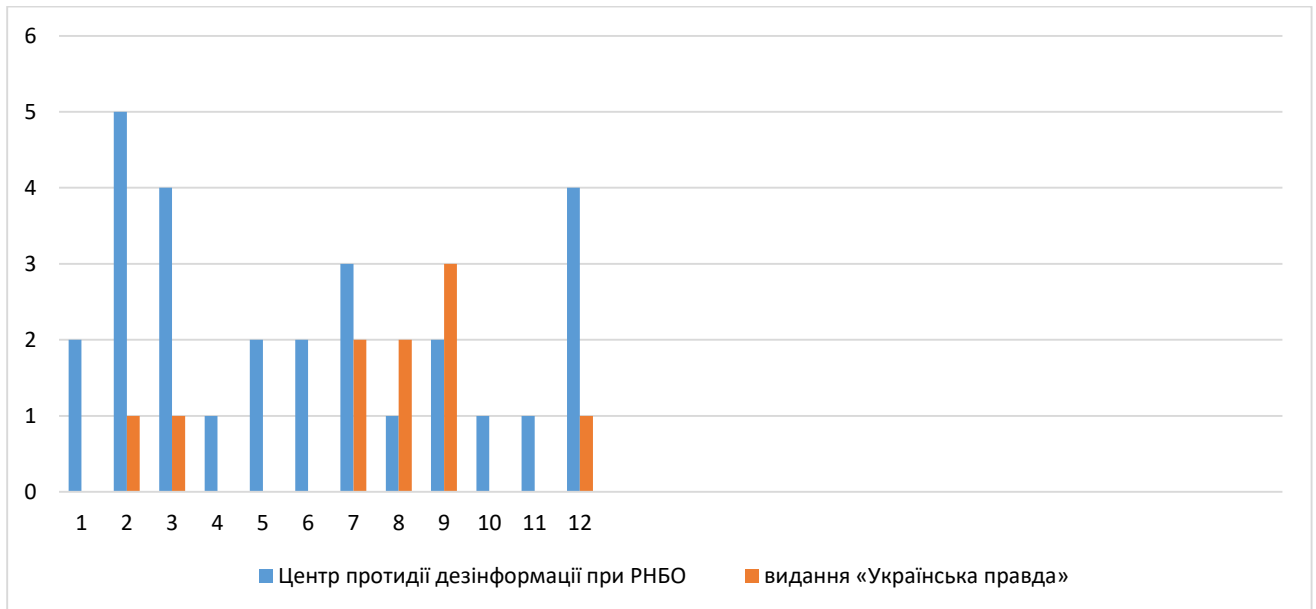


Рисунок 10 – Результати моніторингу за листопад 2022 р.

Примітка: розроблено автором.