

**ДЕРЖАВНИЙ УНІВЕРСИТЕТ
ІНФОРМАЦІЙНО-КОМУНІКАЦІЙНИХ ТЕХНОЛОГІЙ
НАВЧАЛЬНО-НАУКОВИЙ ІНСТИТУТ МЕНЕДЖМЕНТУ
ТА ПІДПРИЄМНИЦТВА
КАФЕДРА ДОКУМЕНТОЗНАВСТВА ТА ІНФОРМАЦІЙНОЇ
ДІЯЛЬНОСТІ**

КВАЛІФІКАЦІЙНА МАГІСТЕРСЬКА РОБОТА

на тему: «Види і технології інформаційних війн»

на здобуття освітнього ступеня	<u>магістра</u>
зі спеціальності	<u>029 Інформаційна, бібліотечна та архівна</u>
	<u>справа</u>
освітньо-професійної програми	<u>Управління інформаційно-комунікаційною</u>
	<u>діяльністю</u>

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

(підпис)

Євгеній ОБЕРТАС

Виконав:	здобувач вищої освіти гр. ДЗДМ-62 Євгеній Обертас
Керівник:	Володимир ДАНИЛЕНКО, к.філол.н, доц.кафедри.
Рецензент:	Світлана СТЕЖКО, к.філол.н., доцент.

Київ 2024

Завдання на кваліфікаційну роботу

ДЕРЖАВНИЙ УНІВЕРСИТЕТ ІНФОРМАЦІЙНО-КОМУНІКАЦІЙНИХ ТЕХНОЛОГІЙ Навчально-науковий інститут менеджменту та підприємництва

Кафедра документознавства та інформаційної діяльності
 Ступінь вищої освіти магістр
 Спеціальність 029 Інформаційна, бібліотечна та архівна справа
 Освітньо-професійна програма Управління інформаційно-комунікаційною діяльністю

ЗАТВЕРДЖУЮ

Завідувач кафедри

_____ Тетяна СИДОРЕНКО
 «_____» _____ 202_ р.

ЗАВДАННЯ НА КВАЛІФІКАЦІЙНУ РОБОТУ

Обертаса Євгенія Олеговича

1. Тема кваліфікаційної роботи: «Види і технології інформаційних війн»
 керівник кваліфікаційної роботи Володимир ДАНИЛЕНКО, к.філол.н,
 доц.кафедри.

затверджені наказом Державного університету інформаційно-комунікаційних
 технологій від «15» жовтня 2024 р. № 320

2. Строк подання кваліфікаційної роботи «16» грудня 2024р.

3. Вихідні дані до кваліфікаційної роботи

Мета дослідження - аналіз видів та технологій інформаційних війн, їх впливу на
 суспільно-політичні процеси та розробка рекомендацій щодо протидії.

Об'єктом дослідження є інформаційні війни як соціально-політичне явище.

Предметом дослідження є види, технології та особливості інформаційних війн в
 Україні, а також методи протидії.

4. Перелік питань, які потрібно розробити

1. Сутність, види та технології інформаційних війн.

2. Передумови розвитку інформаційних війн в Україні.

3. Наслідки та протидія інформаційним війнам в Україні.

5. Перелік ілюстративного матеріалу: *презентація*

6. Дата видачі завдання «09» Вересня 2024 р.

КАЛЕНДАРНИЙ ПЛАН

№ з/п	Назва етапів кваліфікаційної роботи	Строк виконання етапів роботи	Примітки
1	Визначення тематики, вибір наукового керівника, уточнення теми	09.09.2024	<i>виконано</i>
2	Розроблення та складання плану кваліфікаційної магістерської роботи	18.09.2024	<i>виконано</i>
3	Підготовка 1 розділу	18.11.2024	<i>виконано</i>
4	Підготовка 2 розділу	25.11.2024	<i>виконано</i>
5	Підготовка 3 розділу	04.12.2024	<i>виконано</i>
6	Висновки	05.12.2024	<i>виконано</i>
7	Підготовка остаточного варіанта роботи	08.12.2024	<i>виконано</i>
8	Написання відгуку науковим керівником	13.12.2024	<i>виконано</i>
9	Оформлення та представлення роботи на кафедрі та перевірка на плагіат	16.12.2024	<i>виконано</i>
10	Підготовка доповіді, презентації та ілюстративного матеріалу, рецензія	18.12.2024	<i>виконано</i>
11	Попередній захист роботи	20.12.2024	<i>виконано</i>
12	Основний захист кваліфікаційної магістерської роботи	22.01.2025	<i>виконано</i>

Здобувач вищої освіти

Євгеній ОБЕРТАС

Керівник
кваліфікаційної роботи

Володимир ДАНИЛЕНКО

АНОТАЦІЯ

Текстова частина кваліфікаційної роботи на здобуття освітнього ступеня магістра: __59__ стор., __14__ рис., __1__ табл., __49__ джерел.

Мета роботи – полягає у дослідженні сутності, видів і технологій інформаційних війн, аналізі їх розвитку в Україні, особливо в контексті російсько-української війни, а також у вивченні наслідків і розробці ефективних заходів протидії.

Об’єкт дослідження – Інформаційні війни як соціально-політичне явище.

Предмет дослідження – Види, технології та особливості інформаційних війн в Україні, а також методи протидії.

Короткий зміст роботи: Дослідження присвячене аналізу інформаційних війн як суспільно-політичного феномену, їх видів і технологій. Розглянуто передумови розвитку інформаційної боротьби, особливості її ведення в Україні, зокрема в контексті російсько-української війни. Окрема увага приділяється ролі соціальних мереж у державній політиці та протидії дезінформації. У роботі також висвітлено наслідки інформаційних війн та запропоновано методи протидії інформаційному впливу проти України.

КЛЮЧОВІ СЛОВА: Інформаційна війна, соціальні мережі, дезінформація, пропаганда, російсько-українська війна, інформаційна безпека, суспільно-політичний вплив, технології інформаційних війн, протидія інформаційним загрозам.

Анотація англійською мовою
для кваліфікаційної магістерської роботи

ABSTRACT

Text part of the master's qualification work: __59_ pages, _14__ pictures, __1__ table, __49__ sources.

The purpose of the work is to explore the essence, types, and technologies of information wars, analyze their development in Ukraine, particularly in the context of the Russian-Ukrainian war, as well as to examine their consequences and develop effective countermeasures.

Object of research is information wars as a socio-political phenomenon.

Subject of research is types, technologies, and characteristics of information wars in Ukraine, as well as countermeasures.

Summary of the work: The research is dedicated to analyzing information wars as a socio-political phenomenon, their types, and technologies. It examines the preconditions for the development of information warfare, the specifics of its conduct in Ukraine, particularly in the context of the Russian-Ukrainian war. Special attention is given to the role of social networks in state policy and countering disinformation. The paper also highlights the consequences of information wars and proposes methods to counter information influence against Ukraine.

Key words Information warfare, social networks, disinformation, propaganda, Russian-Ukrainian war, information security, socio-political influence, technologies of information wars, countering information threats.

Подання голові екзаменаційної комісії щодо захисту кваліфікаційної роботи

**ДЕРЖАВНИЙ УНІВЕРСИТЕТ
ІНФОРМАЦІЙНО-КОМУНІКАЦІЙНИХ ТЕХНОЛОГІЙ
Навчально-науковий інститут менеджменту та підприємництва**

**ПОДАННЯ
ГОЛОВІ ЕКЗАМЕНАЦІЙНОЇ КОМІСІЇ
ЩОДО ЗАХИСТУ КВАЛІФІКАЦІЙНОЇ РОБОТИ
на здобуття освітнього ступеня магістр**

Направляється здобувач _____ до захисту кваліфікаційної роботи за спеціальністю 029 Інформаційна, бібліотечна та архівна справа
(код, найменування спеціальності)
освітньо-професійної програми __Управління інформаційно-комунікаційною діяльністю на тему: «_____».

Кваліфікаційна робота і рецензія додаються.

Директор ННІ _____ Ім'я ПРИЗВИЩЕ

Висновок керівника кваліфікаційної роботи

Керівник кваліфікаційної роботи _____ Ім'я ПРИЗВИЩЕ
«_____» _____ 202_ року

Висновок кафедри про кваліфікаційну роботу

Кваліфікаційна робота розглянута на засіданні кафедри документознавства та інформаційної діяльності. Здобувач _____ допускається до захисту даної роботи в Екзаменаційній комісії.

Завідувач кафедрою _____

Ім'я ПРИЗВИЩЕ

ДОДАТОК Д

Рецензія

РЕЦЕНЗІЯ

**на кваліфікаційну роботу
на здобуття освітнього ступеня бакалавра (магістра)**

здобувача(ки) вищої освіти _____
(прізвище, ім'я, по батькові)

на тему « _____ »

Актуальність.

Позитивні сторони.

- 1.
- 2.
- 3.

Недоліки.

- 1.
- 2.

Відзначені зауваження не впливають на загальну позитивну оцінку кваліфікаційної роботи бакалаврської (магістерської).

Висновок: кваліфікаційна робота на здобуття ступеня бакалавра (магістра) заслуговує оцінку " _____ ", а здобувач(ка) _____ заслуговує присвоєння кваліфікації:

Рецензент:

науковий ступінь, вчене звання

_____ підпис

_____ Ім'я, ПРІЗВИЩЕ

ЗМІСТ

ВСТУП	9
РОЗДІЛ 1. ТЕОРЕТИЧНІ ОСНОВИ ДОСЛІДЖЕННЯ ІНФОРМАЦІЙНИХ ВІЙН	
1.1. Суспільно-політична сутність інформаційних війн	10
1.2. Види і технології інформаційних війн	15
РОЗДІЛ 2. Передумови та сучасний стан розвитку інформаційної війни в Україні	
2.1. Передумови розвитку інформаційних війн	24
2.2. Роль соціальних мереж у державній політиці та обмеженні дезінформації	29
2.3. Особливості ведення інформаційної війни в Україні на прикладі російсько-української війни	35
РОЗДІЛ 3. Наслідки і протидія впливу інформаційної війни проти Росії	
3.1. Наслідки інформаційних війн в Україні	48
3.2. Протидія України в інформаційній війні проти Росії	51
ВИСНОВКИ	61
СПИСОК ВИКОРИСТАНИХ ДЖЕРЕЛ І ЛІТЕРАТУРИ	63

ВСТУП

Сучасний світ характеризується стрімким розвитком інформаційних технологій, які трансформують усі сфери суспільного життя. У умовах глобалізації інформація перестала бути лише засобом передачі знань, перетворившись на потужний інструмент впливу у політичній, економічній та військовій сферах. У цьому контексті феномен інформаційної війни набуває особливого значення, стаючи важливим механізмом боротьби за панування і контроль.

Інформаційна війна є багатогранним явищем, що включає використання дезінформації, інформаційних операцій, кібератак та інших сучасних технологій для досягнення геополітичних цілей. Її вплив не обмежується лише міжнародними відносинами — це явище глибоко зачіпає національну безпеку та суспільно-політичну стабільність. Особливого значення це питання набуло для України, яка з 2014 року є одним із ключових театрів інформаційної війни в умовах конфлікту з Росією.

Соціальні мережі стали важливою платформою для поширення фейків, маніпуляцій і пропаганди. Вони впливають на громадську думку, дестабілізують політичні режими й формують соціальні конфлікти. Аналіз цих процесів необхідний для створення стратегій протидії загрозам інформаційної безпеки.

Дослідження спрямоване на комплексне вивчення передумов, особливостей і наслідків інформаційної війни, зокрема в контексті російсько-українського конфлікту. Вивчення цих аспектів дозволить краще зрозуміти механізми інформаційного впливу і знайти ефективні шляхи їх нейтралізації, що є важливим кроком у забезпеченні стійкості держави до сучасних викликів.

Робота апробована на II Всеукраїнській науково-практичній конференції "Соціальні комунікації в умовах глобалізації суспільства: виклики та перспективи".

РОЗДІЛ 1. ТЕОРЕТИЧНІ ОСНОВИ ДОСЛІДЖЕННЯ ІНФОРМАЦІЙНИХ ВІЙН

1.1. Суспільно-політична сутність інформаційних війн

21 століття називають «інформаційною епохою», і часто можна почути розмови про значний прогрес, досягнутий у боротьбі з інформаційною війною за останні кілька років. Термін «інформаційна війна» не є загальновизнаним. Так В. Лизанчука вважає, що інформаційна війна слугує платформою або стартовим майданчиком для ініціювання реального військового конфлікту [2, с. 13];

Її колега А. Студнік визначає сучасну інформаційну війну як «процес створення певного інтересу для залучених сторін». Він розуміє сучасну інформаційну війну як «самостійну інформаційну стратегію, спрямовану на вплив на суспільну свідомість і громадську думку з метою принесення певних користностей зацікавленим сторонам» [3, с. 89]. Вплив такої інформації призводить до формування найрізноманітніших думок, що ускладнює визначення істини в хаотичних ситуаціях.

Щодо решти українських дослідників, то Г. Почепцов визначає інформаційну війну як комунікаційну технологію, спрямовану на вплив на масову свідомість для досягнення короткострокових або довгострокових цілей [4, с. 20]. Він стверджує, що основною метою інформаційних операцій є створення дестабілізуючого впливу на керівництво держави, особливо військову та політичну еліту з метою маніпулювання суспільною свідомістю [4, с. 169].

Енциклопедія сучасної України надає дещо інше формулювання даного поняття, так «інформаційна війна - це вплив на населення іншої країни шляхом поширення певної інформації в мирний або повоєнний час з метою отримання політичної, економічної або військової переваги та захисту власного населення від такого впливу».

Академіки П. Шпіг та Р. Рудник у своїй роботі виділили чотири підходи до визначення поняття інформаційної війни [5, с. 328]:

- Перший підхід розглядає інформаційну війну як сукупність політичних, правових, соціально-економічних та психологічних дій;
- Другий підхід розглядає інформаційну війну як найбільш насильницьку форму конфлікту в інформаційній сфері, основними факторами якої є відсутність компромісу, висока інтенсивність конфлікту та короткочасність насильницького конфлікту;
- Третій підхід трактує інформаційну війну як спосіб підтримки і проведення військових операцій за допомогою найсучасніших електронних засобів, таких як цифрові передавачі, супутникові передавачі та інші подібні інструменти, що використовуються для виконання військових місій;
- Четвертий підхід ототожнює інформаційну війну з кібервійною, тобто конфліктом між технологічними системами [5, с. 328].

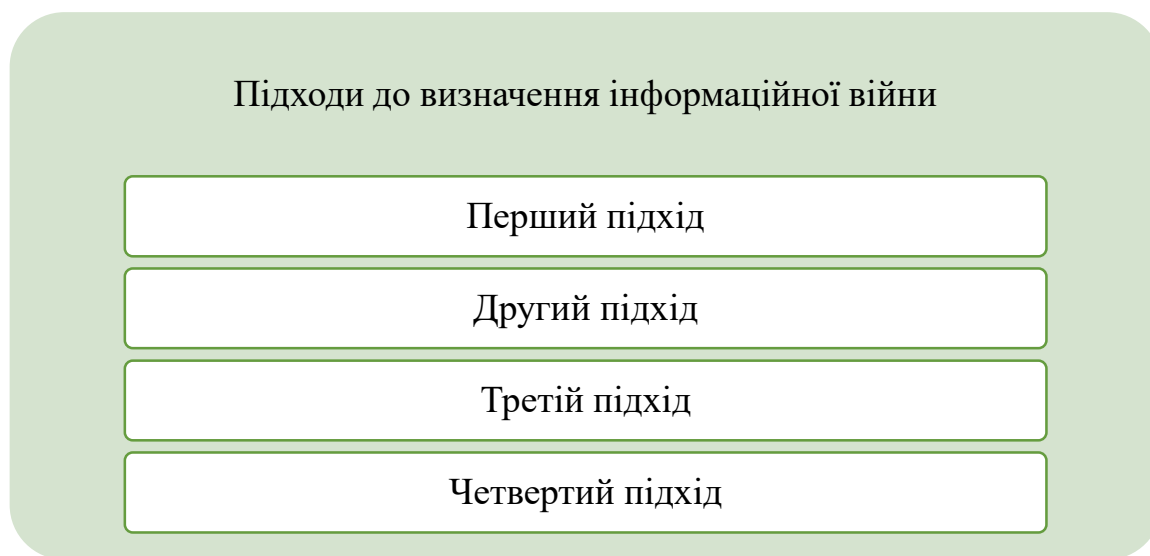


Рис. 1.1. – Перелік підходів до визначення поняття інформаційної війни за думкою П.Шпіг та Р.Рудник

Нині термін «інформаційна війна» можна охарактеризувати у двох значеннях: широкому та вузькому.

У широкому сенсі передбачені конфлікти в інформаційній сфері, в яких використовуються засоби масової інформації для досягнення різних політичних цілей.

У вузькому ж сенсі маються на увазі безпосередньо військові конфлікти в інформаційній сфері, вони спрямовані на отримання односторонньої переваги у зборі, обробці та використанні інформації на полі бою (в операціях і битвах) [6, с. 81-82].

Попри вище зазначеного, сьогодні інформаційна війна є важливим інструментом у міжнародних конфліктах, оскільки має значний вплив на досягнення політичних і стратегічних цілей без застосування фізичної сили. Наразі існує два покоління інформаційних війн: перше і друге покоління, представлено на рис. 1.2.

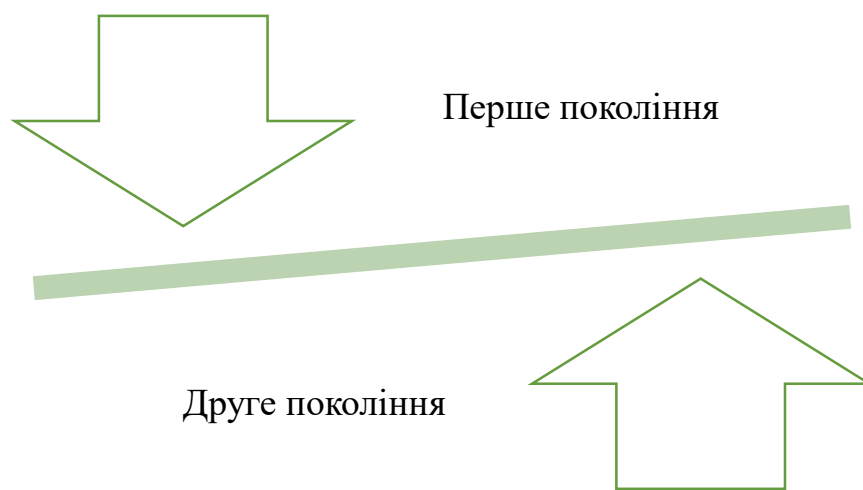


Рис. 1.2. – Покоління інформаційних війн

Перше покоління має наступні аспекти:

- ведення електронної війни;
- отримання розвідувальних даних шляхом перехоплення та розшифровки інформаційних потоків;

- надання великих обсягів дезінформації в канали розвідки противника з метою впливу на осіб, які приймають рішення;
- отримання інформації шляхом перехоплення відкритих джерел розвідки.

Друге покоління зосереджується на дещо інших аспектах:

- створення атмосфери аморальності та негативного ставлення до спадщини;
- маніпулювання національною свідомістю соціальних груп у країні з метою створення політичної напруженості та плутанини;
- дестабілізація політичних відносин між партіями;
- послаблення міжнародного авторитету держави;
- послаблення життєво важливих інтересів держави в політичній, економічній, оборонній та інших сферах.

Щодо суспільно-політичної сутності, то до основних частин даного поняття відносять: маніпулювання громадською думкою, політичний контроль і вплив, наслідки національної безпеки та інформаційну безпеку.

Маніпулювання громадською думкою полягає в тому, що інформаційна війна має впливати на сприйняття громадськістю певних подій чи осіб за допомогою пропаганди, фейкових новин та перекручування фактів. Це може змінити політичні погляди і створити позитивне або негативне ставлення до урядів, лідерів і міжнародних організацій.

Політичний контроль і вплив проявляється у використанні інформаційних технологій для контролю над політичним середовищем у національних або міжнародних справах. Сюди входить маніпулювання виборчим процесом, зміна результатів виборів за допомогою кібератак, а також сприяння політичним кризам і зміні режимів в інших країнах.

Наслідки для національної безпеки можуть бути катастрофічні. Інформаційна війна здатна підірвати національну стабільність, послаблюючи

внутрішній контроль, розпалюючи соціальні протести, і навіть, провокуючи військові конфлікти. Роль інформаційної війни особливо важлива в державних справах, де вона може бути інструментом для зміни внутрішньої політики або провокування конфлікту.

В умовах глобалізації та розвитку цифрових технологій інформаційна війна піднімає питання захисту даних, приватності та управління інформацією як важливим стратегічним ресурсом, це формує, так звану, інформаційну безпеку. Саме тому виклик для людства полягає у створенні механізмів інформаційної безпеки та протидії кіберзагрозам.

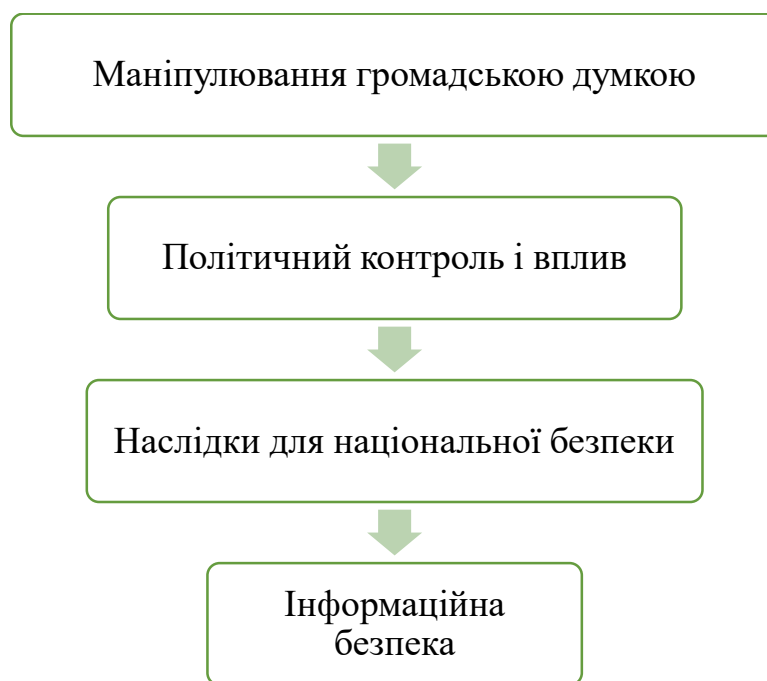


Рис. 1.3. – Основні аспекти суспіль-політичної сутності

Таким чином, інформаційна війна - це інструмент, який використовується для маніпулювання свідомістю, дестабілізації суспільства і досягнення політичних цілей без фізичного насильства. Вона включає пропаганду, фальсифікацію та підтримку військових операцій. Загрози включають підрив національної безпеки, політичний вплив і маніпулювання громадською думкою. Їм можна протидіяти, зміцнюючи інформаційну безпеку та медіаграмотність.

1.2. Види і технології інформаційних війн

Стрімкий розвиток інформаційних технологій зробив інформаційну війну ще більш потужною та ефективною. Кожен вид інформаційної війни має свої інструменти та методи для ефективного маніпулювання інформаційними потоками. Загалом виділяють три основні види війни: психологічна війна, гібридна війна та кібервійна.

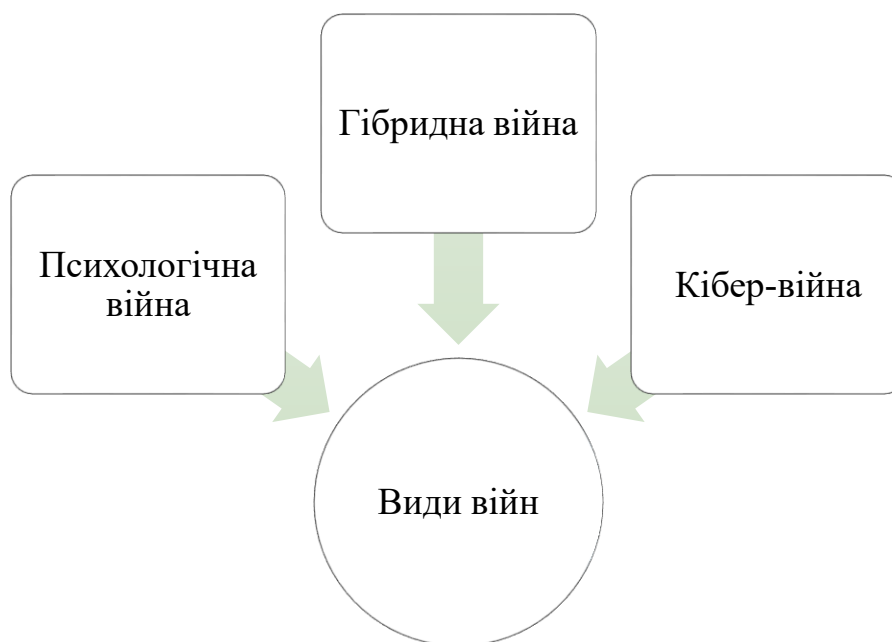


Рис. 1.4. – Види інформаційних війн

Психологічна війна - це метод цілеспрямованої пропаганди, спрямований на залякування, запам'ятовування, деморалізацію та інший вплив на моральний дух і світогляд противника. Основними мішенями таких атак є уряди, різні організації, військові та громадські діячі.

Хоча цей метод здається новим, психологічна війна тісно пов'язана з поняттям війни. Ще в 13 столітті Чингісхан відрубав голови своїм переможеним ворогам, щоб зміцнити свою репутацію могутньої і кровожерливої монгольської армії.

Інший приклад - операція «Скайвар», яку проводив уряд США під час Другої світової війни. У своїй книзі «Психологічна війна проти нацистської Німеччини» колишній агент Деніел Лернер визначає пропаганду в трьох категоріях:

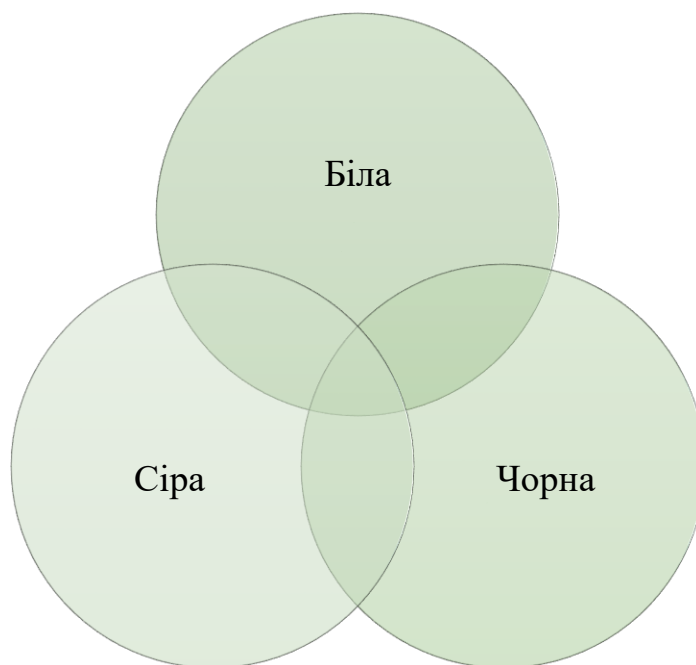


Рис. 1.5. – Категорії пропаганди

Біла пропаганда характеризується точною інформацією в наданих межах. Джерело інформації чітко вказане.

Сіра пропаганда - це інформація від місцевих органів влади, яка не містить спростовуваної інформації, але джерело інформації не вказано.

Чорна пропаганда, як випливає з назви, називається «фейковими новинами», коли інформація є неправдивою або такою, що вводить в оману.

У будь-якому випадку, пропаганда передбачає використання психологічного тиску для отримання інформації, що є деморалізуючим методом.

Якщо раніше психологічний тиск полягав у поширенні друкованих матеріалів із закликами до капітуляції, то зараз він активно поширюється через соціальні мережі. Створюються штучні ситуації, які втомлюють людей на

тривалий час, наприклад, позбавлення сну, постійне відтворення звуків ворожої техніки та погрози застосувати ядерну зброю, щоб психічно виснажити людей. Що стосується військовослужбовців безпосередньо на полі бою та окупованого цивільного населення, то, крім вищезазначеного, вони наражаються на пастки, снайперів, засідки, неправильно розміщену вибухівку тощо, а також перебувають у постійному стресі через відсутність довіри до місцевості.

Кібервійну часто визначають як кібератаку або серію атак на інформаційні системи країни. Ці атаки можуть завдати шкоди державній та цивільній інфраструктурі і включають злам комп'ютерних мереж, крадіжку даних і руйнування критично важливої інфраструктури. Тому кібератаки можна вважати актами війни. Існує кілька типів кібератак, представлені на рис. 1.6.:



Рис. 1.6. – Види кібератак

Кібершпигунство використовується для викрадення даних і передачі їх іноземним державам. Найбільш поширеними інструментами для досягнення цієї мети є використання ботів та фішингові атаки.

Фішингові атаки - це спосіб отримати інформацію, скориставшись необережністю або довірою користувача. Зловмисники видають себе за надійні джерела інформації та отримують легкий доступ до конфіденційних даних.

Найчастіше використовуються такі методи:

- фішинг електронної пошти;
- фішинг за допомогою шкідливого програмного забезпечення;
- цільовий фішинг;
- атаки спрямовані на конкретних осіб;
- SMS-фішинг;
- атаки на основі SMS-повідомлень;
- вішинг - телефонні атаки.

Ще однією сферою нових загроз для кіберпростору є так звані саботажні атаки. Це цілеспрямовані атаки, метою яких є знищення або витік інформації. Ненадійні паролі, слабкі системи та програмне забезпечення ускладнюють роботу кіберзлочинців.

Пропагандистські атаки зосереджені на спробах контролювати свідомість людей, які живуть у певному регіоні або відвідують його. Такі атаки можуть бути використані для поширення оманливої інформації, щоб підірвати довіру до власної країни і спонукати людей підтримувати ворога.

Економічні підриви включають атаки на такі установи, як фондові біржі, платіжні системи та банки, де основною метою є крадіжка грошей або перешкоджання доступу людей до необхідних їм коштів.

DDoS-атаки - один з найпоширеніших методів кібератак, який порушує роботу веб-сайтів і серверів, перешкоджаючи використанню мережевих сервісів. Мета кіберзлочинця - виснажити програмні ресурси, використовуючи

підроблений трафік, і спричинити погіршення роботи веб-сайту або його повне закриття. DDoS-атаки впливають на широкий спектр компаній у різних галузях, але компанії в ігровій, електронній комерції та телекомунікаційній галузях піддаються більшому ризику.

Найвідоміші форми шкідливих програмних забезпечень представлені на Рис. 1.7:

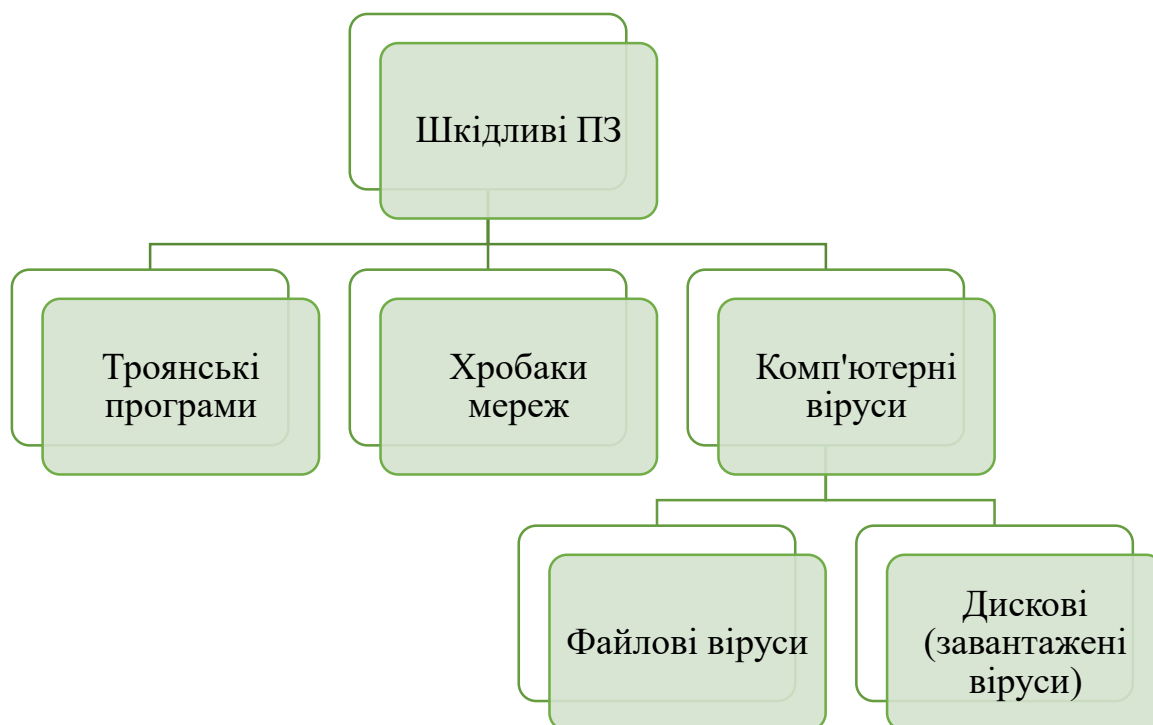


Рис 1.7. – Форми шкідливих програмних забезпечень

Програми, які таємно завантажуються разом з основним програмним забезпеченням, відомі як трояни. Вони часто використовуються для шпигунства.

Комп'ютерні черв'яки - це тип програмного забезпечення, яке намагається проникнути на віддалені комп'ютери. Вони поширюються, приєднуючись до електронних файлів і документів.

Комп'ютерні віруси - це програми, які можуть таємно розмножуватися. Віруси можуть одночасно переписувати свій код, спричиняючи часткове або повне пошкодження операційних систем, а іноді й комп'ютерів.

Приклади операцій кібервійни:

Вірус Stuxnet став відомим як черв'як, що заразив енергетичну та ядерну програму Ірану в 2010 році. Це один з найскладніших випадків в історії кібератак. Експерти характеризують Stuxnet як неймовірно складний фрагмент коду і першу в світі кіберзброю. Stuxnet пошкодив майже 1000 центрифуг в Ірані, заставляючи їх працювати на максимальній швидкості.

Stuxnet використовував одну з найбільших проблем безпеки в програмному забезпеченні - нульова вразливість, що надзвичайно ускладнювало його виявлення. Зменшуючи ймовірність виявлення шляхом надсилення хибних сигналів, він також завантажив руткіт, який дозволив йому взяти під контроль систему на найглибшому рівні.

Атака на Sony Pictures була пов'язана з розповсюдженням фільму «Інтерв'ю» про спробу вбивства Кім Чен Ина. ФБР звинувачує в цьому урядових хакерів з Північної Кореї. Також виявлено схожість з попередніми атаками північнокорейського шкідливого програмного забезпечення, включаючи код, механізми видалення даних і алгоритми шифрування.

Кібервійна в першу чергу використовується для того, щоб порушити, вивести з ладу або перешкодити використанню військових і урядових мереж. Західні країни покладаються на кіберпростір на щоденній основі майже в усіх аспектах життя сучасного суспільства, а країни, що розвиваються, з кожним роком стають все більш залежними від кіберпростору.

Все, що необхідно сучасному суспільству для функціонування, від критично важливої інфраструктури та фінансових установ до методів торгівлі та інструментів національної безпеки, певною мірою залежить від кіберпростору. Тому загроза кібервійни і її передбачувані наслідки викликають велике

занепокоєння урядів і військових в усьому світі. Хоча це не обов'язково відповідає точному визначенню кібервійни, кілька серйозних кібератак, що відбулися, свідчать про те, чого можна очікувати від справжньої кібервійни в майбутньому.

Гібридна війна, з іншого боку, складається з традиційних і нетрадиційних методів ведення війни, в яких інформаційні технології використовуються як важливий інструмент впливу на противника.

До технологій інформаційних війн відносять кіберзброю, соціальні мережі та аналіз великих даних.



Рис 1.8. – Технології інформаційних війн

Кіберзброя: розробка і використання шкідливого програмного забезпечення для знищення, пошкодження або викрадення інформації.

Соціальні медіа: використання платформ для маніпулювання громадською думкою, поширення фейкових новин, організації протестів і створення політичних криз.

Аналіз великих даних: використання технологій для збору та аналізу великих обсягів даних з метою створення прогнозів і стратегій впливу на інші держави та суспільства.

Отже, інформаційна війна стає важливим аспектом сучасного конфлікту, в якому технології відіграють ключову роль у досягненні стратегічних цілей.

Розвиток кіберзброї та методів маніпуляції призводить до появи нових загроз національній безпеці та стабільності.

У цьому контексті важливим є розробка міжнародних стандартів та заходів з протидії кіберзагрозам та інформаційним операціям.

Для ефективної протидії інформаційній війні необхідно вдосконалювати освітню та нормативно-правову базу у сфері інформаційних технологій та телекомунікацій. Тому дослідження типів і технологій інформаційних війн сприятиме з'ясуванню їхніх механізмів, підвищенню готовності до таких загроз та визначенню інноваційних стратегій захисту інформації. Особливо в умовах геополітичної напруженості та постійної конкуренції на світовій інформаційній арені вивчення різних методів інформаційного впливу є вкрай важливим для ефективного реагування на новітні виклики.

Висновок до розділу 1:

В інформаційну епоху термін «інформаційна війна» набув багатозначності та широкого спектру інтерпретацій. З одного боку, це явище можна трактувати як сукупність дій, спрямованих на маніпулювання суспільною свідомістю з метою отримання політичної, економічної чи військової переваги. З іншого боку, інформаційна війна охоплює також технологічно складні операції в цифровій сфері, такі як кібератаки та дезінформаційні кампанії. Дослідження вітчизняних

і зарубіжних науковців показують, що інформаційна війна може бути як платформою для збройного конфлікту, так і самостійним інструментом впливу на суспільну свідомість. Наприклад, такі дослідники, як В. Лизанчук, Г. Почепцов та А. Студнік акцентують увагу на складності цього явища, його методах та інструментах.

Розвиток інформаційних технологій значно розширив засоби інформаційної війни. Від простих пропагандистських інструментів до складних кібератак - кожен вид війни має свої особливості. Кібервійна, психологічна війна та гібридна війна вже є важливими елементами сучасних конфліктів, які не обов'язково пов'язані з фізичними атаками. Особливої уваги заслуговують виклики, пов'язані з інформаційною та кібернетичною безпекою.

Інформаційна війна може становити серйозні загрози національній безпеці, включаючи дестабілізацію політичних процесів, маніпулювання громадською думкою, руйнування соціальної довіри та інші негативні наслідки. Тому сучасна інформаційна війна є складним і багатогранним явищем, яке потребує комплексного підходу до дослідження, розуміння та протидії. В умовах глобалізації розробка ефективних механізмів захисту інформації, підвищення медіаграмотності та стійкості суспільства до інформаційних маніпуляцій і деструктивних впливів є одним з найважливіших викликів сьогодення.

РОЗДІЛ 2. ПЕРЕДУМОВИ ТА СУЧАСНИЙ СТАН РОЗВИТКУ ІНФОРМАЦІЙНОЇ ВІЙНИ В УКРАЇНІ

2.1. Передумови розвитку інформаційних війн

Інформаційна війна — це сучасний феномен, який став важливим елементом глобальних політичних, економічних та військових конфліктів. Її розвиток відображає еволюцію інформаційних технологій, зміни у соціальних структурах та підвищення значення інформації як стратегічного ресурсу. Інформаційна війна включає в себе використання різноманітних засобів для маніпулювання інформацією з метою впливу на громадську думку, дезінформації, пропаганди та досягнення певних політичних або військових цілей.

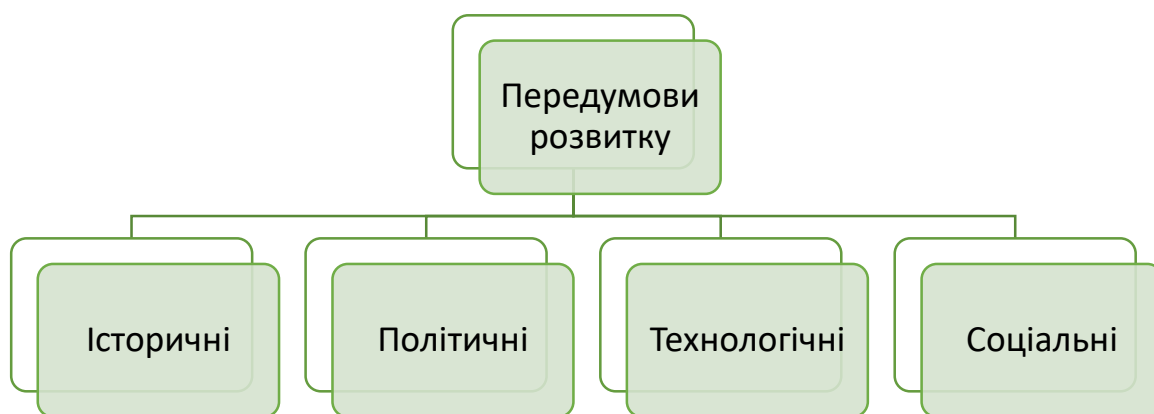


Рис 2.1. – Історичні передумови розвитку інформаційних війн

Інформаційні війни почали формуватися задовго до появи сучасних технологій. Іще в стародавньому світі поширення чуток, маніпуляція масами та використання символів були дієвими інструментами в боротьбі за владу та вплив. Наприклад, римські політики та військові стратеги використовували інформацію як спосіб деморалізації противника: розповсюдження чуток серед населення ворога про неминуче вторгнення часто призводило до здачі міст без бою. У середні віки церква володіла монополією на освіту і доступ до інформації, використовуючи проповіді та церковну іконографію для контролю суспільства та формування його світогляду.

Сучасний формат інформаційної боротьби почав формуватися у ХХ столітті разом із розвитком масових комунікацій. Наприклад, під час Другої світової війни радіо і плакати стали ключовими засобами мобілізації населення, посилення національної єдності та формування образу ворога.

У книзі «Информационные войны и психотронное оружие» В. П. Шейнов описує, як пропаганда того часу стала прототипом сучасних інформаційних кампаній. Він зазначає, що доступ до медіаресурсів був стратегічною перевагою, яка значно впливала на хід війни.

Політичні передумови відіграють одну з центральних ролей у розвитку інформаційних війн. Глобалізація, що розпочалася в другій половині ХХ століття, посилила конкуренцію між державами за домінування не лише у військовій, а й у інформаційній сфері. Кожна держава прагне контролювати інформаційний простір як усередині країни, так і за її межами, розуміючи, що вплив на громадську думку часто виявляється ефективнішим за військову агресію.

Особливу увагу заслуговує перехід до гібридних конфліктів, у яких інформація стає ключовою зброєю. У книзі Джозефа Ная «Soft Power: The Means to Success in World Politics» описується, як «м'яка сила» інформації замінює традиційні методи тиску. Держава може просувати свої інтереси через

культурний вплив, створення позитивного образу в медіа та маніпуляцію глобальною інформацією. Прикладом такого є «холодна війна», яка мала великий вплив на розвиток інформаційної війни. Радянський Союз і США використовували пропаганду для створення ідеологічних конфліктів.

Такі радіостанції, як «Голос Америки» та «Радіо Свобода», поширювали інформацію в країнах соціалістичного табору, тоді як СРСР використовував цензуру та контроль над ЗМІ для підтримки ідеологічної єдності. Крім того, розвиток інформаційної війни тісно пов'язаний з появою недержавних акторів.

Терористичні організації, як «Аль-Каїда» та «Ісламська держава», широко використовують Інтернет для пропаганди, вербування та координації, демонструючи, як інформація може стати інструментом в руках невеликих груп.

Технологічні передумови, вчасності, прогрес є найважливішим фактором, що спричинив вибухове зростання інформаційних війн. Інтернет, що став масовим явищем наприкінці ХХ століття, відкрив нову еру у взаємодії між людьми. Якщо раніше інформація поширювалася через централізовані канали, такі як газети, радіо та телебачення, то тепер кожен користувач може стати не лише споживачем, а й творцем контенту.

Особливу увагу слід приділити ролі соціальних мереж, які стали основним інструментом інформаційних війн. У книзі «The Net Delusion» Євгенія Морозова аналізується, як соціальні платформи, спочатку створені для об'єднання людей, почали використовуватися для маніпуляцій, розповсюдження фейкових новин і створення «інформаційних бульбашок». Алгоритми, які рекомендують контент, налаштовані так, щоб утримувати увагу користувача, часто просуваючи емоційно забарвлену, але неправдиву інформацію.

Крім того, важливим фактором стало використання штучного інтелекту та автоматизованих систем. Алгоритми аналізу даних здатні створювати профілі користувачів, визначати їхні слабкі місця та пропонувати інформацію, що впливатиме на їхні рішення. Deepfake-технології дозволяють створювати

фальшиві відео та аудіо, що виглядають максимально реалістично, що посилює ризики маніпуляцій.

Сьогодні швидкість передачі інформації досягає безпрецедентного рівня: За даними Statista, до 2023 року понад 5 мільярдів людей мають доступ до інтернету, що створює безпрецедентні можливості для маніпуляцій. Крім того, що ШІ використовується для створення фейкових новин, він також відіграє важливу роль у таргетингу. Скандал з Cambridge Analytica, наприклад, показав, як персоналізована реклама в соціальних мережах може впливати на вибори. Нові технології також впливають на створення «інформаційних полюсів». Інтернет-боти генерують сотні повідомлень, щоб створити ілюзію масової підтримки певної позиції. Це сприяє ефекту групової поляризації, коли користувачі соціальних мереж схильні вірити інформації, яка підтверджує їхні існуючі переконання.

До соціальних передумов відносять зростання ролі інформації в сучасному суспільстві, яка зумовила появу інформаційних воєн. У ХХІ столітті інформація стала одним із найцінніших ресурсів, який прирівнюється до енергетичних чи природних ресурсів. Усі сфери життя, від освіти до політики, залежать від доступу до інформації, її якості та достовірності.

У книзі С. В. Бондаренка «Информационная безопасность в условиях глобализации» підкреслюється, що сучасне суспільство переживає інформаційне перевантаження. Люди отримують занадто багато даних, що часто ускладнює критичний аналіз і сприяє поширенню фейків. В умовах такого перенасичення легко сформувати громадську думку через маніпулятивні заголовки чи емоційно насичені повідомлення.

Сучасне суспільство робить акцент на швидкості обміну інформацією, але це часто відбувається за рахунок якості інформації. Згідно з опитуванням Pew Research Centre, 64% американських користувачів вважають соціальні мережі основним джерелом новин, але лише 30% довіряють інформації, яку вони

отримують. Це створює умови для поширення дезінформації та теорій змови. Іншою важливою проблемою є цифровий розрив між країнами. У той час як розвинені країни мають доступ до передових технологій і високошвидкісного інтернету, менш розвинені регіони залишаються вразливими до інформаційних маніпуляцій через брак альтернативних джерел інформації.

Отже інформаційна війна — це ключовий елемент сучасних політичних, економічних та військових конфліктів, що розвивається завдяки технологічному прогресу та соціальним змінам. Її історичні корені сягають стародавнього світу, але особливої актуальності вона набула у XX–XXI століттях завдяки появі Інтернету, соціальних мереж і штучного інтелекту.

Сучасні інформаційні війни використовують пропаганду, дезінформацію, маніпуляцію даними та громадською думкою, впливаючи як на держави, так і на окремих людей. Інтернет, соціальні мережі та алгоритми створюють нові ризики: поширення фейків, інформаційні «бульбашки» та підрив суспільної довіри.

Важливість інформації як ресурсу посилює її значення в глобалізованому світі, але також відкриває простір для маніпуляцій і викликів. Захист інформаційного простору стає критичною складовою національної безпеки.

2.2. Роль соціальних мереж у державній політиці та обмеженні дезінформації

Соціальні мережі - це соціальні структури, створені людьми та організаціями. Вони відображають різноманітні зв'язки між окремими особами або організаціями через низку соціальних відносин, від випадкових знайомств до близьких родичів. Найвідомішими соціальними мережами у світі є Facebook, Youtube, Tiktok, Instagram, Telegram, Watsapp, Viber, X, Pinterest.



Рис 2.2. – Кількість активних користувачів в соц. мережах в млн

Президентська виборча кампанія Обама 2008 року вважається першою політичною соціальною мережею. Вона вважається першою політичною кампанією, яка активно використовувала соціальні мережі як інструмент впливу. Кампанія Обама трансформувала онлайн-активізм у реальну участь у формі фінансування та голосування. Розглядаючи політичну кампанію нинішнього президента України Володимира Зеленського, стає зрозуміло, що соціальні медіа були важливим каналом комунікації під час виборчої кампанії. Під час

президентських виборів команда опонента Зеленського, президента Порошенка, не дуже активно використовувала Instagram, але для команди Зеленського надсилання відео-звернень до цільової аудиторії через цю соціальну мережу було важливим елементом передвиборчої кампанії.

Оскільки громадськість все частіше отримує доступ до інформації про передвиборчу кампанію через соціальні мережі кандидатів, соціальні мережі мають великий потенціал для збільшення, підтримки і навіть мотивації участі в політичному процесі. Дослідження показують, що явка виборців онлайн може передбачити участь у політичних кампаніях офлайн.

Наразі традиційні медіа (паперові, офлайн) можуть мати однакову вагу при переході до онлайн-форматів порівняно з існуючими медіапросторами для молодого покоління. Розуміння того, як нове покоління взаємодіє з політикою, може допомогти кампаніям покращити свої меседжі та залучити нових виборців. Соціальні медіа можуть бути корисним інструментом для зв'язку між кандидатами та інформацією, оскільки вони дозволяють користувачам відчувати політику на більш інтимному міжособистісному рівні.

Аналізуючи участь молодого покоління в політиці, стає зрозуміло, що вона відрізняється від участі попередніх поколінь, яким доводилося відвідувати збори, декларувати партійну приналежність і голосувати в день виборів. Хоча молоде покоління менш схильне до участі у традиційних формах, існує кілька гіпотез, які мають на меті зрозуміти, як політичні повідомлення споживаються в соціальних мережах і як це споживання трансформується в участь у порівнянні з більш традиційними методами.

З іншого боку, в нинішніх політичних умовах важливо розуміти вплив соціальних медіа на політичну комунікацію. Політологи закликають до обережності у використанні соціальних медіа як деструктивного інструменту і заохочують їх використання як ресурсу для більшого залучення виборців, поширення інформації тощо.

Переваги соціальних мереж у політичних кампаніях включають, серед іншого, кліки, використання, залучення, вподобання та поширення, які можуть генерувати цікаві дані про Аналіз даних може допомогти кампаніям писати повідомлення в соціальних мережах, щоб ефективно таргетувати та відстежувати користувачів. Відповіді на пости про кандидатів у соціальних мережах можна використовувати як поведінкові індикатори. Особливо у Твіттері можна визначити ставлення користувачів до певних дописів та зібрати статистику охоплення аудиторії.

Важливо звернути увагу на те, як пости кандидатів-чоловіків і кандидаток, які публікують інформацію про своє приватне життя в соціальних мережах, впливають на наміри виборців. Спостереження за допомогою Facebook і Twitter показують, що обмін особистою інформацією між кандидатами-жінками часто викликає питання щодо їхньої придатності та компетентності, тоді як кандидати-чоловіки виглядають більш привабливими для виборців. Однак це не єдине упередження щодо кандидатів у реальному житті та в соціальних мережах.

Використання соціальних медіа в політиці - це використання онлайн-платформ соціальних медіа в політичних процесах та діяльності. Політичні процеси та діяльність включають усі види діяльності, пов'язані з національним та регіональним управлінням. Сюди входять політичні організації, глобальна політика, політична корупція, політичні партії та політичні цінності. Інтернет створив канали комунікації, які відіграють важливу роль у поширенні новин, а соціальні медіа здатні змінювати не лише повідомлення, а й динаміку політичних рухів, цінності та напрямки політичного конфлікту.

Наразі державні установи активно використовують соціальні медіа для комунікації з громадськістю, підвищення прозорості та надання своєчасної інформації. Зокрема, Верховна Рада України збільшує свою присутність у соціальних мережах і прагне перетворити свою офіційну сторінку на платформу для обміну інформацією та думками між громадянами та вищим законодавчим

органом. Крім цього медіа використовують щоб залучити громадян для обговорень суспільно важливих питань та сприяють підвищенню довіри до державних інституцій через відкритість та прозорість.

З позитивного боку, використання соціальних мереж органами влади несе в собі певні ризики. Зокрема, існує ризик поширення дезінформації, маніпуляцій та радикалізації суспільства через неконтрольований контент. Тому важливо враховувати потенційні загрози та розробляти стратегії ефективного використання соціальних мереж.

Дезінформація в соціальних мережах може мати серйозні наслідки, особливо в кризових ситуаціях. Наприклад, під час пандемії COVID-19 поширювалася дезінформація про методи лікування та профілактики, що призвело до небезпечних медичних практик. Крім того, дезінформація може впливати на політичний процес, підривати довіру до демократичних інститутів і сприяти соціальній радикалізації.

Уряди визнають необхідність боротьби з дезінформацією в соціальних мережах. Зокрема, в Україні розробляється законодавство, покликане зменшити ризик маніпулювання інформацією в соціальних мережах, підвищити прозорість власності та обмежити анонімність.



Рис 2.3. – Актуальність проблеми дезінформації у %

Ефективна протидія дезінформації вимагає співпраці між державою та соціальними медіа-платформами. Це включає розробку спільних стратегій виявлення та видалення фейкових новин, а також впровадження алгоритмів запобігання поширенню дезінформації.

До прикладу USAID-Internews опублікував результати опитування щодо споживання медіа. Більше третини респондентів, які знають про дезінформацію, вважають її нагальною проблемою, 84% опитаних респондентів знають про існування дезінформації, а 72% вважають, що можуть розпізнати дезінформацію. Лише 38% респондентів, які знають про існування дезінформації, вважають дезінформацію нагальною проблемою в Україні. 57% респондентів вважають, що дезінформація не є нагальною проблемою, а 4% респондентів сказали, що не можуть нічого сказати з цього приводу.



Рис 2.4. – Вміння відрізняти дезінформацію на думку людей у %

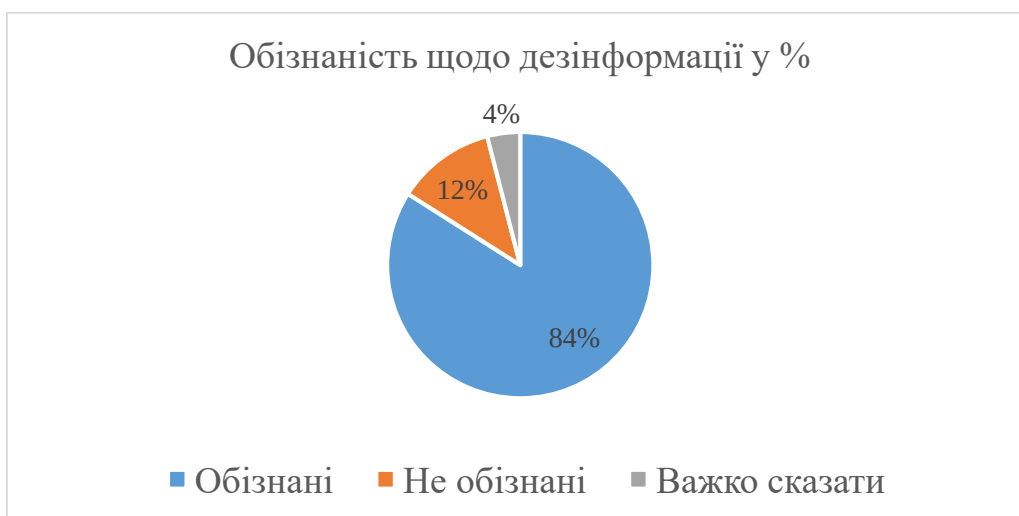


Рис 2.5. – Обізнаність щодо дезінформації у %

Отже, соціальні мережі залишаються важливим інструментом поширення інформації, але вони також є джерелом дезінформації, яка може суттєво впливати на громадську думку. Згідно з опитуванням, лише 38% українців вважають дезінформацію нагальною проблемою. Це свідчить про недостатнє усвідомлення масштабів дезінформації та її впливу на суспільство і створює нові виклики для державної політики.

2.3. Особливості ведення інформаційної війни в Україні на прикладі російсько-української війни

Інформаційна війна Росії проти України розпочалася із здобуттям Україною незалежності у серпні 1991 року. Сучасні експерти зазначають, що Росія веде систематичну інформаційно-пропагандистську кампанію з моменту здобуття Україною незалежності [20, с. 137].

Серед конфліктів між Україною та Росією, в яких елементи інформаційного впливу були помітними, можна назвати територіальну суперечку навколо острова Тузла у 2003 році, «газові» війни у 2005 та 2009 роках та інші подібні інциденти [21, с. 151]. Інформаційна війна посилилася під час перебування на посаді президента Віктора Януковича.

Наприкінці 2013 року російські ЗМІ розпочали масовану інформаційну кампанію проти Майдану, яка згодом переросла у збройний напад. З окупацією Криму Росія розпочала агресивну інформаційну війну проти України. На інформаційну війну проти України Росія витрачала до 4 мільярдів доларів США на рік [22]. Реалізація агресивних планів Росії проти України у 2014 році включала ескалацію конфлікту в інформаційній сфері. Інформаційна війна була спрямована не лише на сприяння анексії української території, а й на легітимізацію цього процесу. Основна стратегія інформаційної війни та психологічних операцій була спрямована проти громадянської ідентичності України та відмови українців захищати свою країну. Головною метою було прищепити громадянам України, Росії та європейських країн переконання, що створення та відновлення української держави було штучним процесом. Поширювалися твердження про правління «неонацистського уряду», який нібито отримав державну владу в результаті державного перевороту, і про те, що поступовий розвиток українського суспільства можливий лише за умови тісної співпраці або об'єднання з Російською Федерацією [23, с. 141].

Через ЗМІ Росія використовувала і повторювала різні соціальні технології, спрямовані проти України. Серед них - поділ країни на «народні республіки», створення кримінальних угруповань, сприяння заворушенням і захопленню влади в містах, організація «референдумів», використання «живих щитів» та інші методи. На думку дослідників, усі ці технології мають певні спільні риси, такі як спільні цілі, використання стандартних методів, синхронізація дій у різних містах України, схожість зовнішніх ознак, символіки, ідеологічного та пропагандистського інформаційного супроводу тощо [24; с. 55].

Починаючи з 2014 року, російські ЗМІ використовували різні методи для пояснення російського вторгнення в Україну, часто вдаючись до перекручування фактів і відвертої дезінформації. Журналісти змінювали реальні події та подавали неправдиві інтерпретації. Російські журналісти намагалися запевнити глядачів, що в Україні панує «хаос і безлад» і що російські війська допомагають стабілізувати ситуацію і захистити російськомовне населення від «коричневої чуми», яку сам президент Путін описав як загрозу [25].

Російські телеканали використовували кадри зіткнень на Євромайдані для ілюстрації ситуації в Сімферополі, транслюючи дезінформацію про те, що українські солдати переходять на бік Росії, і повідомлення про довгі черги українських біженців біля російського кордону. Це було проілюстровано фотографіями пункту пропуску «Шегині», який є пунктом перетину кордону з Польщі в Україну [25]. Ще на початковому етапі російської агресії в 2014 році, під час організації операції із захоплення Криму, експерти Національного інституту стратегічних досліджень відзначали, що російські військові операції супроводжувалися агресивною інформаційно-психологічною кампанією. Ця кампанія була спрямована, з одного боку, на російські маси, а з іншого - на українські та частково західні [26, с. 5-11]. Головною метою цієї спеціальної інформаційної операції була деморалізація української армії, силових структур і суспільства та підбурювання їх до зради. Крім того, велика увага приділялася

створенню хибного «медійного бачення» військових подій серед російських та українських громадян, штучному створенню враження всенародної підтримки дій Росії серед населення півдня та сходу України, фабрикуванню наративів тощо. Для досягнення цих цілей використовувалися різні канали комунікації, включаючи традиційні та електронні ЗМІ, Інтернет і соціальні мережі [27, с. 85].

У 2014-2022 роках пропагандистська машина Кремля активно готувала ґрунт для вторгнення в Україну, розробляла інструменти для легітимізації своїх дій на міжнародному рівні та створювала механізми блокування для своїх громадян інформації із західного світу. Всі ці заходи були частиною інформаційної війни, яка сприяла формуванню у російських громадян і військових поглядів на так звані «спецоперації» та «демілітаризацію і демілітаризацію» в Україні [28, с. 138].

Сьогодні Росія захопила Крим та частини південних і східних областей України і відкрито веде війну проти України. З моменту російського вторгнення 24 лютого 2022 року ворожа пропаганда стала більш активною та агресивною. Найбільші телеканали продовжують широко використовувати фейкові новини та пропагандистські матеріали для виправдання своєї агресії.

Перш за все, Росія розпочала широкомасштабну війну проти України для реалізації своєї ідеології возз'єднання колишнього Радянського Союзу та геополітичного переділу Євразії під керівництвом Москви. Це бачення було особливо підкреслено під час президентства Путіна, коли реформування системи міжнародних відносин і перетворення Росії на наддержаву стало головною метою Кремля. Україна посідає важливе місце в геополітичному плануванні Росії, оскільки вона є місцем зустрічі демократичних та авторитарних цінностей. Після перемоги Революції Гідності та вибору Україною прозахідного шляху розвитку Росія не могла з цим змиритися. Водночас, незважаючи на свою пропагандистську потужність, Росія уникає прямої конфронтації із Заходом,

особливо з НАТО, через величезний розрив між її економічним і військовим потенціалом. Саме тому Росія віддає перевагу гібридній моделі війни [29, с. 194]:

Дезінформація про масове вторгнення Росії в Україну в лютому 2022 року була ескалацією попередніх розвідувальних операцій Росії проти України та західних демократій. З посиленням обмежень на політичну опозицію в Росії дезінформаційний дискурс відійшов від пропаганди та історичного ревізйонізму. Прикладами цього є заяви про те, що Крим, який Москва анексувала в 2014 році, «завжди був російською територією», неправдиві твердження про проникнення неонацистів в український уряд або теорії змови щодо лабораторій з виробництва біологічної зброї в Україні та США. Це лише деякі з способів, за допомогою яких російський уряд та його поплічники використовують дезінформацію як зброю, щоб відволікти, заплутати і послабити своїх опонентів [30, с. 74].

Росія легітимізує свої дії, використовуючи типову для тоталітарних держав стратегію створення внутрішніх і зовнішніх ворогів. Зовнішнім ворогом є весь західний світ, а внутрішнім - опозиція. Створення образу ворога слугує прикриттям агресивної політики Росії та використовується для «мобілізації» населення проти зовнішніх загроз, створення відчуття незахищеності та відволікання уваги від внутрішніх кризових питань [21, с. 102].

Ностальгія за колишнім Радянським Союзом виявилася потужним пропагандистським інструментом, і ці настрої були важливою частиною інформаційної стратегії Росії, спрямованої на захоплення Криму та розв'язання війни на сході України в 2014 році. Це робилося переважно за допомогою фільмів і серіалів, які поглиблювали наратив «великої перемоги» над нацистами і пробуджували тугу за радянським минулим, соціальною захищеністю і стабільністю.[31] День Перемоги 9 травня залишається потужним пропагандистським інструментом, особливо на внутрішньому ринку, а також є важливою частиною російської пропагандистської стратегії щодо війни. У новому наративі Путін називає свої «спеціальні військові операції»

продовженням Великої Вітчизняної війни і стверджує, що Росія все ще бореться з нацистами. [32].

Російська інформаційна політика є віртуальною, а пропагандистські меседжі не завжди мають реальне підґрунтя (наприклад, «Новоросія» ніколи не існувала в реальності). Суспільна свідомість часто не розрізняла реальне і віртуальне, що призводило до того, що росіяни вірили у створену картину світу, яку проектували російські телеканали. Частина громадян України також «побачила» свою майбутню реальність у штучно створеному проекті «Новоросія». Однак виявилось, що ці «республіки» не мали життєздатної моделі розвитку, оскільки їхнє існування ґрунтувалося на пропаганді інформаційної війни. Республіки не мали реального підґрунтя і лише сприяли нестабільності та соціальній напруженості в Україні [3, с. 89].

Інформаційна війна Росії проти України спрямована на зміну сприйняття та розуміння світу в суспільстві - це смислова війна з людьми [21, с. 243]. Вона спрямована на переписування історії не лише шляхом маніпулювання фактами та інформацією, а й шляхом створення альтернативних наративів та викривлення подій. Головною метою є вплив на свідомість громадян для формування певних уявлень і переконань на користь російських інтересів.

За словами російських ЗМІ та офіційних осіб, анексія Криму описується як «повернення до єдності» та «відновлення історичної справедливості», війна на сході України - як «громадянська війна», а повна окупація України - як «деескалація». Натомість міжнародна спільнота звинувачує Україну у введенні «гуманітарної та фінансової блокади Донбасу» та «репресіях проти російськомовного населення», порушенні Мінських домовленостей та збитті літака МН-17 [33, с.11].

У серпні 2020 року Державний департамент США звинуватив Росію у створенні системи пропаганди та дезінформації та опублікував доповідь, в якій виділив п'ять основних елементів цієї системи. На думку американських

експертів, ці стовпи включають офіційні урядові комунікації, фінансовані державою глобальні інформаційні служби, проксі-джерела (ЗМІ інших країн у партнерстві з РФ, «експерти», які поширюють російську риторику за кордоном), соціальні мережі та кібердезінформацію [34, с. 3-4].

Ще одним випробуваним аспектом російської пропаганди є інформаційна війна у сфері освіти. Зусилля щодо впливу на молоде покоління вписуються в загальний контекст інформаційного наступу на Україну. Наприклад, у минулому були спроби просування українських підручників з історії, написаних у співпраці з російськими «науковцями». Ці спроби були зірвані через опір експертів, численних українських істориків та викладачів [25].

Російські ЗМІ, як традиційні, так і онлайн, продовжують поширювати міфи про так званих «неонацистів» (або «нацистів») в Україні, які, за їхніми словами, утискають російськомовне населення України [36, с. 47-51; 35, с. 62].

З іншого боку, ворожі ЗМІ безсоромно відмовляються використовувати термін «війна». Слід зазначити, що використання цього терміну в Росії може призвести до позбавлення волі на строк до 15 років. З цієї причини напади на суверенну державу в Росії часто називають терміном «спецоперації». Коли ж ворожі сили намагаються вторгнутися в іншу країну, бомбардувати її міста і спричиняти загибель цивільних осіб, зокрема жінок і дітей, зрозуміло, що це війна і навіть тероризм. Такі термінологічні зсуви покликані приховати реальні плани і дії російської влади і є спробою відволікти прихильників консервативних поглядів від справжньої суті подій. Використання таких термінологічних зсувів має практичне значення для впливу на свідомість сучасних росіян [37, с. 86].

У цьому списку представлені деякі з найпоширеніших міфів та дезінформації на сайтах, відомих публікаціями неправдивої проросійської пропаганди та дезінформації: Україна готує наступ на Донбас згідно з секретними документами; масове вбивство цивільних осіб було влаштовано в Бучі в перший місяць війни; США розробляють біологічну зброю, спрямовану

проти етнічних росіян, і мають мережу біолабораторій у Східній Європі; Росія не націлена на цивільну інфраструктуру України; університети ЄС виганяють російських студентів; Росія використовує касетні боєприпаси під час «військових операцій» в Україні; Україна не готує дітей-солдатів; Україна готує дітей-солдатів; сучасна Україна була повністю створена комуністичною Росією; Крим приєднався до Росії на законних підставах; США і Великобританія надіслали в Україну застарілу і непридатну зброю; антиросійські сили скинули проросійський український уряд у 2014 році; нацизм, підтримуваний українським урядом, процвітає в українській політиці і суспільстві; російськомовне населення Донбасу піддається геноциду [30, с. 75-76].

Російська інформаційна війна також включає спроби дискредитувати українських військових і політичних лідерів, зображуючи їх як «зрадників» [39]. Одним із найяскравіших прикладів є міф про те, що президент Зеленський є «втікачем». Крім того, російські інформаційні кампанії систематично підкреслюють негативне ставлення українців (особливо західноукраїнських «нацистів») до росіян [39, с. 98-99]. Широко поширений міф про «хлопчика, розіп'ятого українськими нацистами».

Водночас російські офіційні особи представляють окупацію України російськими військами як неминучу і стверджують, що «якби не Путін, війська НАТО прийшли б в Україну». Ще один міф, який поширює російська влада, стосується обстрілів міст, які, за їхніми словами, здійснює виключно українська армія. Наприклад, «Крим.Реалії» повідомляють, що 85% руйнувань у Маріуполі було завдано силами «Азова». Зрозуміло, що російські війська не змогли швидко окупувати місто Маріуполь і вдалися до тотального руйнування [37, с. 86].

Такі аргументи не мають логічного пояснення і існують лише для внутрішнього споживання. Міжнародні організації, оснащені сучасними технічними засобами, можуть легко відстежити, в якому напрямку були випущені бомби і ракети. Варто зазначити, що лише за перший тиждень війни

було зібрано тисячі реальних доказів військових злочинів Росії. Такі заяви, швидше за все, робляться для того, щоб мобілізувати внутрішню підтримку. Очевидно, що нинішня російська «еліта» готова частково розірвати свої зв'язки із Заходом, тому для стабільності путінського режиму важливо мати повний контроль над настроями власного народу. У цій війні між Росією та Україною ЗМІ часто ставлять за мету не надання об'єктивної інформації, а збір фактів, які підтверджують певну точку зору.

До характеристик інформаційної війни можна віднести: створення реальності за допомогою інформації, тобто інформація стає засобом формування певної реальності, і чим інтенсивніше вона поширюється, тим більше шансів на успіх; трансформація цінностей, в тому числі відхилення від радянської традиції, що проявилось, наприклад, у відмові від святкування 23 лютого; спільна історична боротьба: Спільна історія України та Росії стає полем боротьби, включаючи нападки на національні символи та військову славу [3, с. 89].

Усі ці елементи показують, як інформаційна війна використовується для впливу на суспільні настрої та переконання, формування образів та зміни цінностей. Агресивна війна Росії проти України характеризується своєю інтенсивністю в Інтернеті. Обсяг доступної інформації та її поширення через Інтернет і соціальні мережі відіграли важливу роль у цій війні.

Соціальні медіа відігравали певну роль і в попередніх війнах, але їхній вплив у конфлікті на Донбасі 2014 року був ще більшим завдяки розширенню інтернет-покриття та масовому використанню соціальних медіа. Рівень проникнення інтернету в Україні є високим: 75% населення користуються інтернетом, а 89% охоплені принаймні мобільним зв'язком 3G [30, с. 74]. Це створює значні можливості для поширення інформації, пропаганди та інструментів маніпулювання громадською думкою.

Важливою складовою інформаційного фронту є намагання контролювати інтернет-простір і поширювати дезінформацію через онлайн-ресурси. Це

підкреслює, наскільки важливим у сучасних конфліктах став Інтернет як інструмент формування світогляду та впливу на громадську думку.

Основні наративи, що репрезентують Росію та Україну, суттєво відрізняються, і це можна простежити в таких ключових аспектах: історія та суверенітет, людський вимір, геополітичний контекст.

Відмінності між російськими і українськими наративами щодо історії та суверенітету, людського виміру та геополітичного контексту охарактеризовано в таблиці 2.1

Таблиця 2.1.- Відмінності між російськими і українськими наративами

Історія та суверенітет	
Російський наратив	Український наратив
Росія стверджує, що проводить військові операції як оборонний захід проти розширення НАТО і для захисту російськомовного населення України. Путін використовує термін «денацифікація» для легітимізації вторгнення.	Український наратив наголошує на українському суверенітеті та праві на окрему ідентичність, відмінну від російської. Він інтерпретує війну як акт агресії та невинуватеної агресії і підкреслює героїзм своїх громадян і солдатів у захисті батьківщини
Людський вимір	
Російський наратив	Український наратив
Путін намагається спроектувати образ України як агресора, що чинить геноцид проти російськомовного населення, надаючи легітимності військовій операції проти нього.	Україна відмовляється засуджувати геноцид і намагається привернути увагу до гуманітарних наслідків війни, включаючи страждання цивільного населення та порушення прав людини.

<i>Продовж. Табл 2.1</i>	
Геополітичний контекст	
Російський наратив	Український наратив
Реакція Росії на розширення західного впливу, зокрема розширення НАТО у Східній Європі, як виправдання власних дій.	Україна наголошує на своєму праві обирати власне політичне та геополітичне майбутнє і відкидає агресію та іноземний вплив.

Ці наративи формують сприйняття подій у національному та міжнародному контекстах і впливають на громадську думку та реакцію на глобальній арені.

Росія та Україна активно використовують соціальні мережі для представлення власних інтерпретацій війни, що розгортається, і для посилення суперечливих наративів про причини, наслідки та майбутній розвиток війни. Урядовці, громадські активісти та державні установи використовують різні платформи для поширення інформації, зокрема Facebook, Twitter, TikTok, YouTube і Telegram. Хоча важко визначити точний обсяг контенту, завантаженого цими різними суб'єктами, масштаб інформації, пов'язаної з війною, що поширюється в соціальних мережах, надзвичайно великий [30, с. 75].

Важливо зазначити, що Росія вже давно використовує Україну, разом з іншими колишніми радянськими республіками, як приклад країни, що повільно розвивається. Тому нова комунікаційно-пропагандистська кампанія не була чимось абсолютно новим, а скоріше продовженням давньої теми, яка завжди була присутня в російських ЗМІ. Це значно полегшило завдання налагодження пропагандистської комунікації [40].

Якщо війну розглядати як відкритий збройний конфлікт, то інформаційну війну Росії проти України можна розглядати як потенційний вплив через вербальні «удари», які не відразу сприймаються реципієнтом. Вона систематично

впливає на свідомість людей за допомогою слів, образів, інтерпретацій та контекстів, змінюючи їхні погляди та заплутуючи їх для досягнення певних політичних цілей [41, с. 15].

Таким чином, можна узагальнити основні складові інформаційної війни Росії проти України.

Основними об'єктами інформаційної війни Росії проти України є українське суспільство, внутрішньополітична ситуація в Україні, українська система влади та окремі політичні і громадські організації, такі як політичні партії, громадські рухи, релігійні організації та засоби масової інформації. Головною метою російської інформаційно-психологічної війни є вплив на українське суспільство та його руйнування «зсередини» шляхом дискредитації української влади, української армії, курсу на європейську та атлантичну інтеграцію та провокування соціального конфлікту [42, с. 3]. Головне завдання Кремля - «послабити» Україну зсередини і створити переконання, що Україна та українці нерозривно пов'язані з образом Росії як євразійської держави. Цей наратив є спробою позбавити Україну її важливості та впливу на міжнародній арені.

Основним інструментом російської пропаганди є засоби масової інформації, зокрема централізовані телеканали, такі як «Первый канал», НТВ, «Известия» та «Российская газета», а також інформаційні агентства, такі як «РИА Новости» та «ИТАР-ТАСС». Поєднання телебачення і пропаганди пояснюється тим, що телеглядачами легше керувати, ніж читачами газет і соціальних мереж [43, с. 134]. При цьому телебачення використовує різні методи впливу на суспільну свідомість, такі як створення, повторення та маркування фейкових новин [44].

Окрім України та Росії, інші державні суб'єкти, такі як Китай і Білорусь, також виявляють активний інтерес до воєнної журналістики, просуваючи власні наративи та координуючи дезінформаційні кампанії через соціальні мережі. Ці

кампанії спрямовані на мінімізацію відповідальності Росії за конфлікт і просування антиамериканських і антинатовських позицій. Конвергенція різних наративів різних державних акторів та окремих користувачів соціальних мереж може розширити роль технологічних платформ у формуванні динаміки війни та впливу на її результат [30, с. 75].

Маніпулятивні психоінформаційні технології, що використовуються Росією проти України, включають деякі з основних напрямів і методів, виділених дослідником П. Шевчук: Підрив міжнародного іміджу України та послаблення її геополітичних позицій; управління та викривлення інформації з метою дестабілізації України та реалізації політики «керованого хаосу»; розробка та поширення стереотипів, які пропагують ідею меншовартості та підпорядкованості українців, що призводить до знищення національної гідності та самоідентифікації українців через домінування російської мови, культури і традицій та придушення українського мовного та культурного аспектів [45].

Український дослідник інформаційної безпеки І. Валюшко до основних методів інформаційної агресії проти України відносить дезінформацію, маніпуляції, пропаганду, відволікання громадської думки, психологічний тиск, поширення невпевненості та створення плутанини, а також кібератаки. Інструментарій інформаційної війни Росії включає різні засоби, такі як ЗМІ, інтернет-тролі, боти, текст, відео, аудіо, зображення та меми. Інформаційна війна також може вестися окремими політичними, соціальними і навіть релігійними групами, залежно від їхніх цілей і завдань [46, с. 181]. Інформаційна сфера виявилася найбільш вразливою сферою безпеки в Україні, що пов'язано як з правовими, так і з інституційними проблемами. У той час як розвідувальні та диверсійні елементи є життєво важливими у загальних військових операціях на нашій території, розвідувально-психологічні елементи відіграють важливу роль у розвитку конфлікту між Росією та Україною.

Таким чином, військова агресія Росії проти України активно супроводжується інформаційною війною. Засоби масової інформації є основним джерелом інформації в суспільстві і тому мають найбільш впливовий вплив на формування громадської думки. У сучасному глобалізованому світі ЗМІ стали невід'ємною частиною людського життя і можуть спричиняти відчутні соціальні ефекти, розкриваючи сприйняття реальності [41, с. 13]. Прикладом цього є інформаційна війна Росії проти України, яка паралельно з широкомасштабною агресією призвела до загибелі багатьох людей та руйнування перспективних галузей економіки.

Висновок до розділу 2:

Інформаційні війни виникають внаслідок поєднання технологічного прогресу, політичних амбіцій та вразливості суспільства до маніпуляцій. Цифрові технології та глобалізація інформаційного простору значно розширили можливості впливу на суспільну свідомість, які держави використовують для досягнення своїх геополітичних цілей.

Соціальні мережі, які стали важливим елементом державної політики, також є середовищем для поширення дезінформації, що вимагає узгоджених зусиль для протидії їй. В умовах війни між Росією та Україною інформаційний фронт набув критичного значення. Росія активно проводить пропагандистські та інформаційні операції, а Україна, за підтримки громадянського суспільства та міжнародної спільноти, розробляє власні заходи протидії.

РОЗДІЛ 3. НАСЛІДКИ І ПРОТИДІЯ ВПЛИВУ ІНФОРМАЦІЙНОЇ ВІЙНИ ПРОТИ РОСІЇ

3.1. Наслідки інформаційних війн в Україні

Інформаційна війна проти України є частиною гібридного конфлікту, спрямованого на підрив суспільної довіри, зменшення національної цілісності та послаблення держави на всіх рівнях. Основні наслідки цього впливу можна розділити на політичні, соціальні, безпекові та економічні аспекти.

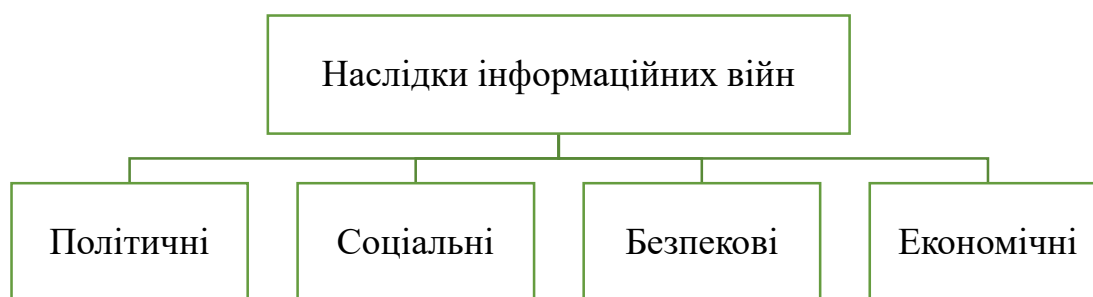


Рис. 3.1. - Наслідки інформаційних війн в Україні

До політичних наслідків, перш-за все, відносять підрив міжнародної підтримки та делегітимізація влади всередині країни.

Російська дезінформація часто використовується для створення негативного іміджу України на міжнародній арені. Зокрема, поширення історій про нібито широкомасштабну корупцію, неефективність уряду та нестабільність в Україні може стримувати іноземні уряди від надання фінансової та військової допомоги.

Делегітимізація влади всередині країни. Масове поширення фейкових новин спрямоване на підриг довіри суспільства до органів державної влади. Це створює кризу довіри та ускладнює проведення реформ, необхідних для демократичного розвитку.

Щодо соціальних наслідків до них відноситься:

1. Поляризація суспільства. Дезінформація стає інструментом створення конфліктів між різними групами населення. Розпалювання соціальної ворожнечі та міжрегіональної напруженості є поширеним прийомом, що сприяє послабленню національної єдності.

2. Зниження рівня медіаграмотності. Через постійне поширення дезінформації багато громадян починають втрачати здатність критично оцінювати інформацію, яку вони отримують. Це призводить до подальшого маніпулювання їхньою свідомістю.

Не менш важливими є безпекові наслідки, а саме дестабілізація регіонів та підриг національної безпеки. Інформаційна кампанія має на меті спровокувати конфлікт у стратегічно важливих регіонах України. Це підвищує загрозу терористичних актів, диверсій та інших підригних дій. Підриг національної безпеки. Фейкові новини та інформаційні маніпуляції підригають здатність держави ефективно управляти кризовими ситуаціями. Це також ускладнює співпрацю між правоохоронними органами.

Економічні наслідки – це погіршення інвестиційного клімату. Негативні інформаційні кампанії увічнюють імідж країни, яка перебуває в кризі. Це, в свою чергу, впливає на рішення міжнародних інвесторів і затримує економічний розвиток. І сюди ж дестабілізація фінансової системи. Дезінформація, спрямована на створення паніки серед населення, може вплинути на валютні курси, спричинити масове вилучення депозитів з банків і загрожувати стабільності фінансової системи.

Як висновок можна зазначити, що інформаційна війна проти України має складні та багатогранні наслідки. Вона підриває довіру до держави всередині країни та за кордоном, створює розкол у суспільстві, погіршує безпеку та гальмує економічний розвиток. Боротьба з дезінформацією та підвищення рівня медіаграмотності населення є ключовими елементами для ефективної відповіді України на ці виклики.

3.2. Протидія України в інформаційній війні проти Росії

Використання інформаційних технологій для маніпулювання громадською думкою може мати тривалий вплив на демократичні процеси. Це стосується впливу на виборчі рішення, формування політичних поглядів та зміни ставлення до важливих суспільних питань. Такі маніпуляції можуть призвести до прийняття політичних рішень, які не відображають реальних потреб і прагнень громадян.

Інформаційні війни та пропаганда підривають довіру громадськості до джерел інформації. Це може призвести до загального скептицизму та цинізму у ставленні до ЗМІ, урядових повідомлень та інших офіційних комунікацій. Надмірний скептицизм ускладнює інформування громадськості про важливі соціальні та політичні події. Втрата довіри до джерел інформації спричиняє проблеми в управлінні кризовими ситуаціями та реагуванні на суспільні потреби, оскільки люди можуть ігнорувати або неправильно інтерпретувати ключові повідомлення.

Одним із наслідків пропаганди та інформаційної війни є поглиблення суспільних розбіжностей. Це відбувається тому, що аудиторії, «оброблені» різними «інформаційними потоками», вірять у протилежні погляди на одні й ті ж події. Це не лише призводить до соціального конфлікту, але й створює середовище, в якому кожна група вірить в абсолютну правильність власних переконань та ігнорує інші точки зору. Така поляризація поглядів ускладнює пошук спільних рішень і порозуміння, посилює соціальну напруженість і підриває гармонійне співіснування різних груп.

Сучасна російська інформаційна війна - це стратегія цілеспрямованих, довготривалих дій для досягнення своїх цілей. Однак Україна тривалий час не усвідомлювала необхідності вжиття заходів проти експансіоністської діяльності держави-агресора. Україна бореться з російським наративом, пропагандою та дезінформацією з 2014 року.

Варто зазначити, що спочатку сили в російсько-українській інформаційній війні були нерівними. Громадяни Росії отримували більшу частину інформації через підконтрольні державі федеральні канали. Українці, з іншого боку, часто отримували інформацію з телеканалів, безпосередньо підконтрольних олігархам. Тому довіра до українських телевізійних ЗМІ була набагато нижчою, ніж до російських. У роки незалежності України виклики інформаційних конфліктів значно ускладнювалися відсутністю системи захисту інформації [3, с. 89].

Політолог Є. Магда зазначає, що відсутність державної цензури та комерційний характер українських ЗМІ полегшили Росії взяття під контроль українського інформаційного простору та насичення його російським шоу-бізнесом [48, с. 290]. Кремль розглядає ЗМІ, включаючи телебачення, кіностудії та радіо, як важливий елемент національної безпеки і завжди ставився до них як до інструменту просування своїх інтересів.

Масована інформаційна війна Росії проти України вступила в нову фазу на початку 2014 року з появою таких ключових подій, як Революція Гідності, анексія Криму та війна на сході України. Цей конфлікт виявив усі слабкі місця України у сфері інформаційної безпеки, вказав на відсутність або недостатню ефективність механізмів забезпечення інформаційної безпеки та показав її неготовність до неочікуваних і непередбачуваних інформаційних викликів [30, с. 73-74].

Російська агресія 2014-2023 років виявила численні недоліки українського розвідувального сектору у протидії інформаційній війні. На думку українського науковця І. Лубковича, для того, щоб оцінити ефективність механізмів, які використовує Україна проти Росії в інформаційній війні, важливо більш детально проаналізувати наступні негативні моменти: 1) недостатні сили та обізнаність, 2) бездіяльність російських медіа-мереж на рівні реагування на конкретні дезінформаційні атаки та інформацію, надану російськими медіа-мережами, а також надання власної деталізації подій та фактів; 3) відсутність інформаційної

протидії з боку органів державної влади, що свідчить про необхідність розвитку спеціалізованих структур; 4) проблеми з фінансуванням, оскільки більшість ЗМІ прагнуть уникнути фінансових труднощів та втрати прибутку. бажання і не відмовилися від публікації російського медіа-контенту [49].

Однак Україна стає все більш ефективною у протидії російській інформаційній агресії. Інструменти боротьби з дезінформацією включають регуляторні та інституційні механізми.

З 2014 року українське законодавство, спрямоване на розвиток інформаційного простору України, значно покращилося. Були прийняті та вдосконалені ключові закони в інформаційній сфері: «Про захист інформації», «Про медіа», «Про інформацію» та ін. Одним з найважливіших нормативно-правових документів з питань інформаційної безпеки в Україні є Доктрина інформаційної безпеки України.

Органами, відповідальними за створення та забезпечення інформаційної безпеки в Україні, є Рада національної безпеки і оборони України, Міністерство оборони України, Міністерство закордонних справ, Кіберполіція, Державна служба спеціального зв'язку та захисту інформації України, Міністерство цифрової трансформації України, Міністерство інформаційної політики України, Центр протидії контррозвідці Потік російської дезінформації та її руйнівні наслідки значно зросли після російського вторгнення в лютому 2022 року [30, с. 74].

Для протидії цій дезінформаційній загрозі Україна активно використовує прогрес, досягнутий у зміцненні інформаційно-медійного середовища з 2014 року, та розробляє механізми безпосереднього реагування на інформаційні загрози. Це включає надання достовірної інформації, забезпечення спроможності протидіяти дезінформації та вжиття політичних заходів для протидії загрозам з боку російських державних ЗМІ [30, с. 74].

Україна активно впроваджує інформаційну політику, спрямовану на протидію російській пропаганді. Однією з таких ініціатив є програма інформування громадськості про фейкову інформацію, яка може надходити від ворога [20]. З кінця лютого 2022 року українська громадськість отримала детальну інформацію про війну, з особливим акцентом на тому, що достовірна інформація може надходити лише з офіційних українських джерел. Така стратегія дозволила протистояти традиційній російській тактиці, зокрема поширенню та агресивному розповсюдженню дезінформації через соціальні мережі та інші публічні канали.

Від початку війни між Росією та Україною журналісти та українське військове командування оперативно інформували громадськість про успіхи та невдачі українських сил. Така відкритість сприяла об'єктивному сприйняттю подій, що відбувалися в той час. Такий підхід нейтралізував важливий «козир» Росії, а саме можливість поширення дезінформації та паніки в атмосфері таємничості та невизначеності [37, с. 86].

Крім того, політика відкритості щодо джерел інформації призвела до об'єктивного висвітлення подій у світовій журналістиці. Це призвело до того, що більше уваги стало приділятися об'єктивності у висвітленні подій, що не дозволило російським агентам поширювати дезінформацію, наприклад, твердження про те, що мирні міста бомбардували націоналістичні полки. Слід зазначити, що на це також вплинула загальна політика російських державних ЗМІ. Постійний обман і відверта пропаганда, створення постановочних сюжетів і сумнівних експертних висновків зробили російську версію подій недостовірною у світовому інформаційному просторі [37, с. 86].

Інформаційна політика України була такою, що журналісти акцентували увагу на звірствах окупантів, а не приховували їх. Це створило в українському суспільстві чітке уявлення про злочини російської армії та призвело до формування негативного ставлення до російської армії та її дій. З точки зору

російського керівництва, можна було сподіватися, що війна скоро закінчиться і не потрібно буде приховувати надто багато інформації. Однак реальність виявилася іншою, і їхня інформаційна стратегія не передбачала створення ефективного інформаційного пресу для окупації. Поширення неправдивої інформації про «визволителів» і нерозуміння опору українського народу призвело до деморалізації російських військ [37, с. 86].

Інформаційна політика України була успішною та ефективно протидіяла проросійській пропаганді та іншим інформаційним загрозам. Українські ЗМІ зробили значний внесок у підвищення обізнаності громадськості, навчивши громадян розпізнавати дезінформацію та виявляти пропаганду. Важливим показником успіху є стійке бачення українців, яке демонструє здатність відрізняти достовірну інформацію від маніпуляцій та пропаганди.

Крім того, висока довіра громадян України до збройних сил, зокрема до Збройних Сил України, є свідченням успішності інформаційної стратегії. Ця довіра не лише зберігається в країні, але й зростає, незважаючи на інформаційні виклики, що виникли під час війни між Росією та Україною.

Контроль над медіа-простором має вирішальне значення під час збройного конфлікту.

Україна вирішила обмежити доступ до російських державних ЗМІ, щоб збільшити доступ до неупередженої інформації та обмежити вплив російської пропаганди. Окрім обмеження доступу до російських ЗМІ, це включає санкції проти телеканалів NewsOne, 112 Україна та ZIK, які пов'язані з народним депутатом Віктором Медведчуком, якого пов'язують з російською елітою. Медведчука також звинуватили у державній зраді та спробі зловживання державними ресурсами в Криму. Його звільнення в Росію у 2022 році в рамках обміну полоненими стало частиною широко відомої події в рамках великого обміну полоненими між Україною та Росією. NewsOne, 112 Україна та ZIK відомі своєю дезінформаційною діяльністю та поширюють узгоджені з російським

урядом меседжі, зокрема про вакцину проти COVID-19, а також про національні та міжнародні події в Україні. Їхнє об'єднання в єдиний телеканал «Перший незалежний» відбулося за участі Медведчука нібито з метою уникнення санкцій. Однак незабаром після цього Рада національної безпеки і оборони України (РНБО) заблокувала супутникове мовлення. Це призвело до перенесення «Першого каналу» на YouTube.

Ці дії демонструють спроби української влади послабити вплив проросійських ЗМІ та запобігти поширенню дезінформації, особливо в таких чутливих сферах, як епідемії та гібридна війна.

Після повномасштабного вторгнення Росії в Україну 24 лютого 2022 року український уряд втрутився у сферу приватних ЗМІ. Три великі приватні медіакомпанії («StarLightMedia», «1+1 media» та «Inter Media Group») об'єднали зусилля з суспільними мовниками «UA:Перший» та «Радіо Україна» для забезпечення цілодобового уніфікованого висвітлення подій у рамках проєкту «Єдині новини». Забезпечення єдиного 24-годинного висвітлення подій в рамках проєкту «Єдині новини». Після зустрічі керівників мовників на початку війни, 18 березня президент Зеленський підписав указ, який зобов'язав усі державні телеканали вести мовлення на єдиній платформі. Хоча цей підхід виявився ефективним у забезпеченні доступу до інформації та важливим для контролю нарративу про війну перед обличчям російських дезінформаційних кампаній, він викликає питання щодо прямого втручання держави у післявоєнне медіасередовище [30, с. 76].

Звернення Президента України до іноземних парламентів та міжнародних організацій, таких як Рада Безпеки ООН, Рада Європи, G7 та НАТО, також є важливим способом поширення інформації на міжнародному рівні. Нестандартні, прямі та відверті виступи можуть допомогти заручитися їхньою підтримкою та відтворити реальність і героїзм боротьби українського народу за право стати геополітичним суб'єктом і членом європейської спільноти.

Різноманітні інтерв'ю Володимира Зеленського українським та іноземним ЗМІ, в тому числі російським, наближають Україну до перемоги, а деякі з них є впевненими перемогами на інформаційному фронті. Приїзд до Києва офіційних делегацій, зокрема Державного секретаря США, прем'єр-міністрів європейських країн, зокрема Великої Британії, та лідерів інших країн, демонструє нашу солідарність з Україною та ефективність нашої інформаційної стратегії.

Президент України В. Зеленський налагодив ефективні канали обміну інформацією та прямого спілкування з українським народом через соціальні мережі. Він регулярно публікує селфі-відео, ділиться новинами про військові події, показує об'єкти, зруйновані внаслідок російської агресії, звертається до міжнародної спільноти та оголошує результати дипломатичної діяльності з лідерами інших країн. Такий підхід дозволяє Президенту ефективно комунікувати з громадянами, забезпечуючи прозорість і відкритість [30, с. 77].

Україна додала новий елемент до своєї боротьби з Росією, перенісши кібертактику на користувачів мережі. За допомогою «ІТ-армії» хакерів користувачі долучаються до цифрової боротьби проти російських організацій. Фахівці з кібер- та інформаційної безпеки з української сторони активно беруть участь у цифровій війні, атакуючи офіційні російські сайти, збираючи інформацію, протидіючи дезінформації та поширюючи меседжі.

Тому контроль над інформаційним простором сьогодні є дуже важливим і забезпечується низкою дій, серед яких [28, с.139]:

- 1) Забезпечити ефективне функціонування та регулярне оновлення інформації на офіційних веб-сайтах Президента України, Збройних Сил України, Національного банку України та інших державних органів України;
- 2) Ведення офіційних телеграм-каналів українських державних установ, зокрема Міністерства цифрової трансформації та Міністерства охорони здоров'я;
- 3) Створення офіційного телеграфного каналу для вищих посадових осіб та голів державних адміністрацій в Україні;

4) Розміщення новин на сторінках державних організацій у соціальних мережах (наприклад, на Facebook-сторінках Збройних Сил України та Кабінету Міністрів України);

5) Публікувати щоденний запис звернення Президента до українського народу;

6) Єдиний інформаційний канал стратегічних комунікацій, що транслюється на загальнонаціональному інформаційному каналі United News #Ua Together, відповідно до рішення Ради національної безпеки і оборони України від 19 березня 2022 року, створений Указом Президента України від 18 березня 2022 року [52]. Створення платформи.

Інформаційна війна є частиною російської агресії проти України, її народу та міжнародної спільноти в цілому. Як наслідок, зараз вона успішно функціонує як інформаційна зброя у формі пропаганди та дезінформації лише на території Росії. Україні поступово вдалося досягти як військового успіху, так і перемоги на інформаційному фронті.

Лідерство України на інформаційному фронті є важливим питанням для всіх рівнів влади, дипломатичних представників, журналістів, громадських діячів та широкої громадськості. Головна мета лідерства на інформаційному фронті - донести до міжнародної спільноти об'єктивні факти і дати їй можливість правильно оцінити дії Росії під час війни. Це призведе до запровадження санкцій проти держави-агресора та надання військової та економічної підтримки українським військам.

На міжнародному рівні уряди швидко визнали загрозу дезінформації в контексті широкомасштабної агресії Росії проти України. Вони відреагували проактивно, висвітлюючи сценарії та методи, які використовує російський уряд, запроваджуючи санкції проти медіа-організацій та окремих осіб, а також підтримуючи медіа-середовище не лише в Росії та Україні, але й на національному рівні. Міжнародні організації також надавали допомогу у вигляді

програм перевірки фактів і розвінчання дезінформації, а також механізмів обміну інформацією та технічної допомоги.

Однак через складну та нагальну ситуацію, спричинену війною, уроки, винесені з реакції влади на дезінформаційні загрози в перші роки війни, не завжди можуть бути застосовані в мирний час. З огляду на триваючу агресивну війну Росії проти України, необхідно розглянути, як досягти балансу між боротьбою з дезінформацією та підтримкою заходів, спрямованих на зміцнення свободи преси, інформаційних систем та демократії.

Висновок до розділу 3:

Російська агресія проти України є безпрецедентним явищем у сучасних міжнародних відносинах і була здійснена з порушенням міжнародних норм та інтересів європейської стабільності. Однак цей акт агресії не є одномоментним рішенням російського керівництва, а є результатом довготривалої політичної траєкторії Росії, в якій інформаційна війна є ключовим елементом.

Сучасна інформаційна війна стала невід'ємною частиною загального військового конфлікту між Росією та Україною. Росія розпочала війну проти України, щоб реалізувати возз'єднання колишнього Радянського Союзу та геополітичний перерозподіл євразійського простору під керівництвом Кремля. Це бачення було особливо підкреслено під час президентства Путіна, коли трансформація системи міжнародних відносин і перетворення Росії на наддержаву стало головною метою Кремля.

Одним із головних завдань російської пропаганди на цьому етапі є дискредитація української влади, української армії та суспільства в цілому. Це включає в себе поширення дезінформації про Україну. Аналіз показує, що російсько-українська інформаційна війна використовує як перевірені стратегії (стратегії створення зовнішнього та внутрішнього ворога, поширення міфів та

дезінформації, історичних наративів), так і відносно нові, такі як модель віртуалізації.

Протягом усього періоду розвитку України після здобуття незалежності рівень готовності українського суспільства до самозахисту та протидії маніпуляціям свідомістю був низьким, що є серйозною проблемою. Це може бути наслідком недостатньої інформаційної грамотності та браку знань про методи маніпуляції та їхні наслідки. Другою проблемою є слабкість державних систем протидії інформаційним операціям.

Однак, порівняно з минулим, включаючи відкриту атаку в 2014 році, Україна значно покращила свою підготовку до інформаційної війни. Чітко визначені канали комунікації з громадськістю допомогли запобігти поширенню паніки. Ефективна комунікація була налагоджена і з західними партнерами, які отримували об'єктивну інформацію про перебіг конфлікту. Завдяки діяльності українських ЗМІ, незалежних експертів та військових, російська пропаганда втратила свої вигідні позиції і була змушена зосередитися на «внутрішньому» ринку.

Кроки, зроблені українською владою у співпраці з громадянським суспільством та міжнародними організаціями для протидії російському інформаційному впливу, надають важливі перспективи та уроки щодо того, як протистояти неправдивому та оманливому змісту інформаційних атак.

Для ефективної протидії інформаційним атакам необхідно розробити та впровадити комплексну стратегію, що включає освіту, медіаграмотність, кібербезпеку та державні заходи з виявлення та протидії дезінформації. Важливим завданням є вдосконалення законодавчої бази на національному рівні для протидії та запобігання інформаційній війні та негативним інформаційно-психологічним впливам в Україні.

ВИСНОВКИ

Дослідження інформаційних війн підтверджують, що вони відіграють важливу роль у сучасному світі, де інформація стала стратегічним ресурсом і джерелом впливу. Інформаційна війна не лише формує громадську думку, але й здатна змінювати політичні режими, посилювати соціальну напругу та підривати національну безпеку. Аналіз соціально-політичної природи цього явища показує, що інформаційна війна - це діяльність, спрямована на дестабілізацію суспільства за допомогою маніпуляцій, дезінформації та пропаганди.

Дослідження видів і методів інформаційної війни показує, що сучасні інформаційні кампанії є багаторівневими, охоплюють як традиційні медіа, так і новітні цифрові технології. Роль соціальних мереж у державній політиці та боротьбі з дезінформацією є неоднозначною: з одного боку, вони сприяють поширенню інформації, з іншого - є платформою для інформаційних маніпуляцій.

Український досвід війни між Росією та Україною є прикладом масштабного використання інформаційних технологій для досягнення геополітичних цілей. Ворог активно використовує дезінформацію, фейки, пропаганду та кібератаки для дестабілізації ситуації в Україні, підриву довіри до влади та створення розколу в суспільстві. Водночас Україна поступово вдосконалює свої заходи протидії, розробляючи ефективну стратегію інформаційного захисту.

Наслідки інформаційної війни для України є значними, включаючи поглиблення соціальної напруженості, втрату довіри до державних інституцій, економічні збитки та шкоду міжнародному іміджу. Однак важливо відзначити, що Україна продемонструвала здатність адаптуватися до викликів інформаційної агресії, зміцнюючи власні механізми захисту.

Протидія інформаційним загрозам потребує комплексного підходу, що включає підвищення інформаційної грамотності населення, розвиток національного законодавства у сфері інформаційної безпеки та активну співпрацю з міжнародними партнерами. Успішна реалізація цих заходів є передумовою захисту суверенітету України та досягнення стабільного розвитку в умовах глобальної інформаційної конкуренції. Таким чином, отримані результати підкреслюють важливість подальших досліджень та вдосконалення стратегій протидії одній з ключових загроз сучасності - інформаційній війні.

ПЕРЕЛІК ПОСИЛАНЬ

1. Інформаційна війна. URL: <https://esu.com.ua/article-12460> (дата перегляду: 19.11.2024)
2. Лизанчук В. В. Антиукраїнська інформаційна агресія в телерадіопросторі Росії та України. URL: http://nbuv.gov.ua/UJRN/Nzizh_2014_56_5 (дата перегляду: 19.11.2024).
3. Стадник А. Г. Основні моделі організації інформаційних війн та їх різновиди. *Соціальні технології: актуальні проблеми теорії та практики*. 2015. Вип. 67-68. С. 81-91.
4. Почепцов Г. Г. Информация и дезинформация. Київ: Ника-Центр, 2001. 256 с.
5. Шпиґа П. С., Рудник Р. М. Основні технології та закономірності інформаційної війни. *Проблеми міжнародних відносин*. 2014. Вип. 8. С. 326- 339.
6. Конотопенко О. П. Засоби і методи інформаційної війни в українському просторі. URL: <https://library.vspu.net/jspui/bitstream/123456789/> (дата звернення: 21.11.2024).
7. Інформаційна війна і Україна. URL: <https://science.lpnu.ua/sites/default/files/journal-paper/2022/feb/26730/malyk.pdf>
8. Вступ до психологічної війни. URL: https://www-thoughtco-com.translate.goog/psychological-warfare-definition-4151867?_x_tr_sl=en&_x_tr_tl=ru&_x_tr_hl=ru&_x_tr_pto=sc
9. Введення до психологічної війни. URL: <https://anoncyberarmy.wordpress.com/2019/10/20/настъпва-ли-ерата-на-психотронните-ор/>
10. Що таке шкідливе програмне забезпечення та його види. URL: <https://www.microsoft.com/uk-ua/security/business/security-101/what-is-malware>
11. Що таке Stuxnet. URL: <https://www.malwarebytes.com/ru/stuxnet>

12. Злом Sony Pictures. URL: <https://coverlink.com/case-study/sony-pictures-entertainment-hack/>
13. Кібератака і кіберзахист. URL: <https://www.britannica.com/topic/cyberwar/Cyberattack-and-cyberdefense>
14. В. П. Шейнов, Информационные войны и психотронное оружие.
15. Джозеф Най, Soft Power: The Means to Success in World Politics.
16. Евгений Морозов, The Net Delusion.
17. С. В. Бондаренко, Информационная безопасность в условиях глобализации.
18. Роль соціальних мереж в політичних кампаніях. URL: <https://conferences.vntu.edu.ua/index.php/mn/mn2021/paper/viewFile/11205/9691>
19. USAID-Internews опублікувало результати опитування про споживання медіа. URL: <https://suspilne.media/culture/607619-tilki-38-ukrainciv-vvazaut-dezinformaciu-nagalnou-problemou-opituvanna/>
20. Горбань Ю. Інформаційна війна проти України та засоби її ведення. *Вісник Національної академії державного управління при Президентові України*. 2015. Вип. 1. С. 136–141.
21. Почепцов Г. Смыслы и войны. Украина и Россия в информационной та смысловой войнах. Київ, 2016. 151 с.
22. Інформаційна війна коштує Росії 4\$ мільярди. URL: www.ukrinform.ua/ukr.news/2030605.
23. Ніколаєць Ю. Інформаційно-комунікаційний простір України в умовах російсько-української війни (2014–2023). *Сіверянський літопис*. 2023. №2. С.140-152.
24. Довгань Б. В., Мартинюк О. В. Становлення та розвиток поняття інформаційної війни. *Вісник студентського наукового товариства ДонНУ імені Василя Стуса*. 2020. №12. С.51-56.
25. Малик Я. Й. Інформаційна війна і Україна. *Демократичне врядування*.

2015. Вип. 15. URL: http://nbuv.gov.ua/UJRN/DeVr_2015_15_3 (дата звернення: 24.11.2024).

26. Чмир Я. Інформаційна війна як ключова загроза демократичному державотворенню України. *Державноуправлінські студії*. 2019. № 10. С. 1–11.

27. Патлашинська І. В. Сучасна російсько-українська інформаційна війна: завдання, методи та особливості використання. *Регіональні студії*. 2022. № 28. С. 84-87.

28. Щеголь А.В. Інформаційна війна в умовах міжнародного збройного конфлікту на території України, викликаного агресією російської федерації. *Матеріали Восьмої всеукраїнської студентської наукової конференції «Актуальні проблеми соціальних комунікацій» 30 травня 2022 р.* Київ: ФМВ НАУ. 2022. С.138-140.

29. Джус О.А. Концептуальні основи ведення інформаційної війни в сучасних умовах збройної агресії РФ проти України. *Політологічний вісник*. 2022. №88. С.189-201.

30. Дунаєва Л. М. Дезінформаційні виклики під час російсько-української війни: політологічний аналіз. *Політикус : наук. журнал*. 2022. № 5. С. 73–78

31. Вперед у світле минуле, або як російська пропаганда маніпулює на ностальгії за СРСР. URL: <https://armyinform.com.ua/2020/12/vpered-u-svitlenynule-abo-yakrosijska-propaganda-manipulyuyey-na-nostalgiyi-za-srsr/> (дата звернення: 28.11.2024).

32. День Победы и бесконечный круг пропаганды. URL: <https://www.stopfake.org/ru/den-pobedy-i-beskonechnyj-krug-propagandy/> (дата звернення: 28.11.2024)

33. Більовська Ю.І. Особливості ведення інформаційної війни рф проти України. *Матеріали Восьмої всеукраїнської студентської наукової конференції «Актуальні проблеми соціальних комунікацій» 30 травня 2022 р.* Київ: ФМВ

НАУ. 2022. С.9-12.

34. GEC Special Report: Pillars of Russia's Disinformation and Propaganda Ecosystem. URL: https://www.state.gov/wp-content/uploads/2020/08/Pillars-ofRussia%E2%80%99s-Disinformation-and-Propaganda-Ecosystem_08-04-20.pdf

(дата звернення: 30.11.2024).

35. Калініченко Б. Визначальні напрями формування стратегії протистояння інформаційній війні. *Держава і право. Серія: Політичні науки*. 2019. Вип. 83. С. 61–73.

36. Меренюк С., Меренюк Х. Україно-російська гібридна війна. *Україна в умовах трансформації міжнародної системи*. Львів, 2019. С. 47–51

37. Патлашинська І. В. Сучасна російсько-українська інформаційна війна: завдання, методи та особливості використання. *Регіональні студії*. 2022. № 28. С. 84-87.

38. Дубас О. Інформаційна війна: нові можливості політичного протистояння. *Освіта регіону: політологія, психологія, комунікації*. 2010. № 1. С. 69-73.

39. Феценко І. Інформаційна війна як органічна складова сучасного збройно-політичного конфлікту. *Філософія та політологія в контексті сучасної культури*. 2021. Вип. 13 (1). С. 96–103.

40. Почепцов Г. Г. Информационные операции и Крым: базовые причины для манипуляций. URL: http://psyfactor.org/psyops/infowar_krym.htm (дата звернення: 02.12.2024).

41. Семен Н. Ф. Російські інтернет-ресурси як чинник інформаційної війни проти України (на прикладі сайтів «Правда. Ру» та «Российский диалог»). Дис. к. соц. наук. Міжнародний економіко-гуманітарний університет ім. акад. С. Дем'янчука. Рівне. 2018. 260 с.

42. Пашков М. Російська інформаційна експансія: український плацдарм. URL: <https://razumkov.org.ua/statti/rosiyska-informatsiyna->

ekspansiya- ukrayinskyyplatsdarm (дата звернення: 04.12.2024).

43. Почепцов Г. Сенси і війни. Україна і Росія в інформаційній та смисловій війнах. Київ, 2016. 151 с.

44. Як маніпулюють інформацією? URL:
http://mediadriverr.online/manipuliatsiyi_ta_propahanda/yak-manipulyuyutinformatsiyeyu/ (дата звернення: 04.12.2024).

45. Шевчук П. І. Інформаційно-психологічна війна Росії проти України: як їй протидіяти. *Демократичне врядування*. 2014. Вип. 13. URL:
http://nbuv.gov.ua/UJRN/DeVr_2014_13_11. (дата звернення: 04.12.2024).

46. Валушко І. О. Інформаційна безпека України в контексті російсько-українського конфлікту. Дис. к. політ. н. Дипломатична академія України при МЗС України. Київ, 2018. 210 с.

47. Наслідки інформаційних війн. URL:
<https://welfare.green/protistoyannya-informacijnim-vijnam-ta-propagandi-u-suchasnomu-sviti/>

48. Магда Є. В. Гібридна війна: вижити і перемогти. Харків: Віват, 2015. 304 с.

49. Лубкович І. М. Місце українських медій в інформаційній війні 2013–2014 рр. *Наукові записки інституту журналістики*. 2014. № 56. С. 182–187.