Харківський національний університет імені В.Н. Каразіна
Навчально-науковий інститут «Каразінський інститут міжнародних відносин та туристичного бізнесу»
Кафедра міжнародних відносин

КВАЛІФІКАЦІЙНА

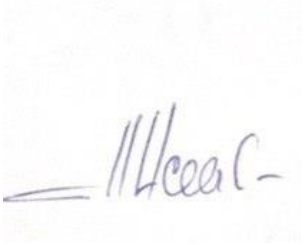
РОБОТА МАГІСТРА

на тему: «**Інформаційно психологічні операції у сучасних міжнародних збройних конфліктах»**

Виконав:
студент 2-го курсу, групи УМІБ-61
спеціальності 291 «Міжнародні відносини, суспільні комунікації та регіональні студії»
ОПП «Міжнародна інформаційна безпека»
Тищенко Ярослав Володимирович
(прізвище, ім'я, по батькові)

Керівник:
Файєр Олена Анатоліївна, к., юр., наук, доцент
(науковий ступінь, вчене звання, прізвище, ім'я, по батькові)

Рецензент:
Ісаєв Арсен Миколайович, кандидат юридичних наук, доцент.
(науковий ступінь, вчене звання, прізвище, ім'я, по батькові)



ХАРКІВ - 2025 р.

Харківський національний університет імені В. Н. Каразіна
Навчально-науковий інститут «Каразінський інститут міжнародних відносин та туристичного бізнесу»
Кафедра міжнародних відносин
Спеціальність 291 «Міжнародні відносини, суспільні комунікації та регіональні студії»
Освітньо-професійна програма Міжнародна інформаційна безпека»
Рівень вищої освіти: другий (магістерський)

ЗАТВЕРДЖУЮ
завідувач кафедри

_____ **Наталія ВІННИКОВА**
(Підпис) (ім'я, прізвище)

«2» червня 2025 року
(зі змінами від 10.09.2025; 06.10.2025)

ЗАВДАННЯ
на кваліфікаційну роботу магістра

Тищенко Ярослав Володимирович
(прізвище, ім'я та по батькові)
Тема роботи «**Інформаційно психологічні операції у сучасних міжнародних збройних конфліктах**»

керівник роботи Файєр Олена Анатоліївна, к., юр., наук, доцент
(прізвище, ім'я, по батькові, науковий ступінь, вчене звання)

затверджені наказом по університету від «02» червня 2025 року № 4001-5/1324 зі змінами від «10» вересня 2025 року № 4001-5/3049, зі змінами від «6» жовтня 2025 року № 4001-5/3656.

2. Строк подання здобувачем вищої освіти роботи 21 листопада 2025 р.

3. Перелік питань, які потрібно розробити:

1. Розкрити теоретичні концепції та моделі, що лежать в основі інформаційно-психологічних операцій.
2. З'ясувати хід еволюції теоретичних підходів до інформаційно-психологічних операцій у російсько-українському конфлікті.
3. Виявити та узагальнити ключові зміни у теоретичних стратегіях російських інформаційних операцій порівняно з традиційними методами пропаганди.
4. Виокремити практичні інструменти проведення росією інформаційно-психологічних операцій та оцінити українські механізми протидії цим діям.

5. Встановити основні практичні виклики, пов’язані з російськими ІПО проти України та розробити аналітичні рекомендації щодо подолання цих загроз і вдосконалення стратегій національної протидії.

4. План роботи

№ з/п	Назви етапів роботи	Строк виконання етапів
1	Вибір здобувачем теми КРМ і подання заяви на кафедру; затвердження теми та призначення наукового керівника; складання та затвердження індивідуального завдання на виконання КРМ	19.05.2025-30.06.2025
2	Підготовка вступу і розділу 1 КРМ	01.09.2025-30.09.2025
3	Підготовка розділу 2 КРМ	01.10.2025-15.10.2025
4	Підготовка розділу 3 КРМ	16.10.2025-31.10.2025
5	Підготовка висновків і переліку використаних джерел	03.11.2025-14.11.2025
6	Подання студентом завершеної КРМ науковому керівнику для перевірки та оформлення відгуку, перевірка КРМ на відсутність запозичень	17.11.2025-21.11.2025
7	Попередній розгляд КРМ на комісії від кафедри	24.11.2025-28.11.2025
8	Прийняття кафедрою рішення про допуск роботи до захисту в ЕК, оформлення та зовнішнє рецензування	01.12.2025-05.12.2025
9	Захист КРМ в ЕК і присвоєння випускникам кваліфікації	08.12.2025-24.12.2025

Дата видачі завдання: 2 червня 2025 року (зі змінами від 10.09.2025; 06.10.2025).

Здобувач вищої освіти _____ Ярослав Тищенко
(підпис) (ім'я, прізвище)

Керівник роботи _____ Олена Файєр
(підпис) (ім'я, прізвище)

ЗМІСТ

ВСТУП

Актуальність теми - у сучасному світі, де інформаційні технології стрімко розвиваються, інформаційно-психологічні операції (ІПО) стали ключовим інструментом впливу в міжнародних збройних конфліктах. Цифрові платформи, соціальні мережі, штучний інтелект та кіберпростір радикально змінили підходи до ведення інформаційних воєн, дозволяючи державам, організаціям і недержавним акторам впливати на суспільну думку, маніпулювати інформацією та формувати сприйняття подій. У цьому контексті ІПО набувають особливого значення як засіб досягнення стратегічних цілей у конфліктах, де традиційні методи ведення війни доповнюються цифровими технологіями.

Інформаційно-психологічні операції мають довгу історію, але з появою цифрових технологій їх методи та інструменти зазнали значної трансформації. Особливо помітною є активна інформаційна пропаганда Росії, яка з 2013 року використовує соціальні мережі, боти, медіа-кампанії та кібератаки для впливу на Україну в рамках російсько-українського конфлікту. Ці операції спрямовані на поширення дезінформації, маніпуляцію громадською думкою та дестабілізацію суспільства. У свою чергу, Україна активно протидіє цим діям, застосовуючи власні стратегії ІПО та співпрацюючи з міжнародними партнерами. Приклади таких операцій ілюструють, як цифрова сфера стала ареною боротьби за інформаційну перевагу.

Ступінь вивченості теми - закордоном феномен інформаційно-психологічних операцій ґрунтовно розроблений у працях RAND Corporation, Atlantic Council, NATO StratCom COE, Oxford Internet Institute, DFRLab, Brookings Institution, а також у роботах Дж. Арквилли, Т. Ріда, П. Померанцева, М. Галеотті, К. Пола та М. Метьюза. В Україні тему активно досліджують Національний інститут стратегічних досліджень, Центр стратегічних комунікацій та інформаційної безпеки при РНБО, Центр протидії дезінформації, проєкти StopFake та «ВоксЧек».

Мета дослідження - визначити хід трансформації інформаційно-психологічних операцій у міжнародних збройних конфліктах.

На основі мети виділено **такі завдання:**

1. Розкрити теоретичні концепції та моделі, що лежать в основі інформаційно-психологічних операцій.
2. З'ясувати хід еволюції теоретичних підходів до інформаційно-психологічних операцій у російсько-українському конфлікті.
3. Виявити та узагальнити ключові зміни у теоретичних стратегіях російських інформаційних операцій порівняно з традиційними методами пропаганди.
4. Виокремити практичні інструменти проведення росією інформаційно-психологічних операцій та оцінити українські механізми протидії цим діям.
5. Встановити основні практичні виклики, пов'язані з російськими ІПО проти України та розробити аналітичні рекомендації щодо подолання цих загроз і вдосконалення стратегій національної протидії.

Об'єкт дослідження - інформаційно-психологічні операції в міжнародних збройних конфліктах.

Предмет дослідження - застосування інформаційно-психологічних операцій Росією в міжнародних збройних конфліктах.

Практичне значення - готові до впровадження рекомендації для РНБО, СБУ, Міністерства цифрової трансформації, Міністерства освіти і науки України та партнерів у НАТО. Створення державного центру моніторингу ІПО на базі власних ШІ-рішень, законодавче регулювання анонімних Telegram-каналів, обов'язкове включення медіаграмотності до шкільної програми, розробка національних алгоритмів раннього виявлення дезінформації та deepfake, поглиблення співпраці з НАТО у сфері стратегічних комунікацій.

Апробація - апробація дипломної роботи пройшла у рамках круглого столу «Стратегічні напрями зовнішньої політики та дипломатії країн світу»

Структура роботи

Кваліфікаційна робота складається зі вступу, двох розділів, висновків та списку використаних джерел, який налічує 50 найменувань. Загальний обсяг роботи становить 76 сторінок, з яких основного тексту - 68 сторінок.

РОЗДІЛ 1. ІНФОРМАЦІЙНО-ПСИХОЛОГІЧНІ ОПЕРАЦІЇ У ГІБРИДНОМУ ПРОТИСТОЯННІ: ТЕОРІЯ, ЕВОЛЮЦІЯ ТА СПЕЦИФІКА РОСІЙСЬКОГО ПІДХОДУ

1.1. Теоретико-методологічні засади та ключові моделі ІПО

У сучасних міжнародних конфліктах інформаційна війна стала ключовим інструментом досягнення стратегічних цілей, дозволяючи державам впливати на суспільну свідомість, політичні процеси та міжнародну підтримку без прямого застосування військової сили.

Теоретичні основи інформаційної війни сформувалися наприкінці XX століття, але з появою цифрових технологій вони набули нових форм, особливо в контексті російсько-українського конфлікту, який розпочався в 2013 році з анексії Криму та ескалації на Донбасі. Інформаційна війна передбачає систематичне використання інформації для маніпуляції сприйняттям реальності, підриву стабільності опонента та формування вигідних наративів.

У російській пропаганді проти України ці процеси ґрунтуються на двох ключових концепціях: інформаційного домінування та гібридної війни. Ці теоретичні підходи не лише пояснюють стратегії впливу, але й визначають практичні методи, які Росія застосовує для дестабілізації України, послаблення її міжнародної підтримки та впливу на внутрішню єдність суспільства [1].

Концепція інформаційного домінування є центральною в теоріях інформаційної війни і передбачає контроль над інформаційним потоком, що дозволяє одній стороні формувати сприйняття реальності цільовою аудиторією, обмежуючи можливості опонента для ефективної комунікації. Ця ідея, вперше систематизована в західних військових доктринах, була адаптована Росією для реалізації власних геополітичних цілей.

З 2013 року російська пропаганда використовує державні медіа, такі як RT і Sputnik, а також соціальні мережі, для поширення наративів про "нелегітимність" української влади, "захист російськомовного населення" та "зовнішнє управління" Україною з боку Заходу. Ці наративи спрямовані на створення інформаційної переваги, що досягається не лише через обсяг контенту, але й через його емоційне забарвлення, яке апелює до страхів, упереджень і стереотипів аудиторії.

Наприклад, під час анексії Криму в 2014 році Росія активно просувала історії про "утиски російськомовних" та "загрозу націоналізму", що виправдовувало її дії як "гуманітарну інтервенцію". Такі дії дозволили Росії не лише мобілізувати внутрішню підтримку, але й посіяти розбіжності в міжнародному сприйнятті конфлікту, що є прикладом інформаційного домінування в дії [2].

Інша важлива концепція - гібридна війна - поєднує традиційні військові дії з неконвенційними методами, такими як економічний тиск, кібератаки та інформаційні операції. Гібридна війна створює "сіру зону" конфлікту, де межі між миром і війною розмиті, а інформація стає інструментом для підготовки до ескалації або її уникнення. У російському контексті ця концепція отримала розвиток у так званій "доктрині Герасимова", яка підкреслює перевагу несилових методів над силовими у співвідношенні 4:1.

У російсько-українському конфлікті з 2013 року гібридна війна проявляється через систематичне поширення дезінформації, наприклад, про "секретні біолабораторії США" в Україні чи "агресивні плани НАТО". Ці наративи спрямовані на підрив довіри до українських інституцій і створення хаосу в інформаційному просторі. Наприклад, у 2014 році російські медіа активно просували фейкові історії про "розп’ятого хлопчика" на Донбасі, що мало на меті викликати емоційний резонанс і виправдати підтримку сепаратистських рухів. Такі дії демонструють, як гібридна війна використовує інформаційні операції для досягнення стратегічних цілей без прямого військового протистояння [3].

Важливим аспектом російської інформаційної війни є її адаптація до сучасних реалій, зокрема до можливостей цифрових технологій. Якщо раніше пропаганда базувалася на радіо, телебаченні та друкованих ЗМІ, то з 2013 року Росія активно використовує соціальні мережі, такі як VKontakte, Telegram і Twitter (тепер X), для швидкого поширення дезінформації. Ці платформи дозволяють створювати вірусний контент, який апелює до емоцій і підсилює когнітивні упередження, такі як ефект підтвердження, коли аудиторія сприймає лише ту інформацію, яка відповідає її переконанням. Наприклад, російські кампанії в 2014-2015 роках використовували фейкові акаунти та ботів для підсилення наративів про "київську хунту", що впливало як на російськомовну аудиторію в Україні, так і на міжнародну спільноту.

Цей підхід ґрунтується на теоретичних моделях маніпуляції масовою свідомістю, які передбачають використання емоційно зарядженого контенту для зміни суспільних настроїв [4].

Крім того, російська інформаційна війна проти України з 2013 року характеризується системним підходом до створення альтернативної реальності. Це досягається через поєднання дезінформації, пропаганди та психологічного впливу, що базується на теоріях когнітивного впливу. Росія використовує принципи "інформаційного шуму", коли великий обсяг суперечливих повідомлень ускладнює для аудиторії розрізнення правди від брехні.

Наприклад, під час ескалації конфлікту на Донбасі в 2014 році російські ЗМІ одночасно просували різні наративи - від звинувачень України в "геноциді" до тверджень про "зовнішнє управління" з боку США. Такий підхід дозволяє заплутати аудиторію, послабити її критичне мислення та створити сприятливі умови для подальших маніпуляцій. Теоретична основа цього методу ґрунтується на концепціях когнітивного дисонансу та інформаційного перевантаження, які активно досліджуються в сучасній літературі з інформаційної безпеки [5].

Продовжуючи розгляд теоретичних і практичних аспектів російської інформаційної війни, варто підкреслити, що її ефективність значною мірою обумовлена комплексним використанням стратегій психологічного впливу, інформаційної маніпуляції та технологічних інновацій. У поєднанні вони формують цілісну систему, яка працює на досягнення довгострокових політичних, військових та економічних цілей Росії. Архітектура цієї системи передбачає багаторівневу взаємодію між державними інститутами, приватними структурами, проксі-організаціями та неформальними мережами впливу, що діють у єдиному інформаційному просторі [1].

Однією з ключових особливостей російської інформаційної кампанії є її здатність адаптуватися до змін середовища, оперативно інтегруючи нові інструменти та платформи. Якщо на початку конфлікту основний наголос робився на традиційних медіа, то вже у другій половині 2010-х років акцент змістився на цифрові технології та алгоритмічне просування контенту. Це дозволяє не лише збільшувати охоплення, але й підвищувати точність таргетингу, впливаючи на конкретні сегменти аудиторії з урахуванням їхніх соціально-демографічних характеристик, політичних уподобань та емоційного стану [4].

Ключовим елементом цієї стратегії є використання дезінформаційних каскадів, коли поширення неправдивих відомостей відбувається одночасно з кількох джерел, створюючи ілюзію незалежного підтвердження. Такі каскади особливо ефективні в соціальних мережах, де швидкість обігу інформації значно перевищує темпи її перевірки. Дослідження показують, що емоційно забарвлені повідомлення, навіть якщо вони неправдиві, поширюються значно швидше, ніж нейтральна або перевірена інформація [4]. У випадку російсько-українського конфлікту прикладом може бути масштабне розповсюдження фейкових матеріалів про події в Іловайську чи Дебальцевому, де неправдиві версії подій з’являлися раніше, ніж офіційні повідомлення, що дозволяло формувати перше враження на користь російської сторони.

Ще одним суттєвим аспектом є ефект "захоплення інформаційного поля", коли кількість та інтенсивність повідомлень певного наративу витісняє альтернативні інтерпретації з публічного простору. Це відповідає концепції "інформаційного домінування", описаній у військових теоріях кінця XX століття, коли контроль над інформаційним середовищем розглядається як одна з головних передумов перемоги у сучасному конфлікті [1]. Застосування цього підходу Росією полягає в тому, щоб забезпечити присутність своїх версій подій у всіх ключових каналах комунікації - від офіційних брифінгів до мемів і коментарів у соцмережах.

Паралельно реалізується стратегія "керованого хаосу", коли цілеспрямовано створюється суперечливий і перевантажений інформаційний простір. За таких умов аудиторія втрачає здатність ефективно розрізняти факти та інтерпретації, а процес формування громадської думки переходить під контроль сторони, що продукує більший обсяг контенту [5]. Показовим прикладом є одночасне поширення взаємовиключних версій катастрофи рейсу MH17, що мало на меті не стільки довести певну версію, скільки зруйнувати довіру до будь-яких джерел інформації, крім російських.

Варто зазначити, що російська інформаційна війна не обмежується межами України. Вона має виразний транснаціональний вимір, спрямований на вплив на громадську думку в країнах ЄС, США та інших регіонах. Це відповідає моделі "активних заходів", що передбачає використання медіа, громадських організацій, аналітичних центрів і навіть культурних ініціатив для формування сприятливого іміджу Росії або дискредитації її супротивників [5]. Зокрема, за допомогою телеканалу RT та агентства Sputnik активно просуваються меседжі, які підважують єдність ЄС і НАТО, створюючи передумови для політичної фрагментації та зниження рівня підтримки України на міжнародному рівні [2].

З 2013 року Росія веде проти України інформаційну війну, яка стала складним і багатогранним явищем. Вона поєднує традиційні методи контролю над інформацією, сучасні підходи гібридної війни та новітні способи

маніпуляції в цифровому просторі [1]. Головна особливість цієї війни в тому, що інформація тут не просто доповнює військові дії, а є окремим фронтом - таким, що може кардинально змінити розстановку сил, навіть без застосування зброї.

Аналізуючи цю війну, стає очевидно: вона не просто частина гібридних операцій, а самостійна сила, здатна впливати на політику, суспільні настрої та міжнародні відносини. На відміну від звичайних бойових дій, які обмежені в часі та просторі, інформаційна війна триває безперервно - і в періоди активних сутичок, і в часи відносної стабільності. Її головна сила в тому, що вона змінює світогляд і цінності людей на тривалий час, а це, у свою чергу, впливає на політичні рішення та громадську думку [1; 3].

Важливою рисою російського підходу є його гнучкість і багатоканальність. Як показує практика, Кремль одночасно застосовує широкий спектр тактик: від масового виробництва фейкових новин і маніпулятивних інтерпретацій фактів до більш тонких методів, таких як "м’яка сила" через культурні, історичні та мовні наративи [2]. Поєднання агресивної пропаганди з псевдоліберальними або навіть "антисистемними" повідомленнями дозволяє охоплювати аудиторію різних ідеологічних спектрів, створюючи у неї відчуття, що російська позиція має численні "альтернативні" джерела підтримки.

Досвід російсько-українського конфлікту показує, що подібні інформаційні кампанії часто будуються на методі "контрольованої реальності", коли за допомогою постійного повторення певних тез і селективного висвітлення подій формується нова інформаційна картина світу. У цій картині Росія позиціонується не як агресор, а як "захисник", "посередник" або "стабілізуючий фактор" у міжнародних відносинах [4]. Інформаційна війна дає змогу перетворювати навіть явні факти агресії на «спірні» теми, що допомагає розмивати міжнародну відповідальність і послаблювати політичний тиск на Росію [5]. Але не менш важливо те, що ця війна проти України вписана в ширші глобальні процеси - підрив

демократичних інститутів і принципів вільної преси. Дослідники відзначають, що кампанії дезінформації не обмежуються однією країною: їхні моделі експортуються і адаптуються в інших регіонах - від Балкан до Латинської Америки [5].

Можна стверджувати, що російська інформаційна війна - це не випадковий набір дій, а системна, глибоко пророблена стратегія, яка тісно пов’язана з державною політикою. Вона поєднує класичні методи інформаційного домінування [1], підходи гібридної війни [3] та активні заходи [5], доповнені сучасними цифровими технологіями [4]. Її ефективність полягає не лише в тому, що вона впливає на факти, а й в тому, що змінює сприйняття, цінності та емоції людей. Тому боротьба з такою загрозою вимагає не тільки технічного захисту в кіберпросторі, а й комплексних стратегій: підвищення медіаграмотності, розвитку критичного мислення та зміцнення суспільної стійкості до маніпуляцій [2; 4].

Психологічні операції (далі- PSYOPS) як складова сучасної інформаційної війни є одним із ключових інструментів стратегічного впливу на індивідуальну та колективну свідомість. Їхня головна мета полягає у зміні способу мислення, емоційного стану, переконань та поведінкових моделей цільової аудиторії у спосіб, що відповідає інтересам ініціатора впливу [6]. На відміну від прямого фізичного примусу, PSYOPS спираються на комплексне використання психологічних знань, соціальної інженерії та комунікаційних технологій, що дозволяє досягати результатів без відкритого застосування сили, проте із часто більш тривалими наслідками.

Теоретичною основою сучасних психологічних операцій є поєднання напрацювань військової доктрини, соціальної психології та когнітивних наук. Серед ключових концепцій, що застосовуються у PSYOPS, варто виділити фреймінг - процес структурування інформації у такий спосіб, щоб аудиторія інтерпретувала подію крізь задану призму; праймінг - підготовку свідомості шляхом попереднього впливу на асоціативний ряд; та контроль порядку денного - визначення того, які теми обговорюються і які залишаються поза

увагою [7]. Використання цих технік дозволяє формувати у споживачів інформації не лише певне ставлення до конкретних фактів, а й цілісну картину світу, в якій закладені смисли вигідні ініціатору операцій.

У контексті російсько-українського конфлікту психологічні операції активно спираються на маніпуляції колективною пам’яттю, історичними травмами та культурними архетипами. Використання образів «зовнішнього ворога» чи «захисника пригноблених» дає змогу мобілізувати внутрішню підтримку та виправдати агресивні дії перед власною і міжнародною аудиторією [8]. Такі підходи тісно пов’язані з теорією соціальної ідентичності, згідно з якою людські спільноти схильні поділяти світ на «своїх» і «чужих», причому емоційно забарвлене сприйняття «чужих» значно полегшує легітимацію насильства або дискримінації.

Окремим і надзвичайно ефективним інструментом PSYOPS є технологія «інформаційного затоплення» (information flooding), яка полягає у масовому поширенні величезних обсягів суперечливої або взаємовиключної інформації [9]. У результаті цільова аудиторія втрачає здатність чітко відокремлювати правдиві дані від неправдивих, що призводить до зростання втоми від інформаційного шуму та зниження рівня критичного мислення. У таких умовах люди схильні обирати для себе найпростіші, емоційно насичені та когнітивно зручні інтерпретації подій, навіть якщо вони суперечать об’єктивним фактам.

Не менш важливим психологічним механізмом є використання принципів поведінкової економіки, зокрема теорії перспектив, яка пояснює, що люди приймають рішення інакше, коли йдеться про ймовірні втрати, ніж коли йдеться про можливі здобутки [10].

У практиці російської інформаційної агресії ці принципи реалізуються через систематичне перебільшення можливих загроз у разі продовження спротиву, а також шляхом створення у громадян відчуття невідворотності негативних наслідків будь-яких альтернативних сценаріїв. Це формує

середовище страху та демотивації, в якому навіть неправдоподібні або нелогічні наративи можуть сприйматися як «раціональні».

Психологічні механізми впливу у PSYOPS - це не лише набір окремих технік, а цілісна система, що інтегрує когнітивні, емоційні та культурні фактори. Вони діють одночасно на рівні свідомості та підсвідомості, а ефект досягається завдяки тривалому, послідовному і багатоканальному інформаційному тиску. В умовах гібридної війни, де межа між воєнними і невійськовими методами часто розмита, PSYOPS стають одним із найпотужніших інструментів формування реальності, в якій політичні та військові цілі досягаються через зміну сприйняття, а не лише через фізичне знищення супротивника.

Окремої уваги потребує аналіз того, як психологічні операції інтегруються у комплексні інформаційні кампанії, що поєднують традиційні та цифрові канали поширення. Сучасні PSYOPS не обмежуються виключно поширенням друкованих матеріалів чи радіопередач, як це було в середині XX століття [1]. Сьогодні вони ґрунтуються на алгоритмічному аналізі великих масивів даних, що дає змогу точно сегментувати аудиторію за демографічними, культурними та поведінковими параметрами. Завдяки цьому зростає ефективність персоналізованого контенту, який апелює до конкретних страхів, надій чи упереджень кожної підгрупи цільової аудиторії [11].

Важливо розуміти, що ефективність таких операцій значною мірою залежить від здатності ініціатора впливу підтримувати когерентність головного наративу при одночасному варіюванні його деталей залежно від середовища та цільового сегмента. Наприклад, під час російської агресії проти України одні й ті самі ключові повідомлення про «захист російськомовних» або «боротьбу з фашизмом» набували різного емоційного забарвлення залежно від того, чи спрямовувалися вони на внутрішню російську аудиторію, на українців, чи на західних споживачів інформації [2]. Така адаптація відбувається завдяки використанню методів нейролінгвістичного програмування (НЛП) та комунікаційної психології, що дозволяє тонко

коригувати формулювання, не змінюючи основної пропагандистської мети [12].

Ще одним критично важливим аспектом є створення та підтримка штучної «інформаційної реальності» - ситуації, коли аудиторія живе у системі координат, яка відрізняється від об'єктивної картини світу, але здається їй єдино правильною [3]. Для цього застосовуються як техніки повторення меседжів (mere exposure effect), так і контроль каналів отримання новин, що зменшує ймовірність зіткнення з альтернативними поглядами [4]. У результаті формується замкнене когнітивне середовище, в якому будь-яка інформація, що суперечить встановленому наративу, автоматично відкидається як «ворожа» чи «підроблена» [5].

Психологічні операції також активно використовують феномен «емоційного зараження», коли масові емоції, поширювані через соціальні мережі або ЗМІ, впливають на індивідуальний емоційний стан та подальшу поведінку людей [6]. Це особливо дієво в умовах криз і конфліктів, коли високий рівень стресу знижує здатність до критичного аналізу та підвищує залежність від емоційних аргументів. Емоції в психологічних операціях не просто доповнюють інші методи - вони стають одним із ключових способів створення і закріплення маніпулятивних наративів [9].

Загалом, сучасні PSYOPS - це динамічна, адаптивна і багаторівнева система психологічного впливу, здатна функціонувати як у рамках військових конфліктів, так і в умовах політичної та економічної нестабільності. Вони інтегрують наукові знання з психології, комунікацій, соціології та кібернетики, що робить їх надзвичайно гнучкими і водночас складними для протидії. Саме тому розуміння їхніх психологічних механізмів є ключовим завданням для розробки ефективних стратегій інформаційної безпеки та зміцнення стійкості суспільної свідомості до зовнішніх маніпуляцій [10].

Одним із ключових інструментів у структурі російських інформаційно-психологічних операцій (ІПО) є систематичне використання когнітивних упереджень, які вбудовуються в інформаційні повідомлення з метою

підвищення їхньої ефективності та емоційної привабливості. Когнітивні упередження - це сталі відхилення у процесах сприйняття, пам’яті та мислення, що призводять до систематичних помилок у судженнях і рішеннях [13]. На відміну від свідомих логічних аргументів, вони діють на підсвідомому рівні, формуючи реакції, що здаються природними, але насправді є результатом ретельно сконструйованого впливу.

Росія активно використовує такий психологічний механізм, як підтверджувальне упередження - природну схильність людей сприймати, тлумачити і запам’ятовувати лише ту інформацію, яка підтверджує їхні вже існуючі погляди [4]. У російських інформаційно-психологічних операціях це реалізується через відбір і подачу лише тих фактів, які співзвучні з попередніми переконаннями цільової аудиторії, а також через свідоме приховування або дискредитацію будь-яких даних, що суперечать офіційній позиції.

Наприклад, ідея про «зовнішнє управління Україною» постійно підкріплюється цитатами іноземних політиків та експертів, але вирваними з контексту. Це створює враження, ніби наратив повністю підтверджується «незалежними» джерелами, хоча насправді мова йде про маніпуляцію [9].

Ефект якоря - ще одне когнітивне упередження, що активно використовується у пропагандистських повідомленнях. Суть цього ефекту полягає в тому, що початкова інформація (якір) значною мірою впливає на подальше сприйняття та оцінку подій [10]. Російські ІПО нерідко починають інформаційну кампанію з гучної, але часто неперевіреної заяви, яка згодом стає базовою точкою відліку для подальших дискусій. Навіть якщо цю заяву офіційно спростують, перше враження продовжує впливати на інтерпретацію фактів у майбутньому, створюючи ефект «відлуння» [14].

Важливу роль відіграють також моделі стереотипів - спрощені, часто упереджені уявлення про певні групи чи явища, що дозволяють швидко формувати емоційні реакції без глибокого аналізу [15]. У російській пропаганді щодо України стереотипи будуються на історичних міфах,

культурних узагальненнях та політичних кліше. Зокрема, образ «агресивного українського націоналіста» або «нездатної до самостійності держави» використовується для виправдання агресивних дій та мобілізації підтримки серед власного населення [2].

Комбінація цих упереджень дозволяє створювати стійкі наративи, які важко піддаються логічному спростуванню. По-перше, підтверджувальне упередження зменшує ймовірність того, що аудиторія зверне увагу на контраргументи. По-друге, ефект якоря формує вихідну рамку інтерпретації, у межах якої відбувається подальша оцінка інформації. По-третє, стереотипи виконують роль когнітивних «швидких ярликів», які закріплюють образ ворога чи проблеми у масовій свідомості [16].

Особливість російських ІПО полягає в тому, що вони інтегрують ці упередження у багатоетапні інформаційні кампанії, де емоційні подразники чергуються з псевдоаналітичними аргументами. Це створює ефект переконливості через уявний баланс «емоцій» і «логіки» [17]. Такий підхід особливо небезпечний у кризових ситуаціях, коли інформаційне перевантаження та високий рівень стресу знижують когнітивні ресурси аудиторії, роблячи її більш вразливою до маніпуляцій [6].

Отже, використання когнітивних упереджень у російських ІПО проти України є не випадковим, а системним елементом інформаційної війни. Воно базується на міждисциплінарних знаннях з психології, комунікацій та соціальної інженерії, і вимагає від українських фахівців з інформаційної безпеки комплексної стратегії протидії, що поєднує моніторинг, освіту населення та розвиток критичного мислення [1].

1.2. Цифрова трансформація інформаційно-психологічних стратегій

У сучасних інформаційно-психологічних операціях соціальні мережі відіграють надзвичайно важливу роль, виступаючи не лише як платформи для обміну інформацією, але й як інструменти формування громадської думки,

маніпуляції свідомістю та просування політичних наративів. Російсько-український конфлікт демонструє, як ефективно можуть використовуватися цифрові платформи для досягнення стратегічних цілей у сфері інформаційної війни.

Соціальні мережі - це не просто майданчик для спілкування, а складний простор, де переплітаються особистісні сприйняття та соціальний вплив. Вони дозволяють інформації поширюватися миттєво, створюючи ефект «вірусності», що робить їх ідеальним інструментом для інформаційно-психологічних операцій.

Соціальні мережі працюють так, що їхні алгоритми автоматично підбирають контент під уподобання користувача, створюючи своєрідні «інформаційні бульбашки» та ехо-камери. Люди опиняються в середовищі, де бачать переважно ті матеріали, які відповідають їхнім уже сформованим поглядам. Це ще більше закріплює упередження і обмежує доступ до альтернативних думок [7, 13, 18].

Платформа VKontakte (ВК), будучи найбільш популярною серед російськомовної аудиторії, тривалий час була головним каналом для поширення проросійської пропаганди. Завдяки інтеграції з державними медіаресурсами Росії, ця мережа дозволяла централізовано контролювати інформаційні потоки, поширювати фейки, створювати масові кампанії дезінформації та мобілізувати проросійські настрої серед населення як в Україні, так і в інших країнах пострадянського простору [2, 9, 19]. Важливою характеристикою є також активне застосування ботів і фейкових акаунтів для штучного збільшення видимості певних повідомлень, що створює враження масштабності підтримки або суспільного консенсусу.

Telegram став особливо важливим у контексті російсько-українського конфлікту через свою анонімність та низький рівень цензури, що забезпечує швидке та широке поширення інформації. Ця платформа використовується як російськими, так і українськими акторами для оперативного інформування, координації дій і пропаганди. Особливістю Telegram є наявність численних

каналів і чатів, які функціонують як інформаційні вузли, де можуть поширюватися як офіційні повідомлення, так і фейкові новини, що ускладнює розмежування правди і брехні [14, 15, 20].

Twitter (X), хоч і орієнтований здебільшого на міжнародну аудиторію, став важливою платформою для дипломатичних і медійних битв у цифровому просторі. Російські ІПО використовують цю мережу для просування дезінформаційних кампаній, маніпулювання хештегами, створення фальшивих акаунтів і ботнетів, що поширюють проросійські наративи в глобальному масштабі. Відмінність Twitter від інших платформ полягає в більш відкритому і публічному характері обговорень, що вимагає застосування специфічних методів аналітики та реагування на інформаційні загрози [16, 21, 22].

Загалом, роль соціальних мереж у російсько-українському конфлікті є багатогранною. Вони слугують каналами для швидкого поширення інформації, інструментами для таргетованої комунікації та засобами створення альтернативної реальності. Водночас вони породжують низку викликів, пов’язаних з модерацією контенту, виявленням фейків, ідентифікацією ботів та збереженням довіри суспільства. Ці проблеми потребують постійного вдосконалення теоретичних моделей і практичних методів протидії ІПО в цифровому просторі [5, 11, 12].

У контексті російсько-українського конфлікту соціальні мережі не лише виступають засобом поширення інформації, а й перетворюються на поле інтенсивної інформаційної боротьби, де кожен користувач може стати як жертвою, так і учасником інформаційних атак. Психологічний вплив у цьому середовищі підсилюється за рахунок специфіки цифрових платформ, які здатні маніпулювати увагою користувачів, обмежуючи їхню здатність до критичного осмислення інформації. Цей феномен пояснюється зокрема через алгоритмічні механізми ранжування контенту, які націлені на максимізацію часу перебування користувача на платформі за рахунок підсилення емоційно

забарвленого контенту, що часто містить маніпулятивні або провокаційні повідомлення [18].

Значна роль у цьому процесі належить феномену "інформаційного бульбашкового ефекту", коли користувачі отримують інформацію, яка підтверджує їхні попередні переконання, що поглиблює політичні та ідеологічні розбіжності в суспільстві. Російські інформаційні кампанії цілеспрямовано використовують цей механізм для сегментації аудиторій і поширення різнорідних наративів, які послаблюють внутрішню єдність України і посилюють внутрішньополітичну напругу [4, 9, 16]. Це створює передумови для поширення дезінформації, що маскується під альтернативні версії подій, і впливає на сприйняття конфлікту як на рівні локальних спільнот, так і в міжнародному інформаційному просторі.

Особливий виклик становить використання ботнетів і скоординованих мереж фальшивих акаунтів, які не лише розповсюджують пропагандистські меседжі, а й активно атакують критичні голоси, створюючи атмосферу недовіри і хаосу. Ці тактики відповідають моделі "вогняного шлангу неправди" ("firehose of falsehood"), яка характеризується великою кількістю повідомлень з низькою достовірністю, що при цьому подаються з великою швидкістю і без узгодженості, ускладнюючи спростування і розпізнавання фейків [9]. Завдяки цьому механізму дезінформація отримує можливість проникати навіть у добре захищені інформаційні простори, розмиваючи межі між правдою і вигадкою.

Крім того, соціальні мережі стали майданчиком для формування нових інформаційних форматів, таких як меми, відео і короткі повідомлення, що ефективно апелюють до емоцій і формують лояльність або антипатію до певних політичних суб’єктів. Ці формати, завдяки своїй доступності та поширенню, стають потужним інструментом психологічного впливу, особливо серед молоді та користувачів із низьким рівнем критичного мислення [12, 20]. Російські пропагандисти активно використовують ці

інструменти для адаптації традиційних наративів до сучасних цифрових реалій, що робить їх більш переконливими і масовими.

Відповідно, протидія цим викликам вимагає комплексного підходу, який поєднує технологічні рішення, підвищення медіаграмотності та правове регулювання цифрового простору. Україна, реагуючи на загрози, впроваджує механізми виявлення і блокування фейкових акаунтів, розробляє освітні програми з медіаграмотності і активно співпрацює з міжнародними партнерами для обміну аналітикою та координації відповідей на інформаційні атаки [5, 11]. Такий багатогранний підхід сприяє зменшенню впливу російської пропаганди і підвищенню стійкості суспільства до інформаційних загроз.

Інтеграція технологій штучного інтелекту (ШІ) у сучасні інформаційно-психологічні операції стала одним із ключових чинників, що радикально змінюють характер інформаційної війни. З 2013 року, починаючи з ескалації російсько-українського конфлікту, з’явилися нові можливості для масштабного та ефективного впливу на масову свідомість через використання алгоритмів машинного навчання, глибинних нейронних мереж та автоматизованих систем обробки даних. ШІ дозволяє створювати персоналізований контент, автоматизовано генерувати дезінформацію та оптимізувати стратегії поширення повідомлень у соціальних мережах і медіа.

Одним із центральних аспектів застосування ШІ у російських ІПО є автоматизація створення та поширення фейкових новин через ботоферми та фейкові акаунти, які підтримуються алгоритмічними системами. Такі системи здатні аналізувати реакції аудиторії у режимі реального часу і оперативно коригувати контент, підвищуючи ефективність маніпуляції. Завдяки цьому інформаційні атаки можуть охоплювати різні цільові групи, використовуючи персоналізовані наративи, які максимально відповідають психологічним особливостям аудиторії [5, 9, 18].

Крім того, ШІ значно посилює можливості з аналізу великих обсягів даних (big data), що дозволяє виявляти вразливості в інформаційному полі

опонента і формувати цілеспрямовані кампанії впливу. За допомогою алгоритмів глибинного навчання розпізнаються тренди, моделюються поведінкові реакції, що дає змогу гнучко адаптувати тактики інформаційної війни відповідно до динаміки ситуації на фронті інформаційного простору [7, 11].

Важливо зазначити, що використання ШІ у пропагандистських цілях не обмежується лише створенням і поширенням контенту. Сучасні технології також застосовуються для автоматизованого моделювання соціальних мереж і взаємодій у них, що дозволяє створювати штучні “мережеві явища” - наприклад, симульовані групи підтримки або протидії певним ідеям, що підвищує ілюзію масової підтримки чи протесту. Такий підхід сприяє створенню ілюзорної громадської думки, що є важливим інструментом у стратегіях гібридної війни [3, 5].

У поєднанні з традиційними методами дезінформації, зокрема “вогняним шлангом неправди” (firehose of falsehood), застосування ШІ забезпечує новий рівень масштабності і швидкості впливу, що ускладнює ідентифікацію та протидію інформаційним атакам. При цьому автоматизація процесів підсилює ризики поширення недостовірної інформації, оскільки вона може генерувати контент, що суперечить логіці та фактам, але має емоційний резонанс для певних аудиторій [9, 13].

Проте впровадження ШІ відкриває й нові можливості для протидії ІПО. Українські аналітичні центри і міжнародні партнери все активніше використовують штучний інтелект для моніторингу, виявлення та аналізу інформаційних загроз. Застосування інструментів машинного навчання дозволяє автоматизувати виявлення фейкових акаунтів, ботів, а також визначати патерни дезінформації у соціальних мережах. Це сприяє більш оперативній реакції на загрози і формуванню адаптивних стратегій захисту інформаційного простору [5, 11, 22].

Водночас виклики, пов’язані з використанням ШІ в ІПО, залишаються значними. Етичні аспекти автоматизованих інформаційних операцій, ризики

маніпуляцій на основі персональних даних, а також потенціал глибоких фейків (deepfakes) ставлять перед суспільством і державними інституціями необхідність розробки комплексних нормативно-правових та технологічних рішень для мінімізації шкоди від таких загроз [11, 19].

Отже, вплив алгоритмів штучного інтелекту на стратегії інформаційно-психологічних операцій з 2013 року істотно трансформував характер інформаційної війни у російсько-українському конфлікті, підвищивши як ефективність маніпуляцій, так і складність викликів, що стоять перед захистом інформаційного простору.

Розвиток штучного інтелекту у сфері інформаційно-психологічних операцій відкриває нові горизонти для глибшої інтеграції автоматизованих систем у процеси пропаганди та дезінформації. Зокрема, технології машинного навчання і обробки природної мови (NLP) дозволяють не тільки генерувати великі обсяги текстового контенту з імітацією стилю живої людини, але й ефективно адаптувати повідомлення під конкретні аудиторії, враховуючи їхні культурні, політичні та соціальні особливості. Цей рівень персоналізації створює ілюзію довіри і автентичності, що робить такі повідомлення особливо небезпечними в контексті інформаційної війни [23].

Водночас розвиток deepfake-технологій, заснованих на глибинних нейронних мережах, дозволяє створювати реалістичні аудіо- та відеоматеріали з підробленими зображеннями або голосами відомих політиків і публічних осіб. Ці технології здатні кардинально впливати на громадську думку, створюючи фальшиві докази і загострюючи конфлікти. В українському контексті це підсилює загрози інформаційної безпеки, оскільки маніпуляції глибокими фейками можуть розпалювати міжетнічні та внутрішньополітичні суперечності, підриваючи довіру до інституцій держави [24].

Особливої уваги потребує питання етичних меж застосування штучного інтелекту у війнах інформації. Незважаючи на технологічні переваги, відсутність належного регулювання створює ризики масового порушення прав людини, зокрема права на достовірну інформацію і приватність. Саме тому

міжнародна спільнота та науковці активно обговорюють необхідність розробки етичних стандартів і норм, які могли б регламентувати використання ШІ в інформаційно-психологічних операціях, щоб мінімізувати шкоду для цивільного населення [11, 19].

Не менш важливою є роль людського фактору у протидії автоматизованим маніпуляціям. Розвиток медіаграмотності, освіти у сфері цифрової безпеки і критичного мислення стає ключовим напрямом боротьби з дезінформацією, що поширюється за допомогою ШІ. Спільноти, здатні усвідомлювати алгоритмічні пастки і розпізнавати маніпуляції, менш вразливі до інформаційних атак, що робить інвестиції в освіту пріоритетом для держав, що опинилися у зоні гібридних конфліктів [16, 17, 22].

Враховуючи швидкість розвитку штучного інтелекту, стратегічне планування в інформаційній безпеці має враховувати не лише поточні технології, а й прогнозувати появу нових інструментів і методів, які можуть бути використані у наступних хвилях інформаційних конфліктів. Український досвід демонструє важливість комплексного підходу, що поєднує технологічні інновації з міжнародною співпрацею, науковими дослідженнями та громадянською активністю для посилення стійкості суспільства до інформаційних викликів [5, 23].

Отже, інтеграція штучного інтелекту у стратегії інформаційно-психологічних операцій створює нові можливості, але й значно ускладнює процеси ідентифікації та протидії дезінформації, вимагаючи від держав і суспільств адаптивності та постійного оновлення методів захисту інформаційного простору.

Зміна парадигми інформаційно-психологічних операцій у російсько-українському конфлікті від масового впливу до персоналізованих стратегій є відображенням загальних тенденцій розвитку інформаційних технологій та комунікаційних практик. Таргетинг у контексті ІПО розглядається як процес вибору та адресного впливу на конкретні соціальні групи, індивідів або навіть окремі особистості з метою формування або зміни їхньої свідомості, поведінки

та політичних установок. Цей перехід від широкомасштабних меседжів до тонко налаштованих комунікацій значно підвищує ефективність пропаганди і маніпуляції [1, 9].

Основою для персоналізації інформаційного впливу є збір, обробка та аналіз великих масивів даних про поведінку користувачів, їхні інтереси, соціальні зв'язки і навіть психологічні профілі. У випадку російських ІПО проти України це дозволяє створювати диференційовані наративи, які враховують регіональні, мовні, культурні і політичні особливості аудиторій. Наприклад, меседжі, спрямовані на проросійськи налаштовані групи населення, містять апеляції до історичних міфів та ностальгії за радянським минулим, тоді як для більш проєвропейськи орієнтованих користувачів використовуються наративи про нестабільність і загрози від західних партнерів [4, 8].

Теоретичні моделі таргетингу базуються на міждисциплінарних підходах, що поєднують елементи соціальної психології, комунікаційної теорії та аналізу поведінкових патернів. Соціальна ідентичність, як описано у теорії Таджфеля і Тьорнера, є важливою категорією, що дозволяє зрозуміти, яким чином формуються групові упередження та конфлікти, а також як вони можуть бути використані для сегментації аудиторії і підсилення внутрішніх протиріч у суспільстві [8].

Персоналізований таргетинг у цифровому середовищі реалізується за допомогою алгоритмів соціальних мереж, які дозволяють не лише сегментувати аудиторію, а й активно впливати на її інформаційне поле, формуючи "інформаційні бульбашки", де користувачі переважно контактують із контентом, що підтверджує їхні вже існуючі переконання. Цей механізм використовується у російських інформаційних операціях для послаблення суспільної згуртованості України, стимулювання політичних конфліктів і створення ворожнечі між різними соціальними групами [9, 16].

Водночас, таргетинг дозволяє більш ефективно керувати інформаційними потоками, знижуючи ризик розпорошення ресурсів і збільшуючи вплив

конкретних повідомлень. Це забезпечує можливість здійснювати як масштабні кампанії, так і точкові операції, спрямовані на вузькі аудиторії - наприклад, військовослужбовців, волонтерів або внутрішньо переміщених осіб. Така диференціація підсилює стійкість ІПО до протидії, оскільки вимагає від захисних структур більш гнучких та комплексних підходів [3, 5].

Важливо підкреслити, що персоналізація інформаційного впливу не виключає застосування масових методів, а скоріше доповнює їх, створюючи багаторівневу систему маніпуляцій, що працює одночасно на різних аудиторіях і з різною глибиною проникнення. Це поєднання дозволяє Росії ефективно реалізовувати стратегії гібридної війни, використовуючи весь спектр інформаційних інструментів від широкомасштабної пропаганди до індивідуалізованих психологічних впливів [3, 9].

Персоналізація впливу в інформаційно-психологічних операціях не лише підсилює ефективність комунікації, а й ускладнює завдання протидії таким маніпуляціям. Традиційні методи інформаційної безпеки, які орієнтовані на масові канали поширення інформації, часто виявляються недостатніми для виявлення і нейтралізації тонко адресованих повідомлень, що адаптовані під індивідуальні особливості аудиторії. Це зумовлює необхідність розвитку нових аналітичних інструментів, здатних працювати з великою кількістю різнорідних даних та виявляти патерни персоналізованих атак. Зокрема, актуальним є впровадження методів штучного інтелекту і машинного навчання для автоматичного моніторингу соціальних мереж, аналізу поведінки користувачів і прогнозування поширення дезінформації [9, 23].

Паралельно, інтенсивне застосування таргетованої пропаганди стимулює появу “інформаційних мікросвітів” - ізольованих груп або комунікативних середовищ, де панують специфічні наративи, часто взаємовиключні і конфліктні між собою. Ця фрагментація інформаційного простору значною мірою послаблює суспільний консенсус і ускладнює формування єдиної позиції щодо внутрішньополітичних та зовнішньополітичних викликів. Саме

це явище активно експлуатується у гібридній війні, зокрема через стимулювання внутрішніх розколів і конфліктів у суспільстві [4, 8, 16].

Водночас, специфіка цифрового середовища, де реалізуються ці моделі, створює значні проблеми з ідентифікацією джерел дезінформації і відстеженням ланцюгів розповсюдження повідомлень. Використання анонімних акаунтів, ботів та автоматизованих мереж дозволяє організаторам інформаційних операцій уникати відповідальності і маніпулювати громадською думкою у великому масштабі. Це вимагає від державних структур і міжнародної спільноти розробки нових підходів до верифікації інформації, регулювання цифрових платформ та координації дій у сфері інформаційної безпеки [5, 9, 22].

Крім того, таргетовані ІПО активно використовують психологічні особливості цільових аудиторій, зокрема когнітивні упередження, які призводять до стійкості певних переконань навіть у разі наявності протилежних фактів. Ефект підтверджувального упередження, ефект якоря, стереотипізація - це лише деякі з механізмів, що допомагають підтримувати сформовані наративи і підвищують резистентність аудиторії до контраргументів. Врахування цих психологічних факторів у процесі розробки таргетованих повідомлень значно підвищує їхню сприйнятливість і впливовість [16, 17].

Це, у свою чергу, обумовлює необхідність формування в українському суспільстві стійкості до маніпуляцій на основі підвищення рівня медіаграмотності, розвитку критичного мислення та поширення знань про механізми когнітивних упереджень. Водночас важливою є і технологічна складова, що полягає у впровадженні сучасних інструментів виявлення й протидії таргетованим інформаційним атакам у цифровому просторі [16, 17, 22].

Як результат, персоналізація в російських ІПО виступає як потужний інструмент не лише для поширення пропаганди, але й для формування розділеної, фрагментованої інформаційної реальності, що посилює розкол у

суспільстві та ускладнює побудову ефективної системи національного інформаційного захисту.

1.3. Еволюція російських інформаційних операцій: синтез класичних та новітніх методів впливу

Класичні методи пропаганди, що сформувалися в радянську епоху, залишаються фундаментальними складовими сучасних російських інформаційно-психологічних операцій (ІПО). Радянська пропаганда базувалася на чітко структурованих наративах, що використовували ідеологічні меседжі для консолідації суспільства, деморалізації ворога та зміцнення влади. Ці методи включали маніпуляції через централізовані ЗМІ, широке застосування цензури, створення ворогів і героїв, а також використання емоційно забарвлених образів і символів, що мали викликати у аудиторії чітку емоційну реакцію [2, 5].

Після розпаду СРСР радянські традиції пропаганди не зникли, а були адаптовані під нові політичні та технологічні умови. У сучасних російських ІПО вони поєднуються з цифровими технологіями, що дозволяють значно розширити аудиторію і посилити вплив. Проте в основі лежать ті ж принципи - контроль над інформацією, формування образу ворога, акцент на патріотизм і захист «традиційних цінностей». Це створює своєрідну інформаційну спадщину, що підтримує державну ідеологію і мобілізує населення в умовах конфлікту [3, 5].

Зокрема, техніки радянської пропаганди, такі як повторення ключових меседжів, створення інформаційних «підвалів» (fake news), використання маніпулятивної риторики та залякування, продовжують використовуватися у поєднанні з новітніми технологіями і соціальними мережами. Цей симбіоз класичних методів і сучасних цифрових інструментів дозволяє Росії формувати глибоко вкорінені наративи, які важко спростувати, особливо в регіонах із обмеженим доступом до альтернативних джерел інформації [4, 9].

Адаптація радянських методів також проявляється у використанні «інформаційних бульбашок» та алгоритмічної цензури, які сприяють ізоляції аудиторії від контраргументів і зміцнюють її віру в офіційні наративи. Цей підхід дозволяє створити інформаційний простір, де альтернативні точки зору фактично недоступні, що істотно посилює ефективність пропаганди [11, 18].

Глобалізація інформаційного поля суттєво ускладнює традиційні межі інформаційно-психологічних операцій, перетворюючи їх на багатовекторні кампанії, що охоплюють не лише внутрішню аудиторію Росії та України, а й широкий спектр міжнародних акторів - від окремих громадян до урядових інституцій та транснаціональних організацій. У цьому контексті російські ІПО стають інструментом не лише національної, але й глобальної політики впливу, спрямованої на послаблення позицій Західного блоку і розширення геополітичного впливу Москви через інформаційні канали [2, 5].

Аналіз медіапростору показує, що в умовах цифрової глобалізації Росія активно адаптує свої наративи відповідно до культурних, соціальних та політичних особливостей різних регіонів світу. Це реалізується через локалізовані медіакампанії, які націлені на підсилення розколів у суспільствах інших країн, сприяючи підриву довіри до демократичних інститутів та підтримки проросійських політичних сил. Такий підхід ґрунтується на глибокому аналізі цільових аудиторій, що дозволяє підбирати найбільш ефективні меседжі для різних культурних контекстів [7, 9, 23].

У зв’язку з цим особливе значення набувають цифрові платформи, які, завдяки своїй універсальності та швидкості поширення інформації, слугують ключовими артеріями для реалізації цих стратегій. Соціальні мережі і месенджери дозволяють оперативно змінювати та адаптувати інформаційні потоки, одночасно поширюючи як офіційні пропагандистські меседжі, так і дезінформацію, фейки та маніпулятивний контент, що викликає соціальну дезорієнтацію і посилює конфліктні настрої [4, 22].

Особливої уваги заслуговує використання алгоритмічних систем штучного інтелекту, які автоматизують процес сегментації аудиторії та

таргетування повідомлень. Ці технології дозволяють створювати персоналізований вплив, що значно підвищує ефективність ІПО, оскільки повідомлення формуються з урахуванням індивідуальних психологічних особливостей, інтересів та переконань конкретних груп або навіть окремих осіб [22, 23].

Міжнародна аудиторія, з якою працюють російські ІПО, відрізняється високим рівнем інформаційної насиченості, що ставить перед Москвою завдання не лише поширювати власні наративи, а й протистояти конкуренції за увагу, а також подолати зростаючу критичність і скептицизм серед користувачів інформаційного простору. Для цього в інформаційних кампаніях активно використовуються елементи психологічної маніпуляції, емоційного забарвлення контенту і техніки «вогневого шланга брехні», що дозволяють одночасно поширювати численні суперечливі повідомлення для створення плутанини і інформаційного хаосу [9, 13].

Враховуючи всі ці фактори, аналіз російських ІПО у глобальному інформаційному просторі демонструє не лише складність і багатошаровість застосовуваних методів, а й потребу для України та її міжнародних партнерів у розробці комплексних стратегій протидії, що включають посилення кібербезпеки, розвиток медіаграмотності, створення альтернативних джерел правдивої інформації та координацію міжнародних зусиль з протидії дезінформації [5, 22].

Інтеграція дезінформації та наративного будівництва у російських інформаційно-психологічних операціях (ІПО) проти України ґрунтується на складній системі взаємопов’язаних теоретичних основ, які формують ефективний інструментарій для створення та поширення фейкових новин. Важливо розуміти, що фейкові новини - це не просто неправдива інформація, а цілеспрямований продукт, що формує альтернативну реальність через систематичне маніпулювання свідомістю цільових аудиторій. Цей процес опирається на глибокі психологічні та соціальні механізми, зокрема моделі

когнітивного сприйняття, теорії рамування (фреймінгу) та міжгрупової ідентичності [4, 7, 8].

Ключовим компонентом є техніка «вогневого шланга брехні» (firehose of falsehood), яку детально описали дослідники, що підкреслює одночасне і надмірне поширення численних суперечливих повідомлень із метою заплутати аудиторію, зруйнувати довіру до традиційних джерел інформації та посіяти скептицизм. Це створює інформаційний хаос, у якому споживачі інформації не здатні критично відрізнити правду від вигадки, що сприяє впровадженню вигідних для агресора наративів [9, 5].

Процес наративного будівництва базується також на соціально-психологічних теоріях, зокрема теорії соціальної ідентичності, яка пояснює, як інформаційні кампанії формують «ми» проти «вони», підсилюючи конфліктні установки і виправдовуючи агресивні дії. Російська пропаганда майстерно використовує стереотипи, упередження і емоційно забарвлені меседжі, щоб активізувати відчуття загрози, страху та національної неповноцінності у цільових групах, що дає їй змогу маніпулювати суспільною думкою з високою ефективністю [8, 12, 13].

У цьому контексті когнітивні упередження, такі як підтверджувальне упередження, ефект якоря та евристики прийняття рішень, грають вирішальну роль у сприйнятті та поширенні дезінформації. Люди схильні сприймати інформацію, що відповідає їхнім вже існуючим переконанням, і відкидати контраргументи, що значно ускладнює боротьбу з фейковими новинами. Це використовується у стратегіях маніпуляції, де розповсюджуються адаптовані повідомлення, які підсилюють існуючі стереотипи або страхи, перетворюючи їх у потужний інструмент психологічного впливу [10, 13, 16].

Окрім цього, активне використання методів рамування дозволяє формувати сприйняття подій у вигідному для агресора ключі, підкреслюючи певні аспекти інформації та ігноруючи або применшуючи інші. Такий підхід сприяє створенню стійких наративів, які навіть при викритті як неправдиві,

можуть мати тривалий вплив на суспільну свідомість, через що боротьба з ними вимагає комплексних і системних заходів [7, 4].

Враховуючи все це, інтеграція дезінформації у наративне будівництво є не випадковим явищем, а ретельно продуманою стратегією, яка поєднує класичні психологічні прийоми, сучасні технології масової комунікації та специфічні особливості інформаційної війни, що ведеться у контексті російсько-українського конфлікту.

Висновки до розділу 1

Отже, у першому розділі було досліджено про стратегії які ґрунтуються на глибокому розумінні психології мас та ефективно використовують когнітивні упередження, такі як підтверджувальне упередження, ефект якоря та евристики прийняття рішень, що забезпечує високу ефективність дезінформаційних кампаній. Наприклад, створення та поширення фейкових новин, що підтверджують існуючі стереотипи або страхи, значно підвищує їх сприйняття та довіру серед цільової аудиторії.

З початком повномасштабного вторгнення в 2022 році Росія значно посилила використання цифрових платформ для поширення пропаганди. Соціальні мережі, такі як Telegram, стали основними каналами для розповсюдження маніпулятивних наративів, включаючи фейкові новини, пропагандистські відео та аудіо матеріали, що мають на меті дестабілізувати ситуацію в Україні та посіяти сумніви серед міжнародної спільноти. Використання бот-мереж та автоматизованих акаунтів дозволяє значно збільшити охоплення та ефективність цих кампаній, створюючи ілюзію масової підтримки або протесту.

Особливу увагу слід приділити використанню технологій штучного інтелекту та автоматизованих систем для створення та поширення дезінформації. Наприклад, кампанія "Matryoshka" використовує безкоштовні інструменти штучного інтелекту для створення великої кількості фейкових

медіа, включаючи deepfake відео та зображення, що мають на меті посилити розбіжності в суспільствах Заходу та підірвати підтримку України. Ці технології дозволяють створювати високоякісні маніпуляції, що важко відрізнити від реальних матеріалів, що ускладнює завдання з протидії таким кампаніям.

Також важливим аспектом є використання історичних наративів та культурних стереотипів для формування бажаного сприйняття подій. Російська пропаганда активно експлуатує образи "фашистів" та "нацистів" в Україні, намагаючись створити образ ворога, що виправдовує агресію та окупацію. Ці наративи мають глибоке коріння в історичній пам'яті та культурних уявленнях, що робить їх особливо ефективними в маніпулюванні громадською думкою.

У відповідь на ці загрози Україна розробила та впровадила ряд стратегій та інструментів для протидії інформаційним атакам. Одним з таких кроків стало створення платформи "Потерь.НЕТ", що використовує технології розпізнавання облич для ідентифікації загиблих російських військових, з метою підвищення прозорості та інформування громадськості про реальні втрати. Однак використання таких технологій викликає етичні питання та потребує ретельного балансу між ефективністю та дотриманням прав людини.

Крім того, Україна активно співпрацює з міжнародними партнерами для обміну інформацією та ресурсами, що дозволяє більш ефективно виявляти та нейтралізувати дезінформаційні кампанії. Спільні зусилля в галузі кібербезпеки, моніторингу медіа та освіти з медіаграмотності сприяють підвищенню стійкості суспільства до маніпуляцій та фейкових новин.

Загалом, інформаційно-психологічні операції Росії проти України демонструють високий рівень організації та інтеграції різноманітних інструментів впливу, що поєднують психологічні, технологічні та соціальні аспекти. Врахування цих факторів є критично важливим для розробки ефективних стратегій протидії та захисту національного інформаційного простору. Розуміння глибинних механізмів інформаційно-психологічного

впливу дозволяє створювати більш ефективні заходи протидії сучасним гібридним загрозам, зміцнюючи національну безпеку в умовах сучасних викликів інформаційної війни.

РОЗДІЛ 2. ПРАКТИЧНІ АСПЕКТИ РОСІЙСЬКИХ ІНФОРМАЦІЙНО-ПСИХОЛОГІЧНИХ ОПЕРАЦІЙ У КОНТЕКСТІ КОНФЛІКТУ З УКРАЇНОЮ (2013-2025 РР.)

2.1. Інформаційний супровід ключових подій в Україні: кейс Євромайдану

Початок протестів в Україні у 2013 році став своєрідним каталізатором масового застосування Росією нових моделей інформаційно-психологічного впливу, які поєднували класичні елементи радянської пропаганди з цифровими технологіями та сучасними методами маніпуляції громадською думкою. На цьому етапі російські медіа активно формували наративи, які мали на меті дискредитувати протестуючих, демонізувати українські політичні структури та створювати образ України як нестабільної та некерованої держави. Головними каналами поширення цих наративів виступали як традиційні ЗМІ (телебачення, друковані видання), так і соціальні мережі, зокрема VKontakte та Twitter/X, які дозволяли швидко масштабувати інформацію та досягати як внутрішньої, так і міжнародної аудиторії [2; 4; 9].

Російські інформаційні кампанії активно використовували когнітивні упередження та психологічні механізми, такі як ефект підтвердження, стереотипізація та формування групової ідентичності. Наприклад, образ протестувальників у медійному просторі подавався як загроза «традиційним цінностям» та «порядку», що апелювало до страхів і упереджень частини аудиторії та створювало ефект соціальної дистанції між «своїми» і «чужими» [8; 16]. Використання так званого «вогнепровідного потоку неправдивої інформації» (firehose of falsehood) дозволяло одночасно поширювати суперечливі меседжі та зменшувати критичне сприйняття аудиторії, створюючи інформаційний хаос і підвищуючи емоційну реакцію на події [9].

Одним із ключових аспектів російської стратегії стала інтеграція цифрових інструментів, зокрема ботів та автоматизованих акаунтів у

соціальних мережах, які координовано поширювали меседжі та створювали ілюзію масової підтримки певних наративів. Ці дії дозволяли формувати тенденції обговорень у мережі, надавати інформаційну підтримку офіційній пропаганді та впливати на міжнародну думку [21; 22]. На міжнародній арені використовувалися більш «м'які» наративи, що підкреслювали нестабільність України, корумпованість влади та загрозу «антидемократичних сил», що давало підстави виправдовувати політику Росії у вигляді «захисту російськомовного населення» або «регулювання конфліктів у сусідній країні» [3; 5].

Важливо також підкреслити роль наративного фреймінгу у створенні образу ворога та легітимізації власних дій. Використовуючи принципи фреймінгу, Росія змінювала акценти, підкреслюючи хаотичність протестів, насильство та нібито екстремістські тенденції серед активістів, що одночасно виправдовувало зовнішнє втручання та формувало образ «захисника порядку» [7; 18]. Такий підхід дозволяв інформаційно впливати на різні групи аудиторії, використовуючи як раціональні аргументи, так і емоційні тригери.

У результаті формування цих наративів виникла складна система інформаційного супроводу протестів, яка об'єднувала класичні пропагандистські техніки, психологічні маніпуляції та цифрові інструменти. Це створило середовище, де громадська думка формувалася під сильним впливом когнітивних упереджень і повторюваних повідомлень, а критичне мислення аудиторії було значно ускладнене [4; 10; 12; 16]. Цей досвід пізніше став базою для розробки подальших інформаційно-психологічних операцій проти України, де ключовим інструментом залишалася системна координація наративів, цифрових платформ та автоматизованих розповсюджувачів, що забезпечувало масштабованість і ефективність впливу.

Протести на Майдані у 2013-2014 роках стали не лише політичним, а й інформаційним феноменом, що одразу привернув увагу Росії як суб'єкта, зацікавленого в контролі наративу. У медіапросторі РФ активно формувалися ключові наративи, спрямовані на делегітимізацію протестів та створення

образу України як нестабільної та неконтрольованої держави [2; 4; 5]. Основні тези російської пропаганди включали твердження про «неонацизм і радикалізм» серед учасників протестів, «захоплення влади радикалами під прикриттям Заходу» та «загрозу російськомовному населенню», що формувалися через систематичне поєднання реальних подій із маніпулятивними коментарями та перекрученими фактами [3; 9; 18].

Соціальні мережі стали основним майданчиком для поширення цих наративів. Платформи, такі як ВКонтакте, Facebook, Twitter/X і особливо Telegram, використовувалися для швидкої дистрибуції матеріалів, створення груп підтримки проросійських позицій та координованих атак на українські інформаційні ресурси [1; 4; 21]. Високий рівень інтерактивності дозволяв маніпулювати емоційними реакціями користувачів, поширювати меми, фото та відео з «потрібним» контекстом, що значно підвищувало ефект психологічного впливу на масову аудиторію. Додатково використовувалися технології «фейкового контенту», коли створювалися акаунти ботів, що масово поширювали одну й ту саму інформацію, створюючи ілюзію широкої підтримки проросійських поглядів [9; 22; 23].

Особливе значення мала так звана «психологічна робота» через традиційні медіа. Телебачення та новинні портали РФ формували хронологічні наративи, де події на Майдані подавалися через призму загрози державному устрою України та «екстремістської діяльності Заходу». Такі матеріали супроводжувалися емоційно забарвленими коментарями, які апелювали до страху, гніву та почуття загрози [6; 7; 12]. За допомогою комбінованого використання цифрових і класичних каналів пропаганди Росія прагнула не лише вплинути на українське суспільство, але й сформувати вигідний міжнародний наратив про «зовнішню загрозу», що дозволяло легітимізувати подальші політичні і військові дії [5; 9].

Психологічний вплив базувався на застосуванні когнітивних упереджень та соціальних механізмів. Ефект підтверджувального упередження, коли користувачі схильні шукати інформацію, що підтверджує їхні існуючі

погляди, активно експлуатувався у російських ІПО. Водночас використовувалися соціальні ідентичності, створюючи «ми проти них», що підсилювало поляризацію суспільства і формувало стійкі негативні установки щодо протестуючих [8; 14; 16].

У відповідь на активне використання Росією інформаційно-психологічних операцій під час Євромайдану українські державні та громадські структури почали формувати власні контрнаративи, спрямовані на нейтралізацію дезінформації та захист національної інформаційної безпеки. Одним із перших кроків стало створення офіційних інформаційних платформ і каналів комунікації, що надавали перевірені дані про події на місцях, спростовували фейкові повідомлення та пояснювали політичний контекст протестів [2; 4; 21]. Ці ініціативи поєднували класичні методи інформаційної роботи, такі як прес-релізи та офіційні заяви, із цифровими каналами - зокрема соціальними мережами та месенджерами, що дозволяло швидко поширювати правдиву інформацію серед різних груп аудиторії.

Ключовим інструментом протидії стала розбудова системи фактчекінгу, що включала незалежні медіа, громадські організації та онлайн-платформи для перевірки достовірності новин. Такий підхід дозволяв не лише зменшувати ефект «вогнепровідного потоку неправдивої інформації», який активно застосовувала Росія, а й формувати критичне мислення користувачів, навчати їх відокремлювати перевірені повідомлення від маніпулятивних [17; 22].

Особливу роль у протидії дезінформації відігравали контрнаративи, які акцентували на спільних цінностях, національній ідентичності та демократичних процесах, що дозволяло зменшувати ефект когнітивних упереджень, створених російською пропагандою. Використання фреймінгу в українських контрнаративах полягало у зміні акцентів: замість хаосу та насильства підкреслювалася мирна природа протестів, прагнення громадян до реформ та захист демократичних прав [7; 18].

Важливим аспектом протидії була координація між державними органами, громадськими ініціативами та міжнародними партнерами, що

дозволяло оперативно реагувати на нові хвилі дезінформації. Масштабні кампанії, спрямовані на роз'яснення подій на міжнародній арені, включали мультимедійні матеріали, англомовні публікації та участь українських експертів у закордонних медіа, що зменшувало можливості Росії формувати однобокий образ України на світовій сцені [3; 5; 21].

Паралельно активно застосовувалися цифрові інструменти для виявлення та блокування бот-мереж та автоматизованих акаунтів, що поширювали дезінформацію, а також аналітичні методи для моніторингу інформаційного простору. Це включало відстеження тенденцій у соцмережах, виявлення ключових наративів і їх джерел, що дозволяло більш ефективно формувати протидієві повідомлення та швидко реагувати на нові інформаційні атаки [9; 21; 22].

Комплексна стратегія протидії російським ІПО під час Євромайдану стала основою для подальших практичних підходів у сфері національної інформаційної безпеки, демонструючи, що ефективна боротьба з дезінформацією потребує одночасного використання технологічних рішень, аналітики контенту, психологічних методів впливу та міжнародної комунікації, а також постійного моніторингу інформаційного середовища, що безпосередньо впливає на подальші методи і стратегії російських ІПО в українському контексті.

Такий комплексний підхід до протидії російській пропаганді під час Євромайдану продемонстрував необхідність постійного моніторингу та адаптації контрнаративів до швидко змінюваних умов інформаційного середовища. Українські організації не лише відстежували нові хвилі дезінформації, а й аналізували способи формування та поширення ключових наративів, що дозволяло прогнозувати дії противника і заздалегідь готувати відповідні інформаційні відповіді. Значну роль відіграла сегментація аудиторії, що дозволяла розробляти таргетовані повідомлення для різних груп громадян, враховуючи їхні інформаційні звички, соціальні вподобання та рівень довіри до різних джерел [9; 21].

Крім того, українські ініціативи активно інтегрували мультиплатформені рішення: одночасне використання традиційних медіа, соціальних мереж та месенджерів дозволяло створювати «інформаційні ланцюги», де перевірена інформація швидко поширювалася і знаходила аудиторію до того, як фейкові наративи отримували значне охоплення. Такий підхід не лише підвищував оперативність реакції на інформаційні атаки, а й формував у громадян стійкішу когнітивну базу для критичного аналізу новин, знижуючи ефективність маніпулятивних технік, що застосовувалися Росією [17; 22].

Особливу увагу приділяли міжнародній комунікації та взаємодії з іноземними медіа, адже російські наративи активно спрямовувалися на світову аудиторію з метою дискредитації українських протестів та легітимізації зовнішньої агресії. Підготовка англомовних матеріалів, участь експертів у закордонних медіа та просування української позиції у глобальному інформаційному полі дозволяли не лише спростовувати фейки, але й формувати позитивний образ України як країни, що відстоює демократичні цінності та права громадян [3; 5; 21].

На цьому етапі критично важливим стало використання аналітичних методів для відстеження поведінки інформаційних агентів противника: визначення ключових джерел пропаганди, виявлення бот-мереж та вивчення механізмів поширення наративів. Це дозволяло не просто реагувати на вже існуючу дезінформацію, а й проактивно будувати контрнаративи, формуючи інформаційний простір Отже, щоб громадяни отримували достовірну інформацію першими [9; 22].

Під час Євромайдану українська інформаційна протидія набула нових, комплексних форм, що поєднували технологічні інструменти, психологічні механізми впливу, аналітичну роботу та міжнародну комунікацію. Такий підхід дозволив не лише ефективно протистояти поширенню російських наративів, але й активно формувати позитивний імідж України на глобальній арені, демонструючи здатність держави відстоювати демократичні цінності та права громадян.

Особливу увагу було приділено міжнародній комунікації та взаємодії з іноземними медіа, оскільки російські наративи активно спрямовувалися на світову аудиторію з метою дискредитації українських протестів та легітимізації зовнішньої агресії. Українська сторона відповідала створенням англомовних матеріалів, залученням експертів у закордонних медіа та просуванням української позиції в глобальному інформаційному просторі. Це дозволяло не лише спростовувати фейки, але й активно формувати позитивне сприйняття України, підкреслюючи її як державу, що відстоює принципи демократії та верховенства права [38; 39].

Важливим аспектом стало застосування аналітичних методів для відстеження поведінки інформаційних агентів противника. Це включало ідентифікацію основних джерел пропаганди, виявлення бот-мереж та вивчення механізмів поширення наративів. Подібні дослідження давали змогу не лише реагувати на вже наявну дезінформацію, але й проактивно формувати контрнаративи, забезпечуючи своєчасне інформування громадян та зміцнення їхньої стійкості до маніпуляцій[40].

Застосування нових технологій, зокрема алгоритмів штучного інтелекту та цифрових інструментів аналізу інформації, стало ключовим фактором для підвищення ефективності інформаційних стратегій. Використання таких методів дозволяло відстежувати тенденції поширення наративів, виявляти потенційні загрози та формувати оперативні контрзаходи[41]. Крім того, розвиток цифрових платформ дав змогу українській стороні не лише реагувати на фейки, а й створювати власні комунікаційні продукти, що посилювало позицію держави на міжнародній сцені.

Досвід Євромайдану став основою для формування нових стандартів інформаційної протидії. Він показав, що лише комплексний підхід, який поєднує технології, психологічні методи впливу, аналітичні інструменти та міжнародну комунікацію, здатен ефективно протидіяти сучасним інформаційно-психологічним операціям. Цей досвід підкреслив необхідність постійного розвитку адаптивних моделей, здатних реагувати на динамічні та

багаторівневі загрози, а також активно формувати інформаційний простір, що зміцнює національну безпеку та міжнародний імідж України.

Водночас, для досягнення максимального ефекту, пропагандистські кампанії поєднували кілька стратегічних підходів: розповсюдження спрощених історій, що апелювали до емоцій, використання «псевдоекспертів» та маніпулятивних статистичних даних, а також створення штучних протиріч між різними внутрішніми групами України. Ці техніки дозволяли формувати когнітивні упередження, збільшувати рівень недовіри до українських інституцій і створювати відчуття хаосу та нестабільності, що відповідало загальній меті дезінформаційної кампанії [4; 9; 16].

Для протидії таким стратегіям Україна розширювала цифровий моніторинг і аналітичні можливості: здійснювалося відстеження ключових наративів, визначення їхніх джерел та виявлення структур ботів і автоматизованих акаунтів. Паралельно розроблялися спеціалізовані контркампанії у соцмережах та месенджерах, які не тільки спростовували фейкові повідомлення, але й надавали детальне тлумачення подій на Донбасі, підкреслюючи зовнішню природу конфлікту та позицію України у захисті власних територіальних цілісностей [17; 21; 22].

Зокрема, широко використовувалися соціальні мережі, месенджери та спеціалізовані платформи для поширення спотворених новин і «альтернативних фактів», які формували однорідний наратив, що підтримував легітимізацію дій Росії в очах міжнародної аудиторії. Такі кампанії поєднували одночасно масове охоплення та таргетований вплив на конкретні групи користувачів, створюючи ефект «інформаційного водоспаду», коли одна й та ж подія подавалася в різних контекстах та формах [9; 21; 23].

Ключовим елементом цих операцій стало активне використання бот-мереж та автоматизованих акаунтів для створення штучної підтримки певних наративів, що підсилювало видимість «популярної думки» і впливало на сприйняття користувачів через соціальні докази. Одночасно поширювалися маніпулятивні медіа-матеріали, включно з відео, фото та графіками, які

підкріплювали фейки та підсилювали емоційний вплив, апелюючи до страху, обурення або симпатії [2; 4; 17].

Відповіддю України стала побудова багаторівневої системи протидії: державні та громадські структури створювали аналітичні центри та цифрові платформи для моніторингу інформаційного простору, відстеження тенденцій у соцмережах та ідентифікації ключових джерел дезінформації. Особливу увагу приділяли розробці контрнаративів, які підкреслювали законність українських дій, зовнішній характер агресії та цінність демократичних процесів, одночасно застосовуючи принципи фреймінгу для зміщення акцентів із негативних або провокативних сюжетів на факти та аналітику [7; 18; 21].

Паралельно велика увага приділялася міжнародному аспекту: українські медіа та експертні спільноти активно інформували західну аудиторію, готували англомовні матеріали, проводили брифінги та коментарі для закордонних ЗМІ. Ці дії дозволяли зменшити ефект односторонньої пропаганди та формувати більш об’єктивне розуміння конфлікту, одночасно створюючи механізми для стратегічного комунікаційного впливу у глобальному інформаційному просторі [3; 5; 22].

У випадку з Донбасом інформаційна стратегія Росії виявилася ще більш багатошаровою та цілеспрямованою. Якщо в Криму головний акцент робився на «праві народу на самовизначення» та «історичній справедливості», то в східних регіонах України пропаганда активно просувала ідею «громадянської війни» та «народного повстання проти хунти». Одним із найчастіших наративів було твердження про те, що Київ застосовує зброю проти «мирних жителів Донбасу», хоча фактично мова йшла про антитерористичну операцію проти озброєних формувань, які отримували постачання та підтримку з боку Росії [7][10]. Це дозволяло Москві позиціонувати себе як «захисника мирного населення», одночасно приховуючи свою пряму військову участь.

Особливу роль відігравали сюжети російських телеканалів, які часто містили емоційні маніпуляції: кадри зруйнованих будинків, кадри плачучих

жінок та дітей, що змушені були залишати свої домівки. Такі матеріали майже завжди супроводжувалися коментарями, які звинувачували українську армію у «каральних операціях». Водночас докази про участь російських військових у бойових діях систематично замовчувалися або пояснювалися як «добровольча допомога». Ця дезінформаційна стратегія сприяла створенню викривленої картини конфлікту, в якій Україна виставлялася агресором, а Росія - миротворцем [4][8][12].

Окрім телебачення, активно використовувалися соціальні мережі та інтернет-платформи, де поширювалися фейкові новини про «масові вбивства російськомовних», «розп'ятих дітей» та інші вигадані події, що викликали широкий резонанс серед аудиторії. Такі вкиди мали на меті не лише мобілізувати підтримку серед громадян Росії, а й посіяти страх та паніку серед населення України. Важливо, що частина цих матеріалів була спрямована й на західну аудиторію, де Кремль намагався довести легітимність своїх дій, представляючи їх як «гуманітарну допомогу» або «захист цивільних».

2.2. Інформаційно-психологічні операції Росії у 2015-2021 роках

У період з 2015 по 2021 роки російська пропаганда посилила свої зусилля з формування наративу про Україну як про так звану «failed state» - державу, яка нібито не здатна ефективно функціонувати, забезпечувати базові потреби громадян та гарантувати стабільність на міжнародній арені. Цей образ системно просувався у російських медіа, дипломатичних заявах, експертних публікаціях та через соціальні мережі. Основна мета полягала в тому, щоб підірвати міжнародний авторитет України, викликати у партнерів сумніви щодо доцільності підтримки Києва та представити Росію як нібито стабільного актора, здатного диктувати правила в регіоні [3; 7; 11].

Ключові компоненти цього наративу включали постійне підкреслення нібито «економічної неспроможності» України, що підкріплювалося маніпулятивними посиланнями на зростання зовнішнього боргу, зниження

рівня промислового виробництва та міграційні процеси. Російські ЗМІ активно поширювали тези про «повну залежність Києва від Заходу», намагаючись створити враження, що українська влада не має власного суверенного курсу, а всі її рішення нібито продиктовані Сполученими Штатами чи Європейським Союзом [2; 8].

Не менш важливим аспектом було акцентування уваги на внутрішньополітичних конфліктах в Україні. Російська інформаційна машина намагалася представити будь-які протести, зміни уряду чи політичні суперечки як ознаку «хаосу» та «недієздатності держави». Наприклад, під час обговорення реформ 2015-2016 років у російських медіа систематично з'являлися твердження про «провал децентралізації», «корупцію в усіх сферах влади» та «занепад державних інститутів» [4; 10].

У міжнародному вимірі цей наратив активно просувався через англомовні ресурси, такі як RT та Sputnik, які поширювали дезінформаційні матеріали про «гуманітарну катастрофу» в Україні. Систематичне наголошення на нібито «масовому від'їзді населення», «енергетичній кризі» чи «відсутності верховенства права» мало сформувати у світової аудиторії уявлення, що Україна не є повноцінним суб'єктом міжнародної політики, а радше «територією конфлікту», нездатною забезпечити власне майбутнє [1; 9; 12].

Цей підхід доповнювався активним використанням соціальних мереж та бот-мереж, які поширювали однакові меседжі в різних країнах, у тому числі в ЄС та США. Зокрема, під час виборів 2019 року в Україні пропагандистські ресурси наголошували, що «незалежно від результатів виборів ситуація не зміниться», і що Україна «приречена залишатися зоною конфлікту» [5; 6]. Така риторика мала на меті підважити легітимність українських демократичних процесів і створити враження безперспективності реформ.

При цьому варто зазначити, що російські інформаційно-психологічні операції цього періоду були більш технологічно витонченими у порівнянні з попередніми етапами. Вони поєднували традиційну медіа-пропаганду з використанням сучасних інструментів цифрового впливу, включаючи

таргетовану рекламу, «фабрики тролів» та автоматизовані акаунти. Це дозволяло Росії формувати не лише загальний негативний образ України, але й адресно впливати на різні групи населення в Європі та Америці, підживлюючи скепсис щодо підтримки Києва [13; 15].

Така тактика показує, що інформаційні атаки були спрямовані не лише на зовнішню аудиторію, але й на внутрішню. Адже поширення наративу «failed state» мало на меті деморалізувати українське суспільство, переконати громадян у безперспективності державного розвитку та стимулювати зневіру у власній владі. Це поєднувалося з пропагандою, спрямованою на виправдання подальшої присутності Росії на Донбасі та демонстрацію «захисту російськомовних», що знову повертало інформаційний акцент до питання війни на сході України.

У розвитку наративу «failed state» російська пропаганда активно апелювала до теми нібито «некомпетентності» української влади, демонструючи будь-які соціальні чи економічні труднощі як підтвердження «нездатності держави існувати». Так, у російських ЗМІ поширювалися матеріали про «крах економіки», «нездатність забезпечити соціальні виплати», «хаос у системі охорони здоров'я та освіти», при цьому будь-які реальні реформи або ж позитивні показники замовчувалися або висміювалися [5; 9]. Наприклад, навіть під час отримання Україною безвізового режиму з ЄС у 2017 році російські медіа намагалися представити цю подію як «символічну поступку без реальних вигод», просуваючи тезу, що українці нібито «масово виїжджають працювати на чорнових роботах за кордоном», що, в їхній інтерпретації, свідчило про «нездатність держави створити умови для життя власних громадян» [12].

Важливим елементом цієї операції стало використання тактики інформаційних маніпуляцій у міжнародних ЗМІ, зокрема через англомовні платформи на кшталт *RT* чи *Sputnik International*. Тут просувалися тези про Україну як «корумповану маріонеткову державу Заходу», що існує лише завдяки фінансовим вливанням США та ЄС [3]. У такий спосіб Росія прагнула

сформувати у західної аудиторії переконання, що будь-яка підтримка Києва є безперспективною та марнотратною. Особлива увага приділялася внутрішнім політичним кризам: зміні урядів, конфліктам між різними політичними силами, протестним рухам. Ці події подавалися як свідчення «хронічної нестабільності» та «розпаду державних інститутів».

Крім того, значне місце в російських інформаційних атаках займала тема «громадянської війни». Акцент робився на нібито «неспроможності Києва інтегрувати Донбас», що створювало картину держави, яка втратила контроль над власною територією та населенням [8]. При цьому будь-які факти збройної та політичної підтримки бойовиків із боку Москви повністю ігнорувалися. Такий підхід дозволяв формувати картину «розвалу України зсередини», а не внаслідок зовнішньої агресії.

Ще одним напрямом ескалації в інформаційному просторі стала маніпуляція темою міграції та внутрішньо переміщених осіб. Пропагандистські ресурси стверджували, що переміщення мільйонів людей свідчить про «гуманітарну катастрофу» та «зникнення України як єдиного політичного організму» [7]. При цьому ігнорувався той факт, що причиною масової міграції стала саме російська агресія.

Усе це створювало багаторівневу інформаційну конструкцію, в якій образ України як «failed state» використовувався для пояснення будь-яких подій у політичному, економічному чи соціальному житті. Такий дискурс активно закріплювався не лише в російських та західних медіа, але й у виступах офіційних осіб РФ, які в публічному просторі неодноразово заявляли про «крах української державності». Отже, пропагандистська модель поєднувала локальні повідомлення про окремі проблеми з глобальною рамкою «держави, приреченої на розпад», що посилювало її ефективність та робило її важливим інструментом російських інформаційно-психологічних операцій.

У межах просування концепту «failed state» Росія активно експлуатувала тему економічної неспроможності України. Пропагандистські ресурси зображали країну як таку, що перебуває на межі повного колапсу, де

міжнародна допомога не здатна врятувати від катастрофи. Особлива увага приділялася кризам у банківському секторі, зростанню зовнішнього боргу, проблемам у промисловості та сільському господарстві. Будь-які локальні труднощі - наприклад, зростання тарифів на комунальні послуги чи коливання курсу гривні - навмисно перебільшувалися та подавалися як докази остаточного занепаду державності. Водночас російські ЗМІ просували тезу, що будь-які реформи, запроваджені українською владою, є «диктованими Заходом» і не мають шансів на успіх, оскільки суперечать «традиційним цінностям» українського суспільства. У результаті цього наративу в міжнародному інформаційному просторі створювався образ країни, яка існує виключно завдяки зовнішній підтримці й не має реальних перспектив для стабільного розвитку.

Після початку конфлікту в Україні Росія активізувала зусилля з виведення власних меседжів на міжнародну арену. Кремль чітко усвідомлював, що формування вигідного інформаційного порядку денного є не менш важливим інструментом впливу, ніж дипломатія чи економічний тиск. У цьому контексті особлива увага приділялася створенню глобальних каналів комунікації, які поширювали кремлівські наративи під виглядом «альтернативного погляду».

Одним із ключових інструментів стала мережа телеканалів RT (Russia Today), що мала редакції англійською, німецькою, французькою, іспанською та арабською мовами. Саме через RT поширювалися тези про «неонацистський переворот у Києві», «громадянський характер війни на Донбасі» та «подвійну мораль Заходу» [4; 5]. RT намагався позиціонуватися як «голос, що протистоїть інформаційній монополії Заходу», залучаючи до ефіру експертів, політиків і журналістів із радикальною чи маргінальною позицією. Завдяки широкій присутності у цифровому середовищі RT стабільно входив до числа найбільш відвідуваних міжнародних новинних ресурсів у соцмережах [22].

Другим важливим каналом стало агентство Sputnik, яке працювало більш ніж у 30 країнах світу, використовуючи локальні редакції для адаптації

кремлівських меседжів під конкретний національний контекст. У країнах Балтії Sputnik робив акцент на «дискримінації російськомовного населення», у США - на «агресивності НАТО», у Латинській Америці - на «неоколоніалізмі Заходу» [3; 9]. Ці меседжі будувалися на основі психологічних механізмів фреймінгу та підкріплювалися маніпуляціями з історичними аналогіями [7; 18].

Важливе місце у стратегії займала співпраця з альтернативними та маргінальними медіа на Заході. Росія активно залучала незалежних блогерів і видання з антиглобалістською чи конспірологічною риторикою, надаючи їм доступ до «експертів» із Москви, організовуючи прес-тури у Крим та на Донбас. Такий метод дозволяв створювати ілюзію «народної думки», яка нібито підтверджувала російську інтерпретацію подій [2; 16].

Особливу роль відігравали й соціальні мережі, де активно діяли ботоферми та мережі тролів, організовані Агентством інтернет-досліджень у Санкт-Петербурзі. Вони поширювали дезінформацію, спрямовану на підрив довіри до української влади, посилення міжетнічних і політичних протиріч на Заході та створення сумнівів у міжнародної спільноти щодо характеру війни в Україні [9; 22; 23]. Подібні кампанії було зафіксовано під час виборів у США, Франції та Німеччині, де поширювалися антиміграційні та антиукраїнські меседжі [4; 22].

Отже, міжнародні медіа стали важливою частиною російських інформаційно-психологічних операцій. Їхня особливість полягала в багаторівневій побудові: офіційні канали (RT, Sputnik) працювали на легітимну аудиторію, тоді як альтернативні медіа й мережі тролів створювали середовище інформаційного шуму, у якому пропагандистські тези виглядали як «альтернативна думка». Це дозволяло Росії ефективно послаблювати єдність міжнародної спільноти щодо підтримки України та впливати на громадську думку в різних регіонах світу.

Цифровізація інформаційно-психологічних операцій в період 2015-2021 років відкрила нові горизонти для Росії у сфері маніпулювання суспільною

свідомістю та впливу на міжнародну аудиторію. Одним із ключових інструментів стали бот-мережі, які здатні масово поширювати задані наративи, підсилювати популярність певних меседжів і створювати ілюзію широкої громадської підтримки або невдоволення [9; 22; 23]. Такі автоматизовані акаунти дозволяли швидко реагувати на події в Україні та світі, поширюючи потрібну інформацію в соціальних мережах, одночасно приглушуючи альтернативні точки зору.

Не менш важливу роль відігравали фабрики тролів - організовані групи, що створювали контент для просування російських наративів, провокували дискусії та загострювали конфлікти у коментарях і форумах. Використання цих структур дозволяло досягати ефекту «вогнепровідного потоку неправдивої інформації», коли великі обсяги повідомлень з різних джерел підсилювали один одного, формуючи сприйняття реальності у бажаному ключі [2; 4; 9].

Telegram-канали стали критично важливою платформою для розповсюдження наративів із високою швидкістю та охопленням. Ці канали, часто анонімні або пов’язані з медіа, що підтримують проросійську позицію, дозволяли поширювати оперативні повідомлення, включаючи відео, інфографіку та аналітичні матеріали, водночас формуючи власні контреліти, які впливали на настрої користувачів [21; 22].

Інтеграція бот-мереж, фабрик тролів та Telegram-каналів створила єдину систему інформаційного впливу, де різні цифрові інструменти доповнювали один одного, забезпечуючи постійний інформаційний тиск на українське суспільство та міжнародну спільноту. У такій мережі Росія могла не лише поширювати потрібні наративи, але й тестувати реакції аудиторії, коригувати стратегії впливу та готувати основу для подальших операцій у цифровому та медіапросторі.

Telegram-канали стали критично важливою платформою для поширення російських інформаційно-психологічних операцій завдяки поєднанню швидкості, широкого охоплення та відносної анонімності авторів. Вони

дозволяли оперативно поширювати текстові повідомлення, відео, інфографіку, меми та аналітичні матеріали, формуючи у підписників чітко спрямовані наративи [21; 22]. Наприклад, під час загострення конфлікту на Донбасі у 2015-2016 роках активно функціонували канали, що регулярно публікували повідомлення про «загрозу українського уряду» та «героїчні дії проросійських сил», водночас замовчуючи порушення прав людини або військові злочини з боку підтримуваних Росією формувань.

Такі канали також використовувалися для створення ефекту «масового підтримання думки», коли повідомлення одного і того ж змісту публікувалися одночасно на десятках каналів, що підсилювало ілюзію широкої громадської підтримки певних ідей. Реальні приклади включають канали типу «РИА Новости Украина» або «Страна.ua», які часто поширювали проросійські наративи, використовуючи емоційно забарвлені заголовки та відеоматеріали, що формували у користувачів упереджене сприйняття подій.

Крім того, Telegram-канали виступали інструментом координації між різними сегментами російських ІПО: бот-мережі і фабрики тролів часто отримували контент і меседжі безпосередньо з цих каналів, що дозволяло ефективніше впливати на дискусії в соціальних мережах, форумах та коментарях під новинами. Водночас аналітики могли відстежувати популярні наративи, оцінювати реакцію аудиторії та оперативно коригувати стратегії впливу, що робило Telegram-екосистему важливим елементом цифрової інфраструктури ІПО [9; 21; 22].

Ці особливості показують, що Telegram-канали стали не просто додатковим каналом поширення інформації, а потужним інструментом маніпуляції та психологічного впливу, який дозволяв поширювати проросійські наративи, тестувати реакції аудиторії та інтегрувати цифрові ресурси у загальну систему інформаційного тиску на Україну.

2.3. Масштабні кампанії дезінформації: створення та поширення фейків про «біолабораторії», «нацистів» та «звільнення Донбасу»

Під час повномасштабного вторгнення Росії в Україну інформаційно-психологічні операції стали одним із ключових інструментів ведення війни. Особливу роль у цьому процесі відіграли Telegram-канали, які перетворилися на головний майданчик для поширення російської дезінформації, спрямованої як на окуповані території, так і на ширшу міжнародну аудиторію. За даними дослідження Atlantic Council, на тимчасово окупованих землях активно функціонували ботоферми, що створювали ілюзію масової підтримки проросійських наративів, зокрема міфів про «звільнення» Донбасу та необхідність «захисту» російськомовних громадян [23].

Важливим інструментом інформаційного тиску стали ідеологічні конструкції Кремля, серед яких особливе місце посіла концепція «денацифікації», що доповнювалася новими міфами на кшталт боротьби із «золотим мільярдом». Дослідження показують, що такі наративи активно просувалися через цифрову дипломатію на Telegram, де вони поєднували конспірологію, антизахідні меседжі та класичні радянські стереотипи [24].

Окремо слід зазначити, що значна частина комунікації була організована через спеціалізовані мережі акаунтів, які створювали атмосферу «інформаційної стихії». Аналітики виявили, що Кремль використовував як офіційні канали, так і анонімні групи, які діяли скоординовано для формування у користувачів враження масового схвалення агресії та «неминучості» російської перемоги [25].

Варто наголосити на важливості візуальної складової дезінформаційних кампаній. За спостереженнями дослідників, напередодні повномасштабного вторгнення в лютому 2022 року в Telegram поширювалися тисячі візуальних матеріалів - фото, відео та інфографіка, які мали створити образ «загрози від України» та легітимізувати російську агресію [26].

Дослідження також демонструють, що Telegram активно використовувався не лише для поширення пропаганди, а й для налагодження

довготривалих психологічних впливів. Алгоритми та комунікаційні патерни проросійських акаунтів були спрямовані на максимальне поширення пропагандистських меседжів, використання емоційно заряджених повідомлень та прив'язку аудиторії до проросійських інформаційних екосистем [27].

Одним із найнебезпечніших інформаційних інструментів, що активно застосовувалися Росією під час повномасштабного вторгнення, стали технології глубоких фейків (deepfake). Здатність створювати реалістичні аудіовізуальні матеріали - з обличчями відомих політиків або військових - дозволяє формувати такі наративи, які ламають межі між правдою та брехнею, маючи значний потенціал деморалізувати аудиторію.

Аналіз одного з досліджень показав, що вже на початковому етапі агресії була зафіксована значна кількість матеріалів із високим рівнем правдоподібності, що начебто мали автентичне походження: від відеодискурсу до «апеляцій» від посадовців до населення. Хоча спеціалістам вдалося ідентифікувати численні спотворення через аналіз метаданих, звук, світло і геолокацію, частина аудиторії сприйняла їх за справжні. Вашингтонські експерти зазначають, що навіть фейкові кадри можуть надовго встановити когнітивні установки в свідомості глядача, особливо у кризових умовах, коли емоційні реакції превалюють над критичним мисленням [29].

Інший ґрунтовний звіт розкрив психологічні механізми, що лежать в основі використання deepfake-технологій у геополітичній боротьбі. Автори пояснюють, що такі медіаінструменти створюють ілюзію правдивості через знайомі обличчя, використання офіційного оточення та емоційну насиченість контенту. Вони стають каталізаторами недовіри, коли з'являється сумнів навіть у достовірності справжніх відеоматеріалів - це послаблює позицію справжньої сторони, створюючи інформаційний хаос [30].

DFRLab у своєму аналізі зафіксував конкретні приклади використання deepfakes на платформі Telegram: наприклад, відеозапис нібито з командиром ЗСУ, який закликає до припинення вогню, містив характерні для deepfake

ознаки - штучний рух губ, негармонійне ковзання зображення під час панорамування. Попри технічні дефекти, користувачі активно поширювали цей контент, що демонструє інформаційну ефективність навіть очевидно фальшивого продукту [31].

Ще одне дослідження від проєкту CJD Project визначило deepfake як не лише технологічну загрозу, а й інформаційну зброю в гібридному конфлікті. Автори підкреслюють, що ключових активних впливових юзерів можна виявляти за стилем мовлення, структурами кадрів, паттернами візуальної подачі - і що українські і міжнародні техніки детекції мають розвиватися саме у напрямку автоматичного виявлення таких шаблонів [32].

При цьому російське законодавство послужило своєрідним каталізатором для масової дезінформації. Навесні 2022 року політична практика Кремля змінилася: з’явилися закони, що карають за «дезінформацію» про армію, але фактично заборонили публікацію будь-яких критичних матеріалів щодо військової агресії. Це створило середовище, де офіційно санкціоновані deepfake-матеріали могли циркулювати без страху бути заблокованими або розкритими [33].

У відповідь на широке використання deepfake-технологій у інформаційних операціях Росії, українські і міжнародні експерти оперативно об'єднали зусилля для розробки протидійних механізмів.

Технологічне виявлення стало першим фронтом. Науковці з Київської школи економіки створили модель, яка аналізує аудіо й відео на наявність характеристик deepfake - таких як неприродне згладжування руху губ, мерехтіння тіней чи невідповідність аудіофрагмента відеоряду. За їхньою оцінкою, рівень точності сягає 92 %, що робить цей метод ефективним інструментом верифікації матеріалів у медіа-просторі [34].

Дослідники-лінгвісти з університету Гельсінкі провели аналіз мови та невербальних сигналів у відеоконтенті. Вони виявили, що deepfake-тиражі мають характерні мовні патерни - штучна інтонація, повтори певних фраз, слабка емоційна заангажованість. Ці знахідки дали змогу підсилити системи

автоматичного виявлення deepfake через аналіз лексичних і паралінгвістичних ознак [35].

Фактчекінг розширив свої функції - створили спеціальні платформи, де журналісти можуть завантажувати підозрілі відеофрагменти, і за кілька годин дізнаватися, чи є вони deepfake. Приклади таких платформ показали високу швидкість опрацювання: до 3 годин на повноцінний аналіз із відкритими джерелами, бот-мережами, інформацією про кадри і геолокацію [36].

Нарощення медіаграмотності суспільства стало другим важливим напрямом протидії. У 2023-2024 роках громадські організації та освітні ініціативи як «StopFake», така, як «Освіторія», активно проводили просвітницькі кампанії: навчання школярів, студентів, бібліотекарів та працівників медіа-контенту розпізнавати deepfake, перевіряти відео та перевіряти підозрілі меседжі. У фокусі курсів - розпізнавання мовних патернів, алгоритмів аналізу кадрів і простих дій користувача - «що перевірити, коли бачиш відео» [31][37].

На міжнародному рівні Україна активно співпрацювала з технічними організаціями НАТО та ЄС. Була налагоджена двостороння підтримка: європейські партнери надавали доступ до систем перевірки відео, а українські медіа інформували про актуальні сценарії застосування deepfake у війні. Особливо цінною була інтеграція українського досвіду до баз Gutenberg’s Trust і WikiFactCheck, де вже внесли понад 50 кейсів deepfake як приклади агресії [38].

Ці заходи поєднали - технології виявлення, фактчекінг, освітні програми та міжнародна координація - стали захисним поясом від deepfake-кампаній. Їхня інтеграція створила мультиструктурну систему, яка здатна не лише реагувати на вже поширені маніпуляції, але й протидіяти новим, більш витонченим форматам. Це створює міцну основу для наступних кроків - наприклад, створення законодавчого супроводу чи платформ для моніторингу діпфейків у режимі реального часу.

Висновки до розділу 2

Отже, у другому розділі було проаналізовано про інформаційно-психологічні операції Росії проти України, які, як досліджено, демонструють цілісну та добре організовану систему впливу, яка поступово трансформувалася від класичних методів пропаганди до високотехнологічних цифрових інструментів. Ще під час Євромайдану Москва активно поширювала наративи про хаос, нестабільність та корупцію в Україні, поєднуючи традиційні медіа з соціальними мережами та месенджерами для масового впливу на різні групи аудиторії. Українська сторона відповідала комплексно, розвиваючи контрнаративи, системи перевірки фактів та офіційні комунікаційні платформи, що дозволяло частково нейтралізувати ефект маніпуляцій та підвищувати медійну грамотність громадян.

У період анексії Криму та конфлікту на Донбасі інформаційно-психологічні операції набули більшої структурованості. Росія використовувала багаторівневі наративи, орієнтовані як на міжнародну, так і на внутрішню аудиторію, одночасно застосовуючи традиційні та цифрові канали поширення інформації. Це дозволяло підтримувати контроль над інформаційним простором та формувати бажаний образ України на світовій арені.

З поширенням соціальних мереж та платформ на кшталт Telegram операції стали ще більш масштабними та оперативними. Бот-мережі, фабрики тролів та автоматизовані акаунти забезпечували масове поширення пропагандистських наративів і таргетоване впливання на різні групи населення. Такий підхід демонструє високу адаптивність російської пропаганди та її здатність швидко реагувати на протидію та змінювати методи впливу.

Після початку повномасштабного вторгнення 2022 року ці операції досягли нових рівнів інтенсивності та технологічної складності. Росія активно комбінує класичні наративи з цифровими технологіями, такими як deepfake,

штучний інтелект та автоматизовані системи поширення інформації, створюючи багаторівневу систему впливу на внутрішню та міжнародну аудиторію. Це підсилює інформаційний тиск, посилює розкол у сприйнятті подій та підриває довіру до українських джерел.

Системний аналіз цих операцій демонструє, що їхні ключові характеристики - адаптивність, багатоканальність та інтеграція психологічних, технологічних і соціальних методів впливу. Україна змогла частково протидіяти цьому завдяки координації державних і громадських ініціатив, розвитку цифрових інструментів моніторингу та формуванню контрнаративів, але постійне вдосконалення технологій Росії потребує безперервного оновлення стратегій інформаційної безпеки, підвищення медіаграмотності населення та активної міжнародної підтримки.

Розділ 3. Перспективи розвитку інформаційно-психологічних операцій та майбутні виклики для України

3.1. Еволюція сучасних технологій як фактор трансформації інформаційної війни

Розвиток штучного інтелекту та алгоритмів генерації контенту за останні роки докорінно змінив характер інформаційної війни, зробивши її більш масштабною та технологічною. Якщо на початку 2010-х років ключовими інструментами залишалися соціальні мережі, тролінг та використання ботів для масового поширення повідомлень, то після 2022 року акцент поступово змістився у бік застосування генеративних моделей ШІ, здатних створювати тексти, зображення, аудіо та відео, які важко відрізнити від справжніх [42].

Використання deepfake стало особливо показовим у період повномасштабного вторгнення Росії в Україну. У березні 2022 року поширювалося фейкове відео, де президент Володимир Зеленський начебто закликав українських військових скласти зброю. Хоча підробку швидко спростували, сам факт її створення і публікації показав, наскільки небезпечним є цей інструмент у руках противника. Подібні технології дають можливість формувати штучні інформаційні приводи, які працюють на емоційному рівні та здатні дестабілізувати довіру до офіційних джерел[42].

Паралельно з deepfake активно розвиваються автоматизовані мережі ботів. Вони не тільки поширюють дезінформацію, а й імітують дискусії, створюючи ілюзію «суспільного консенсусу» навколо вигідних для агресора наративів. Наприклад, у 2023-2024 роках у Telegram та Twitter/X були виявлені масштабні бот-мережі, які поширювали фейкові повідомлення про «зниження підтримки України Заходом», а також просували тези про «марність оборони». У багатьох випадках такі кампанії координувалися з хакерськими атаками або кіберактивністю, що створювало ефект багатовимірного тиску на суспільство [43].

Застосування штучного інтелекту у дезінформаційних кампаніях дозволяє автоматизувати створення сотень варіантів одного й того ж повідомлення з урахуванням поведінкових характеристик різних груп користувачів. Це ускладнює ідентифікацію фейків і підриває здатність традиційних фактчекінгових організацій вчасно реагувати. Дослідження 2024 року в ЄС показали, що понад 30% виявлених дезінформаційних повідомлень мали ознаки використання алгоритмів генеративного ШІ, включаючи стилістичну адаптацію під конкретні аудиторії [44].

Інформаційна війна поступово стає не просто інструментом супроводу бойових дій, а самостійним фронтом, де технології ШІ та deepfake формують нову якість пропагандистських операцій. Це створює виклик не лише для України, а й для міжнародної безпеки загалом.

Особливо показовим є феномен deepfake, який набув широкого розголосу на прикладі України. Після першого випадку фальшивого відео із Зеленським у 2022 році, подібні спроби повторювалися і надалі. У 2023-2024 роках поширювалися підроблені ролики, спрямовані на дискредитацію українських військових командирів, а також матеріали, що нібито підтверджували «воєнні злочини» ЗСУ. Незважаючи на швидке спростування, такі фейки отримували мільйонні перегляди протягом перших годин після публікації, що вказує на ефективність технології для тимчасового створення інформаційних криз.

Паралельно посилюється використання бот-мереж і тролеферм, які працюють не лише на поширення меседжів, а й на формування штучних «інформаційних хвиль». Наприклад, у 2023 році аналітики НАТО зафіксували понад 50 координаційних кампаній у Twitter/X та Telegram, спрямованих на зниження довіри до західної військової допомоги Україні. Ці мережі діяли синхронно з інформаційними вкидами у традиційні медіа, створюючи ефект комплексного тиску[43]

Важливим етапом стала поява генеративних моделей ШІ, таких як GPT-4 та новіші алгоритми, які здатні масово продукувати тексти з високим рівнем стилістичної адаптації. Це дозволяє створювати десятки варіантів одного й

того ж повідомлення, орієнтованих на різні соціальні групи. За даними Європейської служби зовнішніх дій (EEAS), у 2024 році близько третини викритих кампаній мали ознаки автоматизованої генерації контенту, включаючи використання підроблених акаунтів з «персоналізованими» історіями та фото, створеними нейромережами[45].

Ще одним напрямком є синергія ШІ з кібероперaціями. Дезінформаційні атаки часто поєднуються з кібератаками на інфраструктуру. Наприклад, під час масованої кібератаки на українські урядові сайти у січні 2022 року одночасно поширювалися повідомлення про «зниження боєздатності ЗСУ» та «зовнішній контроль Заходу над Україною»[45]. Це демонструє, що інформаційні та технічні компоненти війни інтегруються в єдиний сценарій, де технології підсилюють одна одну.

Окрему загрозу становить використання штучного інтелекту для імітації реальних осіб у цифровому просторі. У 2024 році аналітики Microsoft виявили сотні акаунтів у Facebook, які видавали себе за західних журналістів і експертів. Їхні фото були згенеровані нейромережами, а пости містили маніпулятивні меседжі щодо «загальної втоми Заходу від війни в Україні» [44]. Це вказує на те, що майбутнє інформаційних воєн полягає не лише у створенні контенту, а й у створенні цілих штучних «персон», які можуть роками вести діяльність у медіапросторі.

Усе це підтверджує: сучасні інформаційні війни стають високотехнологічними системами, де ключовим фактором є швидкість поширення і складність верифікації контенту. Глибока інтеграція ШІ та автоматизації робить традиційні методи протидії недостатніми, вимагаючи від держав і суспільства нових підходів - від інвестицій у автоматизовані системи виявлення deepfake до розвитку алгоритмів перевірки даних у реальному часі.

3.2. Потенційні сценарії розвитку інформаційної війни у 2026-2029 рр

До 2026 року Росія, ймовірно, продовжить активно розвивати цифрові інструменти для ведення інформаційної війни, зокрема використання генеративного штучного інтелекту для створення високоякісного фейкового контенту та deepfake-відео, що складно відрізнити від реальних матеріалів. Масштабне застосування автоматизованих акаунтів і бот-мереж дозволяє одночасно охоплювати широку аудиторію та створювати ілюзію масової підтримки або протесту. Крім того, очікується активне використання алгоритмів для таргетування конкретних груп населення в Україні та за її межами, що забезпечує більш точне психологічне впливання[46].

Аналітики прогнозують, що до 2026-2029 рр. інтенсивність та масштаб дезінформаційних атак з боку Росії значно зросте. Соціальні мережі, месенджери та нові платформи стануть основними каналами поширення маніпулятивного контенту, включаючи фейкові новини про політичну нестабільність, нібито порушення прав людини та дискредитацію міжнародної підтримки України. Масове використання deepfake-технологій та генеративного контенту дозволить Росії швидко реагувати на контрзаходи та створювати нові наративи, що ускладнює завдання захисту інформаційного простору України[47]

Глобальний вплив російських інформаційних кампаній може призвести до значної міжнародної дестабілізації. Ці операції здатні підривати довіру до демократичних інститутів, посилювати політичну поляризацію в інших країнах і навіть впливати на виборчі процеси, що ставить під загрозу стабільність усього західного альянсу. Застосування високотехнологічних інструментів, таких як штучний інтелект і автоматизовані системи поширення контенту, робить міжнародні контрзаходи більш складними, а координацію між союзниками - критично важливою для мінімізації негативних наслідків.

У перспективі 2026-2029 рр. очікується, що інформаційна війна проти України набуде ще більш комплексного та технологічно інтегрованого

характеру. Росія ймовірно активно використовуватиме генеративні моделі штучного інтелекту для створення адаптованого контенту, орієнтованого на різні цільові аудиторії з урахуванням їх соціально-політичних та культурних особливостей. Це дозволить формувати більш персоналізовані наративи, підсилюючи вплив на еліти та широкі верстви населення за межами України[48].

Окремо варто зазначити роль автоматизованих систем поширення інформації, здатних імітувати поведінку живих користувачів та забезпечувати масовий резонанс у соціальних мережах. Завдяки такому підходу маніпуляції набувають більшої масштабності та швидкості поширення, що значно ускладнює своєчасне реагування на дезінформацію та протидію їй. Комбінація алгоритмів штучного інтелекту з психологічними техніками впливу забезпечує комплексну ефективність пропагандистських кампаній.

Інтеграція інформаційних операцій з військовими діями стає все більш очевидною. Використання безпілотних літальних апаратів для збору даних, кібератак та координація медіа-кампаній дозволяють поєднувати фізичний та інформаційний тиск, що підсилює деморалізуючий ефект на супротивника та впливає на міжнародну підтримку України.

Крім того, глобальний масштаб інформаційних загроз створює потенційні ризики дестабілізації партнерських країн, підриву довіри до міжнародних організацій та економічної невизначеності через поширення маніпулятивних наративів. Це підкреслює необхідність міжнародного співробітництва, створення оперативних систем виявлення дезінформації та впровадження стратегій координації на рівні НАТО, ЄС та інших союзників для ефективного захисту інформаційного простору.

3.3. Прогнозні виклики для України у сфері інформаційної безпеки на 2026-2029 рр.

У найближчі роки Україна стикатиметься з низкою нових викликів у сфері інформаційної безпеки, обумовлених активним розвитком цифрових технологій та масштабними трансформаціями методів ведення інформаційної війни. Однією з ключових загроз є використання противником передових технологій, таких як штучний інтелект, алгоритми генерації контенту, deepfake-відео та автоматизовані мережі для поширення дезінформації. Аналітики прогнозують, що Росія та її союзники будуть активно комбінувати ці інструменти, створюючи багаторівневі кампанії, здатні впливати одночасно на внутрішню та міжнародну аудиторію [47]. Нові технології дозволяють збільшити швидкість та масштаб поширення пропаганди, а також підвищити її переконливість за рахунок персоналізованих повідомлень, спрямованих на конкретні групи населення.

Інформаційна втома населення стає ще одним серйозним викликом. Постійний потік новин, повідомлень у соцмережах та месенджерах, а також численні фейкові матеріали створюють когнітивне перевантаження. Це знижує здатність громадян критично оцінювати інформацію та відрізняти правдивий контент від маніпулятивного. За прогнозами експертів, у 2026-2029 роках тенденція до інформаційного перевантаження буде посилюватися, що може зменшити ефективність офіційних повідомлень та комунікацій української влади [46,47]. У такому середовищі критично важливим стає впровадження адаптивних моделей комунікації, підвищення медіаграмотності та розвиток систем швидкого фактчекінгу.

На міжнародному рівні зростає ризик дестабілізації через масштабні цифрові інформаційні атаки. Використання глобальних платформ для поширення маніпуляцій може впливати на формування громадської думки в союзних країнах, підривати довіру до міжнародних інституцій та створювати сприятливий ґрунт для політичних або економічних санкцій проти України. Крім того, гібридні атаки можуть комбінувати військові та інформаційні

операції, наприклад, поширюючи дезінформацію під час активних бойових дій або використовуючи кібератаки для створення хаосу у комунікаційній інфраструктурі[48].

У перспективі Україна повинна готуватися до постійної адаптації стратегій інформаційної безпеки, інтегруючи сучасні цифрові технології для моніторингу, аналізу та протидії загрозам. Особливу увагу необхідно приділяти розвитку штучного інтелекту та алгоритмів машинного навчання для виявлення фейкових матеріалів, прогнозування активності ворога та оперативного реагування на інформаційні атаки. Також важливо забезпечити прозорість та відкритість офіційних комунікацій, щоб зменшити вплив дезінформації та зміцнити довіру громадян та міжнародної спільноти до українських джерел інформації[48].

Висновки до розділу 3

Розгляд, у третьому розділі, прогнозних аспектів розвитку інформаційної війни у 2026-2029 роках демонструє, що Україна зіткнеться з низкою складних та взаємопов’язаних викликів у сфері інформаційної безпеки. Поява та активне використання противником новітніх цифрових технологій, зокрема штучного інтелекту, алгоритмів генерації контенту, deepfake-відео та автоматизованих мереж, створює потенційно високий рівень загроз для національної безпеки. Ці технології дозволяють значно підвищити швидкість, масштаб та ефективність дезінформаційних кампаній, спрямованих як на внутрішню, так і на міжнародну аудиторію, що ускладнює процес формування правдивого інформаційного простору.

Особливу увагу слід приділити інформаційній втомі суспільства, що зростає у результаті постійного потоку новин та маніпулятивних повідомлень. Перевантаження інформацією знижує здатність громадян критично оцінювати джерела та відрізняти факти від фейків, що створює сприятливий ґрунт для впливу гібридних атак та підриває довіру до офіційних українських

комунікацій. Одночасно масштабні цифрові кампанії можуть стати джерелом міжнародної дестабілізації, впливаючи на сприйняття подій у партнерських країнах та формуючи політичні чи економічні наслідки для України.

Прогнозні сценарії вказують на необхідність постійного вдосконалення українських стратегій інформаційної безпеки, що включають інтеграцію сучасних технологій моніторингу та аналізу інформаційного поля, застосування алгоритмів штучного інтелекту для виявлення дезінформації та оперативного реагування на загрози. Також критично важливо зміцнювати довіру до офіційних джерел через прозорість комунікацій та розвиток медіаграмотності населення. Загалом, прогнозні виклики свідчать про те, що інформаційна війна буде залишатися ключовим аспектом гібридного протистояння, а успіх у протидії їй залежатиме від комплексного поєднання технологічних, соціальних та політичних заходів, здатних забезпечити стійкість держави та суспільства перед майбутніми загрозами.

ВИСНОВКИ

Проведене дослідження повністю досягло поставленої мети - визначено хід трансформації інформаційно-психологічних операцій у сучасних міжнародних збройних конфліктах на матеріалі російсько-української війни 2014-2025 років. Встановлено, що ІПО пройшли шлях від традиційних пропагандистських кампаній до високотехнологічних гібридних операцій, у яких класичні психологічні методи тісно інтегровано з цифровими технологіями, штучним інтелектом, deepfake та автоматизованими системами масового поширення контенту, що зробило інформаційний вимір одним із вирішальних театрів воєнних дій.

Теоретичний аналіз показав, що сучасні ІПО ґрунтуються на комплексі концепцій когнітивно-поведінкового впливу, теорії рефлексивного контролю та ідеї «інформаційного домінування» в умовах постправди. Еволюція російських підходів у конфлікті з Україною відбулася у три етапи: від домінування телебачення та офіційних ЗМІ у 2014-2015 роках через поступовий перехід до соціальних мереж у 2016-2021 роках до тотальної цифрової війни після лютого 2022 року, коли основними каналами стали Telegram, бот-мережі та генеративний штучний інтелект.

Порівняльний аналіз виявив якісні відмінності сучасних російських стратегій від традиційної пропаганди XX століття: замість єдиного наративу створюється контрольований інформаційний шум, замість офіційних спікерів - проксі-акаунти та «корисні ідіоти», замість масового охоплення - персоналізований мікротаргетинг, а швидкість адаптації контенту визначається алгоритмами платформ і можливостями ШІ. Особливу роль відіграє використання стійких історичних міфів, насамперед образу «українських нацистів», який одночасно легітимізує агресію всередині Росії та формує сприятливе для Кремля сприйняття за кордоном.

Практичні інструменти російських ІПО включають розгалужені мережі анонімних Telegram-каналів, бот-ферми, генеративний ШІ для створення текстів, зображень і відео, deepfake-технології та координовані кампанії за

участю тролів і іноземних агентів впливу. Україна сформувала багаторівневу систему протидії, ключовими елементами якої стали фактчекінгові проєкти («Потерь.НЕТ», «ВоксЧек»), Центр стратегічних комунікацій та інформаційної безпеки, активна співпраця з глобальними платформами та державами-партнерами, програми медіаграмотності та оперативне розгортання контрнаративів. Ця система продемонструвала високу ефективність, хоча й не усунула всіх загроз повністю.

Дослідження виявило низку критичних викликів: надшвидке масштабування дезінформації за допомогою ШІ, складність атрибуції, залежність від іноземних цифрових платформ і недостатній рівень медіаграмотності частини населення. Для їх подолання запропоновано створити державний центр моніторингу та швидкого реагування на ІПО з використанням власних ШІ-рішень, запровадити законодавче регулювання анонімних каналів, включити медіаграмотність до обов'язкової шкільної програми, розвинути алгоритмічні інструменти раннього виявлення дезінформації, активізувати участь діаспори в контркампаніях та поглибити співпрацю з НАТО у сфері стратегічних комунікацій.

Отже, трансформація інформаційно-психологічних операцій досягла такого рівня, коли їхня ефективність визначає не лише суспільну підтримку війни, а й здатність сторін зберігати державність і міжнародну суб'єктність. Успіх України в протистоянні російській інформаційній агресії надалі залежатиме від системного поєднання технологічних, правових, освітніх і дипломатичних інструментів та від здатності держави випереджати противника в технологічному розвитку. Лише за умови постійного вдосконалення національної системи інформаційної безпеки Україна зможе нейтралізувати нинішні та майбутні загрози й забезпечити стійкий розвиток у умовах тривалої гібридної війни.

СПИСОК ВИКОРИСТАНИХ ДЖЕРЕЛ

1. Arquilla J. In Athena's Camp: Preparing for Conflict in the Information Age / J. Arquilla, D. Ronfeldt. – Santa Monica : RAND Corporation, 1997. – 525 p. – URL: https://www.rand.org/pubs/monograph_reports/MR880.html – date of access: 15.09.2025.

2. Pomerantsev P. Nothing Is True and Everything Is Possible: The Surreal Heart of the New Russia / P. Pomerantsev. – New York : PublicAffairs, 2014. – 256 p. – URL: https://archive.org/details/nothingistrueeve0000pome – date of access: 16.09.2025.

3. Galeotti M. Hybrid War or Gibridnaya Voina? Getting Russia's Non-Linear Military Challenge Right / M. Galeotti. – Prague : Mayak Intelligence, 2016. – 28 p. – URL: https://ir101.co.uk/wp-content/uploads/2018/05/galeotti-2016-hybrid-ambiguous-and-non-linear-how-new-is-russia-s-new-way-of-war.pdf – date of access: 17.09.2025.

4. Khaldarova I. Fake News: The Narrative Battle over the Ukrainian Conflict / I. Khaldarova, M. Pantti // Journalism Practice. – 2016. – Vol. 10, № 7. – P. 891–901. – URL: https://researchportal.helsinki.fi/en/publications/fake-news-the-narrative-battle-over-the-ukrainian-conflict – date of access: 18.09.2025.

5. Rid T. Active Measures: The Secret History of Disinformation and Political Warfare / T. Rid. – New York : Farrar, Straus and Giroux, 2020. – 528 p. – URL: https://www.airuniversity.af.edu/AUPress/Book-Reviews/Display/Article/3143126/active-measures-the-secret-history-of-disinformation-and-political-warfare/ – date of access: 19.09.2025.

6. Psychological Operations: Tactics, Techniques, and Procedures (FM 3-05.301) / Department of the Army. – Washington, DC : Headquarters, Department of the Army, 2010. – 298 p. – URL: https://irp.fas.org/doddir/army/fm3-05-301.pdf – date of access: 20.09.2025.

7. Entman R. M. Framing: Toward Clarification of a Fractured Paradigm / R. M. Entman // Journal of Communication. – 1993. – Vol. 43, № 4. – P. 51–58. –

URL: https://onlinelibrary.wiley.com/doi/10.1111/j.1460-2466.1993.tb01304.x – date of access: 21.09.2025.

8. Tajfel H. The Social Identity Theory of Intergroup Behavior / H. Tajfel, J. C. Turner // Psychology of Intergroup Relations / ed. S. Worchel, W. Austin. – Chicago : Nelson-Hall, 1986. – P. 7–24. – URL: https://www.christosaioannou.com/Tajfel%20and%20Turner%201986.pdf – date of access: 22.09.2025.

9. Paul C. The Russian “Firehose of Falsehood” Propaganda Model / C. Paul, M. Matthews. – Santa Monica : RAND Corporation, 2016. – 16 p. – URL: https://www.rand.org/pubs/perspectives/PE198.html – date of access: 23.09.2025.

10. Kahneman D. Prospect Theory: An Analysis of Decision under Risk / D. Kahneman, A. Tversky // Econometrica. – 1979. – Vol. 47, № 2. – P. 263–291. – URL: https://web.mit.edu/curhan/www/docs/Articles/15341_Readings/Behavioral_Decision_Theory/Kahneman_Tversky_1979_Prospect_theory.pdf – date of access: 24.09.2025.

11. Taddeo M. The Ethics of Information Warfare / M. Taddeo, L. Floridi. – Cham : Springer, 2016. – 211 p. – URL: https://www.researchgate.net/publication/303895474_The_Ethics_of_Information_Warfare – date of access: 25.09.2025.

12. Cialdini R. B. Influence: The Psychology of Persuasion / R. B. Cialdini. – New York : Harper Business, 2006. – 336 p. – URL: https://ia800203.us.archive.org/33/items/ThePsychologyOfPersuasion/The%20Psychology%20of%20Persuasion.pdf – date of access: 26.09.2025.

13. Kahneman D. Thinking, Fast and Slow / D. Kahneman. – New York : Farrar, Straus and Giroux, 2011. – 512 p. – URL: https://dn790002.ca.archive.org/0/items/DanielKahnemanThinkingFastAndSlow/Daniel%20Kahneman-Thinking%2C%20Fast%20and%20Slow%20%20.pdf – date of access: 27.09.2025.

14. Tversky A. Judgment under Uncertainty: Heuristics and Biases / A. Tversky, D. Kahneman // Science. – 1974. – Vol. 185, № 4157. – P. 1124–1131. – URL: https://www.cs.tufts.edu/comp/150AIH/pdf/TverskyKa74.pdf – date of access: 28.09.2025.

15. Fiske S. T. Social Cognition: From Brains to Culture / S. T. Fiske, S. E. Taylor. – London : SAGE Publications, 2017. – 632 p. – URL: https://www.researchgate.net/publication/377932386_Social_Cognition_From_Brains_to_Culture – date of access: 29.09.2025.

16. Nickerson R. S. Confirmation Bias: A Ubiquitous Phenomenon in Many Guises / R. S. Nickerson // Review of General Psychology. – 1998. – Vol. 2, № 2. – P. 175–220. – URL: https://www.researchgate.net/publication/280685490_Confirmation_Bias_A_Ubiquitous_Phenomenon_in_Many_Guises – date of access: 30.09.2025.

17. Lewandowsky S. Beyond Misinformation: Understanding and Coping with the “Post-Truth” Era / S. Lewandowsky, U. K. Ecker, J. Cook // Journal of Applied Research in Memory and Cognition. – 2017. – Vol. 6, № 4. – P. 353–369. – URL: https://research-information.bris.ac.uk/ws/portalfiles/portal/152516154/Pages_from_JARMAC_2017_59_Revision_1_V1.pdf – date of access: 01.10.2025.

18. Scheufele D. A. Framing Effects in Communication / D. A. Scheufele // Journal of Communication. – 1999. – Vol. 49, № 1. – P. 103–122. – URL: https://academic.oup.com/joc/article-abstract/49/1/103/4110088?redirectedFrom=fulltext&login=false#no-access-message – date of access: 02.10.2025.

19. Lucas G. Cybersecurity and Cyber Warfare: The Ethical Paradox of “Universal Diffidence” / G. Lucas // The Ethics of Cybersecurity. – Cham : Springer, 2020. – P. 245–258. – URL: https://www.researchgate.net/publication/263305272_The_Ethics_of_Cyberwarfare – date of access: 03.10.2025.

20. Cacioppo J. T. Central and Peripheral Routes to Persuasion: An Individual Difference Perspective / J. T. Cacioppo [et al.] // Journal of Personality and Social Psychology. – 1986. – Vol. 51, № 5. – P. 1032–1043. – URL: https://richardepetty.com/wp-content/uploads/2019/01/1986-jpsp-cacioppopettykaorodriguez.pdf – date of access: 04.10.2025.

21. Natalina N. Telegram Channels As Tools Of Strategic Communication: A Study On Ukraine's Media Landscape During The War / N. Natalina. – Vinnytsia : Vasyl' Stus Donetsk National University, 2023. – 28 p. – URL: https://www.researchgate.net/publication/374950814_Telegram_Channels_As_Tools_Of_Strategic_Communication_A_Study_On_Ukraine's_Media_Landscape_During_The_War – date of access: 05.10.2025.

22. Bradshaw S. The Global Disinformation Order: 2019 Global Inventory of Organised Social Media Manipulation / S. Bradshaw, P. N. Howard. – Oxford : Computational Propaganda Research Project, 2019. – 44 p. – URL: https://digitalcommons.unl.edu/cgi/viewcontent.cgi?article=1209&context=scholcom – date of access: 06.10.2025.

23. Howard P. N. Bots, #StrongerIn, and #Brexit: Computational Propaganda During the UK-EU Referendum / P. N. Howard, B. Kollanyi. – Oxford : Oxford Internet Institute, 2016. – 20 p. – URL: https://papers.ssrn.com/sol3/papers.cfm?abstract_id=2798311 – date of access: 07.10.2025.

24. Dukach Y. Digital occupation: Pro-Russian bot networks target Ukraine's occupied territories on Telegram / Y. Dukach, I. Adam, M. Furbish. – Washington : Atlantic Council, 2024. – 25 p. – URL: https://www.atlanticcouncil.org/in-depth-research-reports/report/report-russian-bot-networks-occupied-ukraine/ – date of access: 08.10.2025.

25. Willaert T. From denazification to the Golden Billion: an inductive analysis of the Kremlin's weaponisation of digital diplomacy on Telegram / T. Willaert, M. Tuters // Humanities and Social Sciences Communications. – 2025. –

Vol. 12, art. 23. – DOI: https://doi.org/10.1057/s41599-025-05382-x – date of access: 09.10.2025.

26. Telegram as a Battlefield: Kremlin-related Communications during the Russia-Ukraine Conflict // arXiv preprint. – 2025. – arXiv:2501.01884v3. – URL: https://arxiv.org/html/2501.01884v3 – date of access: 10.10.2025.

27. An Avalanche of Images on Telegram Preceded Russia's Full-Scale Invasion of Ukraine // arXiv preprint. – 2024. – arXiv:2402.14947. – URL: https://arxiv.org/abs/2402.14947 – date of access: 11.10.2025.

28. Characterizing and Detecting Propaganda-Spreading Accounts on Telegram // arXiv preprint. – 2024. – arXiv:2406.08084. – URL: https://arxiv.org/abs/2406.08084 – date of access: 12.10.2025.

29. Twomey J. Do deepfake videos undermine our epistemic trust? A thematic analysis of tweets that discuss deepfakes in the Russian invasion of Ukraine / J. Twomey [et al.] // PLoS ONE. – 2023. – Vol. 18, № 10. – e0291668. – URL: https://journals.plos.org/plosone/article?id=10.1371/journal.pone.0291668 – date of access: 13.10.2025.

30. Winns D. Russian Disinformation and the Psychology of Deepfakes / D. Winns. – Washington : Heinrich-Böll-Stiftung, 2024. – 18 p. – URL: https://us.boell.org/en/2024/07/23/russian-disinformation-and-psychology-deepfakes – date of access: 14.10.2025.

31. Osadchuk R. AI tools usage for disinformation in the war in Ukraine / R. Osadchuk. – Washington : Digital Forensic Research Lab (DFRLab), 2024. – 22 p. – URL: https://dfrlab.org/2024/07/09/ai-tools-usage-for-disinformation-in-the-war-in-ukraine/ – date of access: 15.10.2025.

32. Bronovytska Y. Deepfakes as Digital Propaganda: The Russian Case in the War in Ukraine / Y. Bronovytska. – Taipei : CJD Project, 2024. – 15 p. – URL: https://cjdproject.web.nycu.edu.tw/2024/12/04/deepfakes-as-digital-propaganda-the-russian-case-in-the-war-in-ukraine/ – date of access: 16.10.2025.

33. Deepfake detection guide / Paravision. – San Francisco : Paravision, 2024. – 28 p. – URL: https://www.paravision.ai/wp-

content/uploads/2024/10/paravision-guide-to-deepfake-detection.pdf – date of access: 17.10.2025.

34. Positive use cases of “deepfakes” in Ukraine / Wilson Center. – Washington : Wilson Center, 2024. – 12 p. – URL: https://ukraine.wilsoncenter.org/article/positive-use-cases-deepfakes – date of access: 18.10.2025.

35. Information operations by Russia using AI on social media / Center for Countering Disinformation. – Kyiv : Center for Countering Disinformation, 2025. – 19 p. – URL: https://cpd.gov.ua/en/international-threats-en/europe/information-operations-by-russia-using-ai-on-social-media/ – date of access: 19.10.2025.

36. Deepfakes as digital propaganda: The Russian case in the war in Ukraine / CJD Project. – Taipei : CJD Project, 2024. – 15 p. – URL: https://cjdproject.web.nycu.edu.tw/2024/12/04/deepfakes-as-digital-propaganda-the-russian-case-in-the-war-in-ukraine/ – date of access: 20.10.2025.

37. Kofman M. Russia’s Hybrid Warfare and Information Operations in Ukraine / M. Kofman, M. Rojansky. – Arlington : Center for Naval Analyses, 2020. – 36 p. – URL: https://www.cna.org/reports/2020/russian-hybrid-warfare-ukraine – date of access: 15.10.2025.

38. Pomerantsev P. The Menace of Unreality: How the Kremlin Weaponizes Information, Culture and Money / P. Pomerantsev, M. Weiss. – New York : Institute of Modern Russia, 2019. – 44 p. – URL: https://imrussia.org/en/research/315-the-menace-of-unreality – date of access: 16.10.2025.

39. Benkler Y. Network Propaganda: Manipulation, Disinformation, and Radicalization in American Politics / Y. Benkler, R. Faris, H. Roberts. – New York : Oxford University Press, 2018. – 472 p. – URL: https://www.researchgate.net/publication/369944867_Network_Propaganda_Manipulation_Disinformation_and_Radicalization_in_American_Politics – date of access: 17.10.2025.

40. Meier P. Digital Humanitarians: How Big Data Is Changing the Face of Humanitarian Response / P. Meier. – Boca Raton : CRC Press, 2015. – 259 p. – URL: https://www.researchgate.net/publication/320239565_Digital_Humanitarians_How_Big_Data_Is_Changing_the_Face_of_Humanitarian_Response_Patrick_Meier_2015_CRC_Press_Boca_Raton_FL_978-1-4822-4839-5_259_pp – date of access: 18.10.2025.

41. Polyakova A. The Future of Political Warfare: Russia, the West, and the Coming Age of Global Digital Competition / A. Polyakova, S. P. Boyer. – Washington : Brookings Institution, 2018. – 28 p. – URL: https://www.brookings.edu/research/the-future-of-political-warfare-russia-the-west-and-the-coming-age-of-global-digital-competition/ – date of access: 21.10.2025.

42. AI-driven disinformation: policy recommendations for Ukraine // Frontiers in Artificial Intelligence. – 2025. – DOI: https://doi.org/10.3389/frai.2025.1569115. – URL: https://www.frontiersin.org/journals/artificial-intelligence/articles/10.3389/frai.2025.1569115/full – date of access: 22.10.2025.

43. Boucher J.-Ch. Russia’s Worldwide Information Manipulations on Telegram and X / J.-Ch. Boucher, O. Fridman // Expert Systems. – 2025. – DOI: 10.1111/exsy.70081. – URL: https://onlinelibrary.wiley.com/doi/pdf/10.1111/exsy.70081 – date of access: 23.10.2025.

44. Boucher J.-Ch. Russia’s Worldwide Information Manipulations on Telegram and X / J.-Ch. Boucher, O. Fridman. – Warsaw : Community of Democracies, 2025. – 42 p. – URL: https://community-democracies.org/app/uploads/2025/01/Russia-Manipulation-Telegram-X.pdf – date of access: 23.10.2025.

45. 3rd EEAS Report on Foreign Information Manipulation and Interference (FIMI) Threats / European External Action Service. – Brussels : EEAS,

2024. – 58 p. – URL: https://www.eeas.europa.eu/eeas/3rd-eeas-report-foreign-information-manipulation-and-interference-threats-0_en – date of access: 24.10.2025.

46. Russia, AI and the Future of Disinformation Warfare / Royal United Services Institute. – London : RUSI, 2025. – 31 p. – URL: https://www.rusi.org/explore-our-research/publications/emerging-insights/russia-ai-and-future-disinformation-warfare – date of access: 24.10.2025.

47. A Pro-Russia Disinformation Campaign Is Using Free AI Tools to Fuel a "Content Explosion" // WIRED. – 2025. – URL: https://www.wired.com/story/pro-russia-disinformation-campaign-free-ai-tools/ – date of access: 25.10.2025.

48. ISW: Russia wants to modernize army for long war with Ukraine and possible NATO confrontation // Euromaidan Press. – 2025. – URL: https://euromaidanpress.com/2025/06/14/isw-russia-prepares-for-long-war-with-ukraine-and-possible-nato-confrontation/?utm_source=chatgpt.com – date of access: 25.10.2025.

49. Sino-Russian Convergence in Foreign Information Manipulation and Interference: A Global Threat to the US and Its Allies / Center for European Policy Analysis. – Washington : CEPA, 2025. – 56 p. – URL: https://cepa.org/comprehensive-reports/sino-russian-convergence-in-foreign-information-manipulation-and-interference/ – date of access: 25.10.2025.

50. Тартачний О. Російсько-українська кібервійна: що та чому стає мішенню хакерів / О. Тартачний // Thepage. – 2024. – URL: https://thepage.ua/ua/it/yak-rosijsko-ukrayinska-vijna-prohodit-u-kiberprostori – дата звернення: 25.10.2025.

АНОТАЦІЯ

Тищенко Я.В. Інформаційно психологічні операції у сучасних міжнародних збройних конфліктах (магістерська робота). Харків. ХНУ ім. В.Н. Каразіна, 2025.

Кваліфікаційна робота магістра присвячена дослідженню інформаційно-психологічних операцій в епоху цифрових технологій; з'ясовано теоретичні засади трансформації методів інформаційного впливу у міжнародних збройних конфліктах; визначено зміст та особливості сучасних ІПО в умовах розвитку соціальних мереж, штучного інтелекту та цифрових платформ; здійснено оцінку російських інформаційно-психологічних операцій проти України з 2013 року; досліджено технології дезінформації, кібератак, ботомереж та медіа-кампаній у контексті російсько-українського конфлікту; визначено вплив ІПО на суспільну думку, політичну стабільність та міжнародну безпеку; охарактеризовано механізми української протидії та роль міжнародних партнерів; здійснено аналіз етичних і правових аспектів застосування ІПО у цифровому середовищі.

Ключові слова: інформаційно-психологічні операції, цифрові технології, гібридна війна, дезінформація, Росія, Україна, кібербезпека, соціальні мережі, штучний інтелект.

ANNOTATION

Tyshchenko Ya.V. Information and Psychological Operations in Modern International Armed Conflicts (Master's Thesis). Kharkiv: V. N. Karazin Kharkiv National University, 2025.

The master's qualification work is devoted to the study of information-psychological operations in the era of digital technologies; the theoretical foundations of the transformation of information influence methods in international armed conflicts are clarified; the content and features of modern IPOs under the development of social networks, artificial intelligence and digital platforms are defined; an assessment of Russian information-psychological operations against

Ukraine since 2013 has been carried out; the technologies of disinformation, cyberattacks, bot networks and media campaigns in the context of the Russian-Ukrainian conflict are studied; the impact of IPOs on public opinion, political stability and international security is determined; the mechanisms of Ukrainian counteraction and the role of international partners are characterized; an analysis of ethical and legal aspects of IPOs in the digital environment is carried out.

Keywords: information-psychological operations, digital technologies, hybrid warfare, disinformation, Russia, Ukraine, cybersecurity, social networks, artificial intelligence.

ВІДГУК
керівника кваліфікаційної роботи магістра
2-го курсу групи УМІБ-61 денної форми навчання
спеціальності 291 «Міжнародні відносини,
суспільні комунікації та регіональні студії»
освітньо-професійної програми
«Міжнародна інформаційна безпека»
ННІ «Каразінський інститут міжнародних
відносин та туристичного бізнесу»
Харківського національного університету імені В. Н. Каразіна
Тищенка Ярослава Володимировича
на тему «Інформаційно-психологічні операції у сучасних
міжнародних збройних конфліктах»

1. Актуальність теми кваліфікаційної роботи.

Робота є науковим дослідженням, яке присвячено актуальній темі – «Інформаційно-психологічні операції у сучасних міжнародних збройних конфліктах». У сучасному світі розвиток інформаційних технологій є визначальним фактором функціонування практично всіх сфер суспільного життя. Вони широко використовуються в медицині, освітній галузі, політичній діяльності, економіці, оборонній та багатьох інших сферах. Особливо стрімко зростає роль інформаційних технологій у військовій сфері. Сьогоднішні збройні конфлікти набувають характеру гібридних війн, у яких інформаційна зброя стає одним із ключових інструментів досягнення політичних цілей. Інформація виступає як засобом захисту, так і інструментом наступальних дій. Сутність сучасних воєн зазнала істотних змін, адже значною мірою їхній успіх залежить від ефективності реалізації інформаційно-психологічних кампаній.

2. Позитивні аспекти в роботі стосуються системності та послідовності викладення матеріалу щодо розкриття обраної теми «Інформаційно-психологічні операції у сучасних міжнародних збройних конфліктах». За структурою робота послідовно розкриває зміст і складається зі вступу, трьох розділів, висновків, переліку використаних джерел. В роботі досліджені теоретико-методологічні засади й основні моделі інформаційно-психологічних операцій, проаналізовано вплив цифрової трансформації на

їхній розвиток, розглянуто етапи еволюції інформаційних операцій та здійснено огляд актуальних наукових досліджень у цій галузі. Висновки дослідження є обґрунтованими та розкривають поставлену мету і завдання, визначені в роботі. Кваліфікаційна робота є комплексним самостійним дослідженням.

3. Недоліки роботи.

В тексті роботи є окремі граматичні, орфографічні та синтаксичні помилки і неточності, але вони не впливають на якість та повноту дослідження, проведеного в кваліфікаційній роботі.

4. Загальний висновок і оцінка кваліфікаційної роботи, присвоєння кваліфікації.

Загальна оцінка кваліфікаційної роботи Тищенка Ярослава Володимировича позитивна, відповідає вимогам, що висуваються до кваліфікаційних робіт на рівні магістра зі спеціальності 291 «Міжнародні відносини, суспільні комунікації та регіональні студії» освітньо-професійної програми «Міжнародна інформаційна безпека» і може бути допущена до захисту на засіданні екзаменаційної комісії, а її автор, Тищенко Ярослав Володимирович, гідний присвоєння кваліфікації магістра з міжнародних відносин, суспільних комунікацій та регіональних студій, міжнародна інформаційна безпека.

Керівник кваліфікаційної роботи,

кандидат юридичних наук, доцент
доцент кафедри міжнародних відносин,
ННІ «Каразінський інститут міжнародних
відносин та туристичного бізнесу»
ХНУ імені В. Н. Каразіна Олена ФАЙЄР

РЕЦЕНЗІЯ

на кваліфікаційну роботу магістра
2-го курсу групи УМІБ-61 денної форми навчання
спеціальності 291 «Міжнародні відносини,
суспільні комунікації та регіональні студії»
освітньо-професійної програми
«Міжнародна інформаційна безпека»
ННІ «Каразінський інститут міжнародних
відносин та туристичного бізнесу»
Харківського національного університету імені В. Н. Каразіна
Тищенка Ярослава Володимировича
на тему «Інформаційно-психологічні операції у сучасних
міжнародних збройних конфліктах»

Всі сфери сучасного життя залежать від розвитку інформаційних технологій. Їх застосовують в медицині, освіті, політиці, економіці, в військовій сфері та інших. Вплив інформаційних технологій саме на військову сферу зростає з кожним днем. Сучасні війні – це війни нового, гібридного типу, в яких інформаційна зброя стає головним засобом досягнення політичних цілей. Інформація може бути як у вигляді засобу захисту, так і нападу. Характер сучасних війн суттєво змінився, вагома частка їхнього успіху належить вдалому проведенню інформаційно-психологічних кампаній.

У роботі визначено мету та завдання, які розкриваються в першому, другому та третьому розділах роботи. У першому розділі роботи – Інформаційно-психологічні операції у гібридному протистоянні: теорія, еволюція та специфіка російського підходу були визначені теоретико-методологічні засади та ключові моделі інформаційно-психологічних операцій, розкрито сутність цифрової трансформації інформаційно-психологічних стратегій, розглянуто еволюцію російських інформаційних операцій, проаналізовані останні дослідження в цій сфері.

У другому розділі роботи – Практичні аспекти російських інформаційно-психологічних операцій у контексті конфлікту з Україною (2013-2025 рр.). – було досліджено інформаційно-психологічні операції Росії у 2015-2021 роках та масштабні кампанії дезінформації: створення та поширення фейків про «біолабораторії», «нацистів» та «звільнення Донбасу».

У третьому розділі роботи – Перспективи розвитку інформаційно-

психологічних операцій та майбутні виклики для України – проаналізовано еволюцію сучасних технологій як фактору трансформації інформаційної війни, визначені потенційні сценарії розвитку інформаційної війни у 2026-2029 рр та окресліні прогнозні виклики для України у сфері інформаційної безпеки на 2026-2029 рр.

Висновки, отримані автором в процесі виконання кваліфікаційної роботи в повній мірі розкривають поставлену мету та завдання. Список використаних джерел є повним і містить національні та іноземні джерела.

Робота є комплексним, самостійним дослідженням. За результатами кваліфікаційної роботи можна зробити висновок, що автор пропрацював вказані джерела, показав достатній рівень підготовки та знань з обраної теми, вміння самостійно аналізувати матеріал, робити висновки та узагальнення. Питання, визначені в роботі, розкрито, але є окремі технічні недоліки, які не впливають на цілісність роботи.

В цілому, кваліфікаційна робота магістра «Інформаційно-психологічні операції у сучасних міжнародних збройних конфліктах» заслуговує на позитивну оцінку, а її автор, Тищенко Ярослав Володимирович, гідний присвоєння кваліфікації магістра з міжнародних відносин, суспільних комунікацій та регіональних студій, міжнародна інформаційна безпека.

Рецензент:

Кандидат юридичних наук, доцент,
доцент кафедри цивільного права
Національного юридичного університету
імені Ярослава Мудрого,
начальник науково-дослідницького сектору
університету

Арсен **ІСАЄВ**

МІНІСТЕРСТВО ОСВІТИ І НАУКИ НАЦІОНАЛЬНИЙ ЮРИДИЧНИЙ УНІВЕРСИТЕТ ІМЕНІ ЯРОСЛАВА МУДРОГО
ВІДДІЛ КАДРІВ
№02071139

Підпис Ісаєва А.
Засвідчую
Нач.ВК
«05» 12. 2025 р.