

Чорноморський національний університет імені Петра Могили

(повне найменування вищого навчального закладу)

факультет політичних наук

(повне найменування інституту, назва факультету)

кафедра соціології та політології

(повна назва кафедри)

«Допущено до захисту»

В.о. завідувача кафедри соціології та
політології

Лушагіна Тетяна Вікторівна

«____» _____ 2025 року

КВАЛІФІКАЦІЙНА РОБОТА

на здобуття ступеня вищої освіти

бакалавр

(ступінь вищої освіти, спеціальність)

зі спеціальності:

052 Політологія

(шифр і назва спеціальності)

на тему: «Соціальні мережі як інструмент ведення сучасної
інформаційної війни»

Виконала: студентка IV курсу, групи 431
Богуславська Євгенія Сергіївна

(П.І.Б.)

Керівник: к. політ. н., доц.
Лушагіна Тетяна Вікторівна

(вчене звання, науковий ступінь, П.І.Б.)

Рецензент: д.політ.к, професор
Євтушенко Олександр Никифорович

(посада, вчене звання, науковий ступінь, П.І.Б.)

ОПП: «Політологія»

Миколаїв – 2025 рік

ЗМІСТ

ВСТУП.....	3
РОЗДІЛ 1. ТЕОРЕТИЧНІ ЗАСАДИ ДОСЛІДЖЕННЯ СОЦІАЛЬНИХ МЕРЕЖ ТА ІНФОРМАЦІЙНОЇ ВІЙНИ.....	7
1.1. Соціальні мережі: сутність, роль і значення в сучасному суспільстві.....	7
1.2. Вплив соціальних мереж на формування медіапростору.....	13
РОЗДІЛ 2. ВИКОРИСТАННЯ СОЦІАЛЬНИХ МЕРЕЖ В КОНТЕКСТІ СУЧАСНИХ ІНФОРМАЦІЙНИХ ВІЙН.....	20
2.1. Інформаційні війни в сучасних міжнародних відносинах.....	20
2.2. Типологія проявів інформаційно-психологічних операцій в соціальних мережах під час війни	23
РОЗДІЛ 3. ЗАСОБИ ПРОТИДІЇ ІНФОРМАЦІЙНИМ АТАКАМ У СОЦІАЛЬНИХ МЕРЕЖАХ.....	31
3.1. Перспективи розвитку інформаційних війн.....	31
3.2. Технологічні рішення для боротьби з фейковими новинами.....	35
3.3. Вплив сучасних технологій на можливості протидії інформаційним війнам.....	40
ВИСНОВКИ.....	49
СПИСОК ВИКОРИСТАНИХ ДЖЕРЕЛ ТА ЛІТЕРАТУРИ.....	54

ВСТУП

Актуальність теми дослідження. В умовах стрімкого розвитку цифрових технологій та глобалізації інформаційного простору соціальні мережі стали не лише засобом комунікації, а й потужним інструментом впливу на суспільну свідомість, політичні процеси та міжнародні відносини. Актуальність дослідження цієї теми обумовлена кількома ключовими факторами. Сьогодні мільярди людей використовують соціальні платформи, такі як Facebook, Twitter, Instagram, Telegram, TikTok та YouTube, для отримання інформації, обговорення актуальних подій і поширення власних поглядів. Завдяки швидкому поширенню контенту соціальні мережі стали основним джерелом новин для багатьох користувачів, що відкриває можливості для маніпуляції громадською думкою та використання цих платформ у рамках інформаційних воєн.

У сучасному світі інформаційна війна стала невід'ємною частиною конфліктів між державами, політичними групами та корпораціями. Через соціальні мережі поширюються фейки, пропаганда, дезінформація та елементи психологічного впливу, спрямовані на дискредитацію, деморалізацію чи мобілізацію певних груп населення. Дослідження таких механізмів є важливим для розуміння, як запобігати негативним наслідкам інформаційного впливу. Алгоритми соціальних мереж все більше використовуються для таргетованого поширення контенту. Бот-мережі та автоматизовані акаунти можуть маніпулювати рейтингами публікацій, створювати віртуальну «громадську думку» та впливати на поведінку реальних користувачів. Використання ШІ для генерування контенту, включаючи глибокі фейки (deepfake), ще більше загострює проблему.

З огляду на серйозні загрози, пов'язані з інформаційними війнами у соцмережах, виникає потреба у розробці ефективних механізмів протидії: законодавчого регулювання, фактчекінгу, медіаграмотності населення та створення технологічних рішень для боротьби з маніпулятивним контентом.

Актуальність дослідження соціальних мереж як інструменту ведення інформаційної війни є беззаперечною, оскільки ця сфера безпосередньо впливає на безпеку держав, громадянське суспільство та міжнародні відносини. Вивчення механізмів інформаційного впливу, методів захисту та ефективних стратегій протидії є необхідним для забезпечення інформаційної безпеки та збереження демократичних цінностей у цифрову епоху.

Ступінь наукової розробки дослідження. Тема використання соціальних мереж у контексті сучасної інформаційної війни є надзвичайно актуальною й водночас складною через її міждисциплінарний характер. Проблематику вже частково досліджували фахівці у галузях політології, соціології, інформаційної безпеки та медіакомунікацій.

Суттєвий внесок у вивчення інформаційної війни зробили такі дослідники, як В. Гулай, О. Дубас, О. Зіменко, які висвітлювали питання інформаційного впливу та маніпулятивних технологій у ЗМІ. Зокрема, досліджено поняття інформаційної агресії, методи психологічного впливу та форми дезінформації.

На особливу увагу заслуговують праці, присвячені ролі соціальних мереж у формуванні громадської думки та мобілізації соціальних груп: Ю.Бойко, О. Горбань, Т. Лушагіна, Л. Макаренко досліджували соціальні платформи як середовище поширення фейкових новин, створення віртуальних спільнот і координації протестних дій.

Водночас, попри зростаючу кількість публікацій, відчутною залишається потреба у комплексному аналізі соціальних мереж саме як інструменту ведення цілеспрямованої інформаційної війни — з урахуванням технічних, соціальних, політичних та безпекових аспектів. Особливо недостатньо опрацьованими залишаються питання алгоритмічного поширення контенту, роль бот-мереж, механізмів емоційного впливу та інформаційного тероризму.

Таким чином, тема дослідження перебуває на етапі активного формування наукового підґрунтя, потребує подальшої систематизації знань та розвитку у сфері міждисциплінарних підходів.

Метою дослідження є розкриття ролі соціальних мереж як інструмента ведення сучасної інформаційної війни.

Для досягнення мети, були поставлені наступні **завдання**:

1. Розкрити сутність, роль і значення соціальних мереж у сучасному суспільстві.
2. Вивчити явище інформаційних війн в сучасних міжнародних відносинах.
3. Систематизувати типологію проявів інформаційно-психологічних операцій в соціальних мережах під час війни.
4. Окреслити перспективи розвитку інформаційних війн.
5. Узагальнити вплив сучасних технологій на можливості протидії інформаційним війнам.

Об'єктом дослідження є інструменти ведення сучасних інформаційних воєн.

Предметом дослідження є соціальні мережі як інструмент ведення сучасної інформаційної війни.

Методи дослідження. Для аналізу соціальних мереж як інструменту ведення сучасної інформаційної війни використовуються такі методи дослідження: контент-аналіз – аналіз текстової, візуальної та аудіовізуальної інформації, яка поширюється через соціальні мережі, з метою виявлення маніпулятивних технік, фейкових новин та пропагандистських наративів. Дискурс-аналіз – дослідження мовних стратегій та риторичних прийомів, що використовуються для формування суспільної думки та емоційного впливу на аудиторію. Мережевий аналіз – вивчення зв'язків між користувачами, групами та сторінками в соціальних мережах, що дозволяє ідентифікувати центри впливу та способи поширення інформації. Психолінгвістичний аналіз – оцінка впливу інформації на когнітивні процеси та емоційний стан користувачів

соціальних мереж. Порівняльний метод – зіставлення різних інформаційних кампаній у соціальних мережах для виявлення спільних патернів та відмінностей у використанні інформаційної зброї.

Такі методи дозволяють комплексно дослідити соціальні мережі як інструмент інформаційної війни та оцінити їхній вплив на суспільство.

Практичне значення Отримані результати можуть бути використані у розробці стратегій протидії дезінформації та інформаційним атакам у соцмережах; удосконаленні інформаційної політики державних та недержавних організацій; створенні освітніх програм із цифрової медіаграмотності; аналітичній діяльності з виявлення та нейтралізації інформаційних загроз. Дослідження сприяє розумінню новітніх викликів у сфері інформаційної безпеки та формуванню ефективних механізмів боротьби з маніпулятивними технологіями в соціальних мережах.

Апробація. Результати здійсненого дослідження були апробовані на Міжнародній науковій конференції «Ольвійський форум – 2025: Стратегії країн Причорноморського регіону в геополітичному просторі» (Миколаїв, 2025 р.)

Структура дипломного проекту. Робота складається зі вступу, трьох розділів, 7 підрозділів, висновків та списку використаних джерел та літератури (95 позицій). Загальний обсяг роботи – 65 сторінок, з них 60 сторінок основного тексту

РОЗДІЛ 1. ТЕОРЕТИЧНІ ЗАСАДИ ДОСЛІДЖЕННЯ СОЦІАЛЬНИХ МЕРЕЖ ТА ІНФОРМАЦІЙНОЇ ВІЙНИ

1.1 Соціальні мережі: сутність, роль і значення в сучасному суспільстві

У ХХІ столітті соціальні мережі стали невід'ємною частиною повсякденного життя мільйонів людей. Вони впливають на комунікацію, освіту, бізнес, політику та багато інших аспектів суспільства. Соціальні мережі змінили спосіб взаємодії людей, зробили інформацію доступнішою, але водночас породили нові виклики, пов'язані з безпекою, маніпуляціями та залежністю. Соціальні мережі на сьогоднішній день є одними з найбільш відвідуваних ресурсів в Інтернеті. За даними дослідницької компанії ComScore їх використовують близько 85% всіх Інтернет-користувачів світу. На думку ряду вчених освітня парадигма ХХІ століття включає тріаду найбільших фундаментальних проблем – безперервність, масовість і якість. Саме технологічні інновації (у тому числі модернізація веб-платформ) дозволили по-новому організувати масове та безперервне навчання [47].

Соціальні мережі – це онлайн-платформи, які забезпечують можливість спілкування, обміну інформацією, створення контенту та взаємодії між користувачами. Вони об'єднують людей за спільними інтересами, професійною діяльністю чи особистими зв'язками.

Серед основних характеристик соціальних мереж можна виділити наступні:

- Інтерактивність – можливість миттєвого обміну повідомленнями, реакцій на контент та коментування.
- Доступність – можливість використання будь-де і будь-коли за допомогою смартфонів, планшетів та комп'ютерів.
- Глобальність – можливість спілкування з людьми з усього світу.

- Персоналізація – алгоритми, які підбирають контент відповідно до інтересів користувачів.

Соціальні мережі – це соціальна структура, що складається з групи вузлів, якими є соціальні об’єкти (люди, групи людей, спільноти, організації) та зв’язків між ними (соціальних взаємин). У загальнопоширеному розумінні соціальна мережа – це співтовариство людей, об’єднаних загальними інтересами, спільною справою або іншими причинами для безпосереднього спілкування між собою. У філософському підході під соціальною мережею розуміють безліч соціальних об’єктів і відносин між ними [68].

На думку Є. Патаркіна соціальні мережі – це платформи, за допомогою яких учасники можуть встановлювати відносини один з одним. Отже, соціальна Інтернет-мережа – це інтерактивний розрахований на багато користувачів веб-сайт, що володіє рядом обов’язкових якостей:

- зміст (контент) сайту створюється виключно чи переважно його користувачами;
- сайт є автоматизованим середовищем, в рамках якого користувачі мають можливість створювати зв’язки з іншими користувачами (соціальні зв’язки) або соціальні об’єкти (тематичні групи);
- користувачі мають можливість отримувати статичну та динамічну інформацію про об’єкти, що існують у даному соціальному середовищі, про соціальні зв’язки між ними;
- користувачам доступні функції комунікації з іншими користувачами та соціальними об’єктами [53].

Соціальні мережі виконують широкий спектр функцій, серед яких:

- Комунікативна функція – забезпечення спілкування між людьми незалежно від географічного розташування.
- Інформаційна функція – швидке розповсюдження новин, знань, аналітики.
- Освітня функція – поширення навчального контенту, можливість проходження курсів, консультацій із фахівцями.

– Комерційна функція – створення та просування брендів, реклама, продаж товарів і послуг.

– Розважальна функція – надання користувачам контенту для відпочинку та розваг.

– Соціалізаційна функція – формування спільнот за інтересами, підтримка зв'язків між людьми [68].

Питаннями вивчення соціальних зв'язків у групах людей почали займатися ще наприкінці XIX – на початку XX століття. Так, В. Гулай стверджував, що не всі соціальні феномени можуть бути пояснені з погляду властивостей окремих індивідуумів [16].

У 1930-х рр. Дж. Морено опублікував серію робіт з соціометрії, присвячену міжособистісним та міжгруповим відносинам. Основною інновацією наукових праць Морено прийнято вважати соціограми – схематичне зображення структури міжособистісних відносин у малій соціальній групі. В одному з його експериментів ставилося завдання розмістити вихованців дитячого будинку для дівчаток в окремих котеджах так, щоб у загальному котеджі знаходилися тільки ті з них, хто симпатизував один одному, і не допускалося проживання разом дівчаток, які відчують один одного неприязнь. Досліджуваних запитували, хто їм подобається і з ким разом вони хотіли б працювати чи проводити вільний час. Результати було представлено у вигляді ряду матриць, де кожному члену групи виставлялася оцінка іншими членами групи. Далі підраховувалися індивідуальні та групові індекси, будувалися соціограми у вигляді графів, на яких членам груп приписувалися певні позиції, а вибори (як позитивні, так і негативні) вказувалися стрілками – так відображалася структура переваг у групі. Своїми експериментами Дж. Морено фактично започаткував аналітичне дослідження соціальних мереж [46].

Поняття «соціальна мережа» вперше було запропоновано соціологом Дж. Барнсом у 1954 році. Він започаткував дослідження міжособистісних зв'язків, використовуючи соціограми — графічні схеми, на яких люди

зображувалися у вигляді точок, а лінії між ними символізували зв'язки [79]. Ідея сучасних онлайн-соціальних мереж бере свій початок від концепції «віртуальної спільноти», яку вперше висловив Говард Рейнгольд. Він визначав такі спільноти як соціальні утворення в Інтернеті, що виникають у результаті тривалого публічного спілкування, під час якого формуються особистісні зв'язки у віртуальному просторі [19]. У 1990-х роках інтерес до дослідження соціальних мереж значно зріс. Вагомий внесок у розвиток цієї тематики зробив американський соціолог Марк Грановеттер, який запропонував концепцію соціальних мереж як складних структур, що складаються з індивідів (вузлів) та взаємозв'язків між ними. У 2000-х роках із розвитком Інтернету соціальні мережі набули широкого поширення, що стало поштовхом до нових досліджень.

Початок розвитку інтернет-соціальних мереж припадає на середину 1990-х років. Серед перших значущих проєктів можна назвати платформу «GeoCities», засновану у 1994 році, яка дозволяла користувачам створювати власні веб-сайти, ділитися інформацією про себе та здійснювати онлайн-торгівлю. Цей сервіс сприяв утворенню віртуальних спільнот на основі спільних інтересів, однак припинив існування у 2009 році [80].

У 1995 році було створено сайт «Classmates.com», що допомагав знаходити та підтримувати контакт з колишніми однокласниками. До 2007 року його аудиторія складала близько 50 мільйонів користувачів. Попри те, що сайт функціонує і сьогодні, він значно поступається за популярністю «Facebook» [80]. Іншим новаторським проєктом став «SixDegrees.com», створений у 1996 році та запущений у 1997. Він дозволяв створювати профілі з реальними іменами, додавати друзів і знайомих. Цей сайт вважається одним із перших онлайн-проєктів у форматі соціальної мережі. Платформа проіснувала до 2000 року [15].

Ще одним раннім прикладом соціальної мережі став «LiveJournal», який з'явився у 1999 році. Він дозволяв користувачам вести онлайн-щоденники, залишати пости для друзів або широкого загалу, зберігаючи можливість

анонімності [80]. У 2002 році було запущено «Friendster», що стало прототипом сучасних соціальних мереж, орієнтованим на створення глобальної системи соціальних зв'язків. Уже в 2003 році платформа мала майже 2 мільйони користувачів, однак згодом втратила популярність через конкуренцію з «MySpace» та «Facebook» і перетворилася на ігрову онлайн-платформу [93].

У 2003 році з'явилася мережа «[Tribe.net](#)», заснована М. Пінкусом для об'єднання людей за інтересами. Наступного року був запущений «Facebook», спочатку як платформа для спілкування між студентами Гарварду. Вже у 2005 році мережа мала понад мільйон користувачів, а нині вона є лідером серед соціальних мереж із понад 2,5 мільярдами активних користувачів [80]. Як зазначає Т. Кремень, користувачі Facebook зазвичай підтримують зв'язки з близько 80 іншими профілями, а безпекова політика платформи передбачає видалення фальшивих акаунтів [29].

У 2006 році було створено «Twitter» — сервіс для коротких повідомлень, що спочатку обмежувався 140 символами, а з 2017 року ліміт збільшено до 280. Важливим функціональним доповненням стало введення символу «@» для згадування інших користувачів та хештегів «#» для позначення тем, що значно полегшило навігацію по контенту. Точну кількість підписників Twitter визначити складно через часту зміну облікових записів і налаштувань приватності [80].

У соціальних мережах існує значна кількість неактивних акаунтів або таких, що керуються ботами [80]. За даними кампанії *WeAreSocial* (BiASoушл), станом на початок 2020 року кількість користувачів цієї мережі сягала 340 мільйонів [80]. С. Івашньова описує соціальну мережу як віртуальний простір, що має технічні ресурси та інструменти для комунікації, сприяє налагодженню, розвитку, організації та підтримці соціальних зв'язків, включаючи обмін інформацією між учасниками. При цьому обов'язковою умовою є створення облікового запису [69].

У глобальному Інтернет-просторі існує велика кількість соціальних мереж, які можна класифікувати за різними критеріями. Наприклад, за рівнем доступу вони поділяються на відкриті, закриті та змішані. У межах цього дослідження використовувалися відкриті глобальні платформи, такі як TikTok та Telegram. Щодо географічного охоплення, соціальні мережі можуть діяти на міжнародному рівні, у межах окремої країни або регіону. Також можливе розмежування за цільовим призначенням — на особисті, професійні, тематичні тощо. А. Турчин виокремлює типи соціальних мереж: для особистого спілкування (Facebook), обміну медіа-контентом (Instagram, YouTube), ведення блогів і публічних обговорень (Twitter, Blogger), а також мережі, що об'єднують користувачів за спільними інтересами [66].

Соціальні мережі дають змогу підтримувати контакт із родиною, друзями, однокласниками та колегами. Вони допомагають знайомитися з новими людьми, ділитися моментами життя, виражати свої думки та емоції. Однак соціальні мережі також можуть впливати на особисте життя негативно, наприклад, сприяти залежності від лайків та коментарів, порушенню конфіденційності, створенню ілюзії ідеального життя, що може викликати невдоволення собою.

Для бізнесу соціальні мережі стали потужним інструментом маркетингу. Вони дозволяють компаніям безпосередньо взаємодіяти з клієнтами, отримувати зворотний зв'язок, аналізувати поведінку споживачів та просувати продукцію. До основних бізнес-можливості соціальних мереж належать:

- Таргетована реклама — точне налаштування реклами на цільову аудиторію.
- Брендинг — створення іміджу компанії через контент.
- E-commerce — продаж товарів та послуг через платформи, такі як Instagram, Facebook Marketplace.

Соціальні мережі стали важливим інструментом у політичному житті суспільства. Вони використовуються для агітації, мобілізації громадськості, організації протестів та впливу на громадську думку. Разом із цим вони несуть

загрозу маніпуляціям через фейкові новини, пропаганду, політичний тиск та кібератаки. Сучасні освітні процеси значною мірою інтегровані з соціальними мережами. Вони використовуються для дистанційного навчання, вебінарів, наукових дискусій та обміну знаннями.

Таким чином, можемо зробити висновки, що соціальні мережі є важливим явищем сучасного суспільства, яке охоплює всі сфери людського життя. Вони відкривають безмежні можливості для комунікації, навчання, бізнесу та розваг, але разом із цим несуть певні ризики. Відповідальне використання соціальних мереж та усвідомлення їхніх загроз дозволять максимально ефективно використовувати їхні переваги та мінімізувати негативні наслідки. Соціальні мережі – це не просто технологія, а потужний соціальний феномен, який продовжує змінювати наш світ.

1.2. Вплив соціальних мереж на формування медіапростору

Сучасний інформаційний простір суттєво трансформувався під впливом соціальних мереж. Ці платформи стали не лише засобами комунікації, а й основними каналами розповсюдження інформації, що конкурують із традиційними медіа. Важливим питанням є методологічний підхід до аналізу впливу соціальних мереж на інформаційні процеси, що включає розгляд механізмів поширення інформації, формування громадської думки, алгоритмів ранжування контенту та можливості маніпуляції свідомістю користувачів. У сучасному світі соціальні мережі стали ключовим елементом інформаційного середовища, впливаючи на спосіб поширення, сприйняття та обробки інформації. Вони є не лише майданчиком для спілкування, а й потужним інструментом впливу на суспільну думку, формування новинного порядку денного та розвитку цифрових комунікацій.

Розвиток Інтернету в Україні відбувається надзвичайно динамічно, сприяючи інтеграції країни у глобальний інформаційний простір та процеси інформатизації світової спільноти. Він стає не лише найзручнішим і

найпоширенішим засобом передачі й отримання інформації, але й дедалі доступнішим для широких верств населення. Це зумовлює зростання впливу глобальної мережі, яка нині активно витісняє традиційні ЗМІ, зокрема телебачення. Активний розвиток соціальних мереж — таких як Facebook, Instagram, Twitter, WhatsApp, YouTube, LinkedIn та інших — спричиняє поступове зниження інтересу до телепрограм і друкованих видань.

На думку дослідниці з США Памели Шелдон, користувачів соцмереж можна умовно розділити на дві категорії. До першої належать ті, для кого віртуальна комунікація є відображенням їхніх реальних соціальних зв'язків, — таких називають успішними споживачами медіа. До другої групи входять ті, хто, відчуваючи соціальну ізоляцію або невдачі, прагне компенсувати їх за допомогою онлайн-активності. Ці люди мають небагато контактів у мережі, проте часто відвідують свої сторінки, щоб зменшити почуття самотності [91]. Інші науковці дійшли висновку, що соціально активні особи використовують інтернет-ресурси переважно для підтримки вже існуючих соціальних контактів [78].

Згідно з даними дослідження Інтернет-асоціації України, у 2021 році кількість користувачів мережі в країні зросла на 6–7%. Зокрема, майже всі українці до 35 років активно користуються інтернетом. Це пов'язано з розширенням ринку смартфонів, які забезпечують повноцінний доступ до цифрових сервісів. Для значної частини нових користувачів саме смартфон став першим і єдиним пристроєм для виходу в інтернет [].

Крім того, дослідження USAID-Internews «Споживання медіа» у 2019 році вказує на суттєве падіння рівня довіри до традиційних ЗМІ — у середньому на 11% порівняно з 2018 роком. Найменше довіри мають загальнонаціональні друковані видання (19%), трохи більше — місцеве радіо (22%) і телебачення (49%). Водночас інтернет-медіа на загальнонаціональному рівні викликають довіру в 51% респондентів, що стало найвищим показником року [24].

У жовтні–листопаді 2019 року нами було організовано соціологічне опитування серед студентів закладів вищої освіти Харкова. Усього було

опитано 472 молодих людей віком від 18 до 32 років. Участь взяли: Харківська академія культури — 158 респондентів (33,4%), Національний фармацевтичний університет — 112 (23,7%), НТУ «ХПІ» — 82 (17,4%), Харківський національний автомобільно-дорожній університет — 73 (15,5%) та ХНУРЕ — 47 осіб (10%) [65]. Результати свідчать: 97% опитаних студентів отримують новини із соціальних мереж. Найпопулярнішою платформою виявився Facebook (31%), далі йдуть Instagram (18%), YouTube (15%), Viber (12%), Telegram (10%), WhatsApp (7%) і Twitter (4%). Традиційне телебачення як головне джерело новин обрали лише 3% респондентів [65].

Серед основних причин такого зниження інтересу до телебачення можна виокремити: падіння довіри до національного ТБ, зменшення попиту на традиційний медіаконтент, надмірне політичне втручання у медіа, адміністративний тиск, повільність у реагуванні на події, а також активізацію онлайн-комунікацій. Медіа, зокрема телебачення, суттєво впливають на формування світогляду молоді, використовуючи маніпулятивні техніки впливу на глядача. Якщо споживач не аналізує отриману інформацію критично, його ціннісні орієнтири можуть змінюватися, що спричиняє подальше зниження довіри до ЗМІ [65].

Зменшення рівня довіри до телеканалів часто супроводжується зниженням їхньої популярності. Це характерно як для національних, так і регіональних мовників. Населення дедалі краще усвідомлює наявність так званих «джинсових» матеріалів, замаскованих під журналістику, що призводить до поширення чорного піару та прихованої політичної реклами. Одноманітність сюжетів, повтори та відсутність незалежності журналістів викликають сумніви щодо об'єктивності медіа.

Соціальні мережі дедалі більше відіграють роль головного майданчика для обміну інформацією. Користувачі не лише публікують фото та відео з місця подій, а й активно беруть участь в обговореннях. Популярність таких мереж зумовлена свободою висловлювань, можливістю знаходити однодумців

та формувати спільноти за інтересами. Якщо контент є емоційно насиченим або несподіваним, він часто стає предметом масового обговорення.

Ці оцінки часто мають суб'єктивний характер, що сприяє розвитку плюралізму думок. Таким чином, соціальні мережі стали головним конкурентом телебаченню, особливо серед молоді. Телевізійні канали прагнуть втримати аудиторію, але все частіше глядачі обирають платформи, як-от YouTube, де зручно переглядати улюблені передачі у будь-який час. Інтернет має низку переваг — оперативність, технологічна гнучкість і доступність. У той час, як вітчизняне телебачення поступається за технічними можливостями, зарубіжні телеканали мають розвинену мобільну інфраструктуру, наприклад, пересувні студії, режисерські вертольоти, сучасне обладнання.

Соцмережі мають і свої недоліки: поширення фейків, маніпуляцій, замовних постів. Але телебачення в Україні все частіше програє в цій боротьбі через відсталість матеріально-технічної бази та бюрократичну інертність. Натомість користувач смартфона сьогодні може виступати журналістом, оператором, блогером і коментатором одночасно, миттєво реагуючи на події. Швидкий розвиток цифрових технологій, вдосконалення гаджетів та програмного забезпечення також сприяє зростанню популярності соціальних мереж, у той час як ТБ не встигає за цими змінами.

Щороку соціальні медіа посилюють свій вплив: від простого інформування вони трансформуються у повноцінні платформи розповсюдження інформації. Завдяки інструментам на кшталт Facebook Messenger, користувачі не лише споживають контент, а й активно обмінюються думками, беруть участь у дискусіях, онлайн-конференціях [65].

Сьогодні мережа стала ключовою складовою глобального інформаційного простору. Те, що раніше забезпечувало телебачення, нині виконується соціальними мережами. Вони вийшли далеко за межі своїх початкових функцій, ставши майданчиком для комунікації, самовираження та соціалізації. Залежність від віртуального спілкування зростає, і дедалі більше

людей ототожнюють себе з образом, який формують у мережі, віддаляючись від реальності.

Серйозною загрозою є вплив соціальних мереж на цінності молодого покоління, оскільки відсутність критичного мислення може призвести до маніпуляцій. Отже, українським телеканалам варто звернути увагу на динаміку росту впливу соцмереж, впроваджувати сучасні технології, залучати інвестиції та створювати конкурентоспроможні цифрові продукти, щоб відповідати викликам нового медіапростору. Паралельно, друковані видання втрачають свою вагу в медіаринку України: за даними КМІС, станом на лютий 2019 року лише 6,7% громадян вважали газети основним джерелом інформації, і ця частка продовжує зменшуватися [65]. Натомість багато міжнародних ЗМІ активно використовують Twitter для поширення контенту. В Україні ця мережа ще не надто популярна, але її аудиторія зростає. Можливо, вітчизняне телебачення з часом також перейме цей досвід.

Таким чином, соціальні мережі значно змінили спосіб функціонування традиційних медіа. Багато ЗМІ адаптувались до нових форматів, створюючи сторінки у соцмережах, публікуючи новини у вигляді коротких постів, відео чи сторіс. Це сприяє оперативному поширенню інформації, але також призводить до спрощення змісту. Завдяки соцмережам користувачі отримали можливість самостійно поширювати новини, коментувати події, створювати контент. Це послаблює вплив редакційного контролю та може сприяти поширенню недостовірної інформації або маніпуляцій. Можемо спостерігати зростання недовіри до традиційних ЗМІ на тлі популярності альтернативних джерел у соцмережах, хоча ці джерела не завжди є перевіреними. Це створює виклики для інформаційної безпеки. Отже, соціальні мережі радикально змінили медіапростір, зробивши його більш відкритим, швидким і доступним, але водночас — більш уразливим до маніпуляцій, фейків та інформаційного впливу. Формується нова інформаційна екосистема, де користувач стає не тільки споживачем, а й активним учасником інформаційного процесу.

РОЗДІЛ 2. ВИКОРИСТАННЯ СОЦІАЛЬНИХ МЕРЕЖ В КОНТЕКСТІ СУЧАСНИХ ІНФОРМАЦІЙНИХ ВІЙН

2.1. Інформаційні війни в сучасних міжнародних відносинах

У сучасному світі інформація стала одним із найважливіших ресурсів, а її використання як інструменту впливу стало звичною практикою для держав, корпорацій і громадських організацій. Інформаційні війни є ключовим елементом геополітичного суперництва, оскільки дозволяють досягати стратегічних цілей без відкритого застосування збройної сили. Вони впливають на свідомість мас, формують громадську думку та змінюють політичний ландшафт.

Інформаційна війна — це комплекс заходів, спрямованих на маніпуляцію інформаційними потоками з метою впливу на суспільну думку, політичні рішення або військові операції противника. Основними методами ведення інформаційних воєн є:

- Пропаганда та контрпропаганда – поширення інформації для створення певного наративу та формування відповідних настроїв у суспільстві.
- Дезінформація – свідоме поширення неправдивих або спотворених відомостей для введення противника в оману.
- Фейкові новини та маніпуляції у ЗМІ – створення неправдивих повідомлень, які можуть змінити політичну ситуацію.
- Кібероперації – атаки на інформаційні системи, витік даних, злам соціальних мереж та поширення шкідливого програмного забезпечення.
- Інформаційні блокади – цензура або обмеження доступу до альтернативних джерел інформації [54].

Основними характеристиками інформаційної війни є використання різних каналів для передачі інформації, вплив на світогляд та переконання

громадськості, маніпулювання емоціями та дезінформація. Наслідки інформаційної війни включають загострення міжнародних відносин, збільшення конфліктів і розкол у суспільстві. Для захисту від інформаційної війни важливо бути критичними до інформації, яку ми споживаємо, та перевіряти її достовірність. Треба навчати громадян критичному мисленню та критичному ставленню до інформації, яку вони отримують, а також розробляти та впроваджувати ефективні засоби захисту від дезінформації та інших форм інформаційної агресії.

У 1996 р. Міністерство оборони США ввело в дію «Доктрину боротьби з системами контролю та управління». Цей документ вперше визначав принципи боротьби з системами контролю та управління за рахунок застосування інформаційної війни у військових діях. У цьому документі також були визначені організаційна структура, порядок планування, навчання та управління ходом операції, а також основні поняття у цій галузі [43].

Основні погляди командування ЗС США щодо інформаційного протиборства та інформаційної сфери як нової сфери ведення бойових дій, викладених у редакції доктрини «Інформаційні операції», прийнятої в 2006р. У ній же визначені цілі, завдання та принципи інформаційних операцій. Для цієї сфери характерна своя специфічна форма ведення бойових дій – інформаційне протиборство. Інформаційне протиборство – боротьба в інформаційній сфері, яка передбачає комплексний деструктивний вплив на інформацію, інформаційні системи та інформаційну інфраструктуру протиборчої сторони з одночасним захистом власної інформації, інформаційних систем та інформаційної інфраструктури від подібного впливу. Метою інформаційного протиборства є завоювання та утримання інформаційної переваги над протиборчою стороною [31].

Об'єктом інформаційного протистояння є будь-який об'єкт, щодо якого можливе здійснення інформаційного впливу (у тому числа – застосування інформаційної зброї) або іншої дії (силової, політичної, економічної, технічної тощо), результатом якого буде модифікація її

властивостей як інформаційну систему. Об'єктом інформаційного протистояння може стати будь-який компонент чи сегмент інформаційного простору, у тому числі масова та індивідуальна свідомість громадян; соціально-політичні системи та процеси; інформаційна інфраструктура; інформаційні та психологічні ресурси; технічні системи збору, передачі обробки та подання інформації, а також системи управління.

До суб'єктів інформаційного протистояння відносять: держави, їх союзи та коаліції; міжнародні організації; недержавні незаконні збройні формування та організації терористичної, екстремістської, радикальної політичної, радикальної релігійної спрямованості (у тому числі міжнародні); транснаціональні корпорації; віртуальні соціальні спільноти; медіакорпорації та ЗМІ; віртуальні коаліції [31].

Інформаційні війни стали невід'ємною частиною сучасних міжнародних відносин, змінюючи способи ведення політики та впливу на світовий порядок. Здатність держав та суспільств протистояти інформаційним атакам визначає їхню стійкість у глобальному просторі. В умовах цифрової епохи ключовими інструментами боротьби з інформаційними загрозами залишаються критичне мислення, незалежні медіа та міжнародне співробітництво.

У президентських виборах у США 2016 року значну роль відіграли кампанії з поширення пропаганди та дезінформації, спрямовані на вплив на волевиявлення громадян. Одним із яскравих прикладів є втручання з боку Росії, яке включало активне використання соціальних мереж, розповсюдження фейкових новин і викривлення фактів. Такі дії демонструють, як інформаційна війна може впливати на внутрішньополітичні процеси в інших державах. Унаслідок цього загострилися політичні й дипломатичні відносини між США та Росією, що призвело до суттєвих змін у міжнародних відносинах. Сепаратистські рухи часто застосовують медіа як інструмент для побудови свого позитивного образу на міжнародному рівні. Через інформаційні кампанії вони прагнуть звернути увагу на свою боротьбу, акцентуючи увагу на

проблемах порушення прав людини, дискримінації та прагненні до національного самовизначення. Засоби масової інформації виступають у ролі платформи, що дозволяє представити їх як борців за справедливість, що, у свою чергу, допомагає здобути підтримку світової спільноти та сприяє визнанню їхньої діяльності [6].

Таким чином, інформаційні війни в сучасних міжнародних відносинах є складним і багатоаспектним феноменом, який надає значний вплив на політичні, економічні та соціокультурні процеси у світі. У сучасному світі інформаційні технології відіграють ключову роль у формуванні громадської думки, вплив на політичні процеси та маніпуляції масовою свідомістю. Сучасні технології забезпечують можливість миттєвого розповсюдження інформації по всьому світу, що робить інформаційні війни глобальними та міжнародними за своєю суттю. Це створює нові виклики для міжнародного співноти у сфері безпеки, стабільності та захисту прав людини.

2.2. Типологія проявів інформаційно-психологічних операцій в соціальних мережах під час війни

У ХХІ столітті війна виходить за межі лише збройного протистояння, дедалі активніше переносячись у сферу інформації, свідомості та психіки людини. Особливо це актуалізувалося в умовах повномасштабної агресії Росії проти України, коли засоби масової інформації стали не просто каналами передачі новин, а потужною зброєю впливу. У центрі цього процесу — інформаційно-психологічні операції (ІПСО), які спрямовані на формування, коригування або руйнування уявлень, переконань і поведінки аудиторії. Тому важливим завданням є виявлення типових маркерів ІПСО, їх класифікація та аналіз у медіапросторі під час війни.

Інформаційно-психологічні операції (ІПСО) – це спрямовані на вплив на психологічний стан людей та груп населення дії, що виконуються з

використанням інформаційних технологій та медіа. Мета ІПСО – зміна психологічного стану цільової аудиторії з метою досягнення бажаного результату, який може бути політичним, економічним, військовим або іншим. ІПСО використовуються в різних сферах, включаючи військові конфлікти, політичні кампанії, маркетинг та рекламу, а також для зміни психологічного стану масової аудиторії в цілях соціальної інженерії та маніпуляції громадською думкою. Поняття ІПСО увійшло до активного наукового вжитку із середини ХХ століття, проте медійну популярність в Україні отримало лише з початком україно-російського протистояння [74].

У медіапросторі ІПСО реалізуються через певні типові форми та техніки. Залежно від цілей, рівня охоплення та інструментів впливу можна виділити кілька основних типів інформаційно-психологічних операцій:

1. Дезінформаційні кампанії. Цей тип ІПСО спрямований на навмисне поширення неправдивої інформації з метою ввести аудиторію в оману. Дезінформація часто подається під виглядом «викриттів», «інсайдів», «аналітичних матеріалів» або навіть через фейкові документи. Прикладом є створення фейкових новин про «капітуляцію ЗСУ», «здачу міст без бою», «зраду в командуванні» тощо.

2. Пропагандистські наративи. Пропаганда як форма ІПСО спрямована на формування стійких установок через повторення вигідних меседжів. Російська пропаганда активно використовує такі наративи, як: «Захід втомився від України», «Україна — недодержава», «українці — брати росіянам», або ж «ЗСУ — злочинці». Ці твердження часто підкріплюються «експертними думками», візуальними матеріалами та емоційним забарвленням повідомлень.

3. Маніпуляція фактами та контекстами. Ще одна форма ІПСО полягає у навмисному перекручуванні або вибіркового поданні фактів. Наприклад, втрати цивільного населення можуть подаватися без контексту провини агресора, або ж дії українських військових висвітлюються як «провокації», що виправдовують жорстокість ворога. Маніпуляція також проявляється у використанні подвійних стандартів, емоційних заголовків або перебільшень.

4. Засівання паніки та зневіри. Особливо небезпечний тип ІПСО — кампанії, спрямовані на зниження бойового духу та викликання відчаю. У медіа це проявляється через поширення чуток про «повну поразку», «неможливість перемоги», «зраду союзників», дефіцит ресурсів або «масову мобілізацію без підготовки». Такі операції часто запускаються у періоди інтенсивних бойових дій або політичної нестабільності [7].

Підготовка та проведення інформаційно-психологічних операцій зазвичай здійснюється за подібною загальною схемою та включає кілька основних етапів. На першому – підготовчому – етапі виконується планування операції: визначаються її цілі, завдання, форми й методи реалізації, обирається цільова аудиторія, залучені ресурси, способи впливу, а також розробляються один або кілька можливих сценаріїв проведення операції. Під час інформаційного етапу формується або обирається інформаційний привід, після чого розпочинається активна реалізація операції відповідно до обраного сценарію. При потребі можуть залучатися додаткові ресурси.

На етапі «розкрутки» інформаційного приводу відбувається інтенсивний розвиток операції з метою досягнення визначених цілей – зокрема, впливу на психологічні установки та стереотипи цільової аудиторії, а також стимулювання її до певної поведінки чи змін у сприйнятті. Цей етап часто поєднується з попереднім і реалізується одночасно.

Завершальний етап операції – вихід з неї – передбачає контрольоване завершення активних дій, закріплення досягнутих результатів, оцінювання ефективності заходів, а за потреби – запуск нового циклу операції.

Такий підхід відповідає типовій моделі циклу прийняття рішень у системах управління, відомій як цикл OODA (спостереження – орієнтація – рішення – дія), яка широко застосовується у доктринальних документах Міністерства оборони США та документах НАТО.

Водночас реалізація ІПСО в соціальних мережах має свої особливості, що пов'язані з характеристиками цього середовища, специфікою методів і технік впливу, а також з особливим підбором учасників (виконавців) операції. Етапи

інформаційно-психологічної операції у соціальних мережах (один із варіантів) подані на рисунку 1. Підготовка до ІПСО у цьому контексті починається з аналізу суспільно-політичної та інформаційно-психологічної ситуації, визначення мети операції та цільової аудиторії (об'єкта впливу).

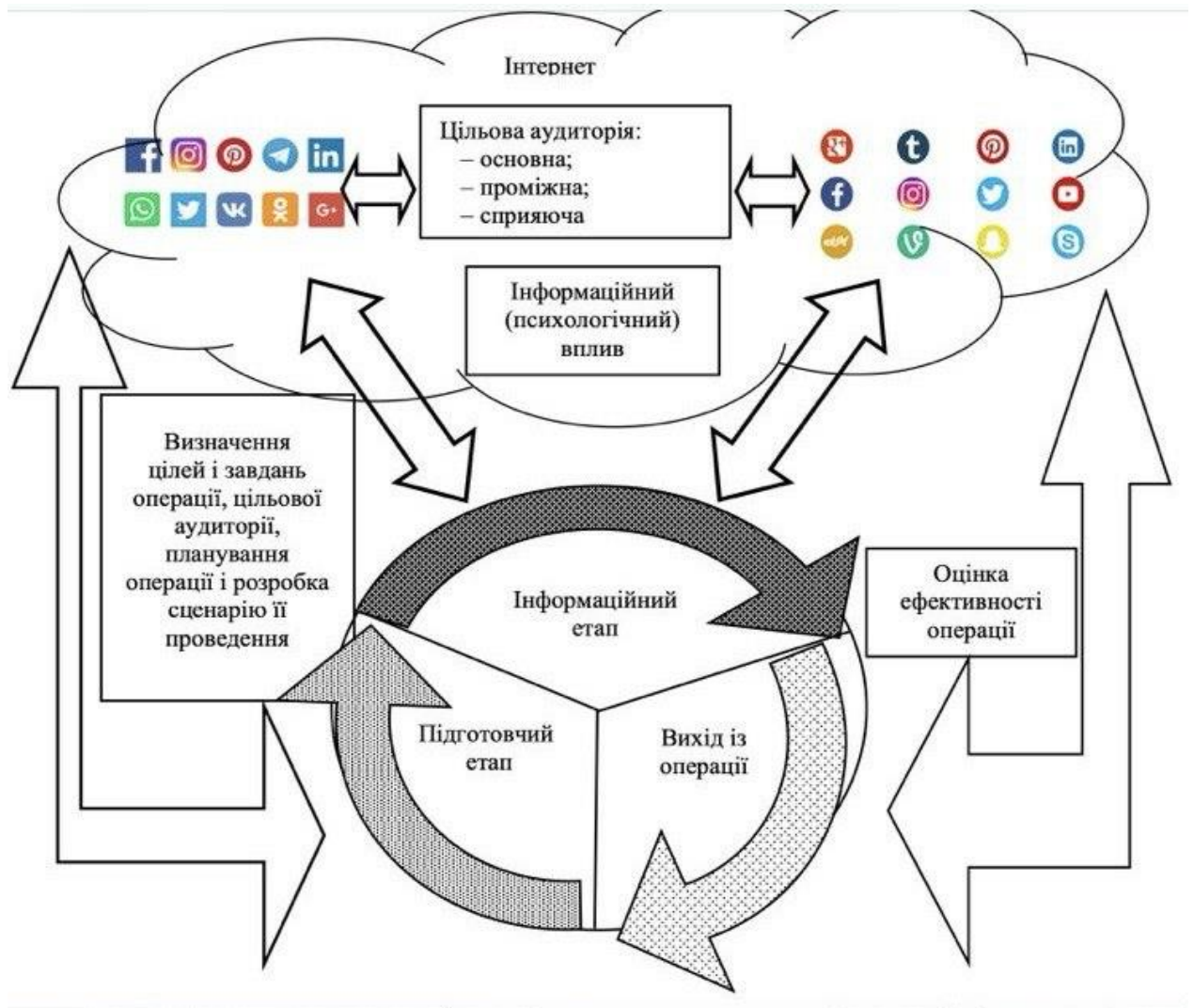


Рис. 1. Етапи інформаційної (психологічної) операції в соціальних мережах [44].

Основними каналами розповсюдження інформаційно-психологічних операцій є соціальні мережі, телеграм-канали, новинні сайти, блогери-агенти впливу, а також медіа, які підконтрольні або афілійовані з державами-агресорами. Особливу небезпеку становить контент, що маскується під

«незалежну журналістику» або «громадську активність», однак має чітке ідеологічне навантаження.

Протягом дії воєнного стану в Україні соціальні мережі на кшталт Facebook, Instagram і Twitter стали об'єктом системного моніторингу, що дозволило виявити ключові тактики інформаційно-психологічних операцій (ІПСО), які активно просуває російська сторона в українському та власному медіапросторі. До інструментів таких операцій входять фейки, маніпуляції, слухи, пропаганда, диверсії та кібератаки. Найчастіше ІПСО поширюються через неофіційні канали — приватні чати, вайбер-групи, месенджери тощо. Основні платформи для реалізації ІПСО — ті медіаканали, що мають потенціал охоплення великої аудиторії. Спочатку формується цільова спільнота, яку поступово привчають до певного способу мислення, а далі нав'язують конкретні дії. Поширеною є тактика використання патріотичної риторики для маскування деструктивних меседжів. Часто хибна теза подається разом із національними гаслами чи позитивною оцінкою ЗСУ, що викликає довіру й маскує справжній намір — дестабілізацію.

Військовий психолог та офіцер ЗСУ А. Козінчук зазначає, що ІПСО реалізуються у вигляді інформаційних атак, дезінформації, цілеспрямованих вкидів [32]. Їхня мета — маніпулювати свідомістю, зламати моральний стан супротивника або власного населення. Характерними ознаками ІПСО є синхронне поширення однотипної інформації, мовні помилки, відсутність реальних авторів (зазвичай це боти з фейковими іменами), а також специфічні конструкції в текстах на кшталт: «Я патріот, але...», після яких подається шкідлива думка [32].

У перші тижні повномасштабного вторгнення РФ активно використовувала повідомлення, покликані спровокувати паніку й втечу населення: «Київ масово виїжджає», «Влада покинула столицю». Ці фейки поширювались переважно російськомовними акаунтами, часто з псевдопатріотичними символами. Пізніше офіційні джерела регулярно спростовували подібну інформацію, або ж наперед попереджали про

можливість фейків. Ще одним напрямом інформаційної агресії були чутки про нібито підготовку наступу з боку Білорусі. Вони з'являлися хвилями, із новими датами та залякуванням прикордонних жителів. Ці повідомлення мали одразу кілька цілей: розхитати ситуацію, змусити українське командування перекидати війська, втягнути Білорусь у війну [32].

Російські ІПСО часто апелюють до емоцій, формуючи в повідомленнях емоційно навантажені наративи: страх, тривогу, паніку. Для цього використовуються як текстові прийоми (лексеми на кшталт «катастрофа», «небезпека», «рятуйте»), так і графічні засоби — капслок, жирний шрифт, візуальні матеріали з відповідним емоційним забарвленням. Окремо варто згадати меседжі, що мають вигляд «інсайдерської» інформації: безіменні «експерти», родичі в силових структурах тощо. Їхня функція — підірвати довіру до офіційних джерел, просуваючи ідею: «усі ЗМІ брешуть — тільки я кажу правду». Аналогічним чином працюють твердження на кшталт: «від нас щось приховують», «офіційні джерела мовчать» — вони слугують для дискредитації держави та інституцій [32].

Ще один різновид ІПСО — фейки з позитивним забарвленням. Наприклад, повідомлення про звільнення населеного пункту без офіційного підтвердження викликає ейфорію, але після спростування породжує розчарування й зневіру. Для психологічно вразливих людей такі інформаційні гойдалки особливо небезпечні — вони можуть призводити до депресивних станів або втрати віри в перемогу. Крім того, російські наративи нерідко використовують теми розбрату між різними регіонами України. Зокрема, поширюється думка, що нібито мешканці сходу й півдня самі винні в агресії, бо розмовляють російською. Це — типовий прийом перекладання провини з агресора на жертву, вигідний російській пропаганді [32].

Російські ІПСО також спрямовані на створення образу всемогутнього ворога. До прикладу, поширювались фейки про «червоне миготіння на горизонті», яке нібито вказує на стеження через телефони, або про обладнання, що блокує мобільний зв'язок. Зазвичай ці фейки супроводжуються технічно

необґрунтованими деталями, які, однак, викликають страх. Варто також згадати маніпулятивне використання теми покарання ворога. Заклики до фізичного знищення окупантів часто переходять межу гуманності. Як зауважує кореспондент «АрміяInform» А. Печерський, така риторика вигідна ворогу, бо дозволяє представити українців як «нелюдів» і виставити в негативному світлі перед міжнародною спільнотою [55].

Під час проведення інформаційно-психологічних операцій у соціальних мережах активно застосовуються спеціалізовані технології. Зокрема, для оперативного донесення певних повідомлень до визначеної цільової аудиторії часто використовуються меми. Їх мета — сформувати відповідну модель свідомості людини та вплинути на її вибір, тобто на процес прийняття рішень.

Кілька ефективних мемів, що передають основну ідею (наратив) та викликають позитивне сприйняття у певної аудиторії, здатні суттєво впливати на її свідомість і мотивувати до конкретних дій. Такий вплив пояснюється поєднанням стислої, зрозумілої інформації з емоційним забарвленням, що резонує як на свідомому, так і на підсвідомому рівнях. Меми відображають глибинні ментальні образи й можуть набувати форми тексту, руху, звуку, кольорових поєднань тощо.

Використання мемотехніки для інформаційно-психологічного впливу не є новим явищем. Зокрема, її активно застосовували ідеологи Ісламської держави Іраку і Леванту (ІДІЛ), а також пропагандистські структури Російської Федерації у гібридній війні проти України. У свою чергу, США та країни НАТО, прагнучи утвердити лідерство в сфері інформаційного протистояння на основі сучасних цифрових технологій, активно впроваджують меми як інформаційні бойові одиниці у своїх військових навчаннях та рольових сценаріях [32].

Ще одним ефективним способом залучення аудиторії в соціальних мережах є використання хештегів. Цей метод маркування постів з'явився у 2007 році, але широку популярність набув із 2010-го. Аналіз свідчить, що

хештеги є дієвим інструментом соціальної комунікації. Окрім того, в соціальних мережах дедалі активніше застосовуються технології штучного інтелекту для реалізації інформаційно-психологічного впливу, що значно розширює можливості впливу на аудиторію, коригування стратегії та оцінки її ефективності. Ефективність такого впливу може вимірюватися кількістю користувачів, які під його впливом переходять від віртуальної взаємодії до реальних дій, підвищенням інтенсивності інформаційного обміну, радикалізацією повідомлень, а також розширенням аудиторії за рахунок прихильників або нових учасників [32].

Таким чином, аналіз сучасних російських ІПСО у соціальних мережах показує їхню різноманітність і адаптивність. Ворог активно використовує інформаційний вакуум, емоційні тригери, мовні конструкції, патріотичну символіку, фейки з обох емоційних полюсів — і позитивного, і негативного — аби дестабілізувати ситуацію в Україні. Водночас українське суспільство демонструє дедалі більшу медіаграмотність і здатність до критичного мислення, що дозволяє ефективніше протидіяти цим інформаційним атакам. Інформаційно-психологічні операції у медіа під час війни є потужною зброєю, здатною впливати на свідомість, емоції та дії людей. Їхні прояви різноманітні — від грубої дезінформації до витончених маніпуляцій контекстом. Розуміння типології ІПСО дозволяє ідентифікувати загрози, вчасно їм протидіяти та зміцнювати інформаційну стійкість суспільства. У часи гібридної війни медіаграмотність та критичне мислення стають не менш важливими за військову підготовку чи технічні ресурси.

РОЗДІЛ 3. ЗАСОБИ ПРОТИДІЇ ІНФОРМАЦІЙНИМ АТАКАМ У СОЦІАЛЬНИХ МЕРЕЖАХ

3.1 Перспективи розвитку інформаційних війн

З появою інформаційних технологій світ став більш пов'язаним, ніж будь-коли раніше. Роль інформаційних технологій у різних сферах життя неоціненна. Вони спростили життя людей і зробили спілкування легшим і швидшим. Проте в наш час інформаційна війна набула особливого значення. Використання сучасних технологій і нейронних мереж, а також ботів і алгоритмів полегшило організаторам інформаційної війни поширення фейкових новин і маніпулювання громадською думкою [67].

У сучасному світі інформаційні війни стали невід'ємною частиною глобального військового протистояння між державами. Основна мета сучасної російської пропаганди полягає в тому, щоб дискредитувати українську владу, Збройні Сили України та суспільство загалом шляхом поширення дезінформації; завдавати шкоди економіці через блокування важливих галузей; виводити з ладу критичну інфраструктуру за допомогою хакерських атак, а також знижувати міжнародний авторитет України шляхом розповсюдження неправдивих відомостей. У зв'язку з цим ключовим завданням для України в умовах війни та інформаційного тиску є забезпечення національної інформаційної безпеки. Інформаційна війна — це складне та багатовимірне явище, яке відбувається на різних рівнях. Для формування ефективної національної політики в сфері інформаційної безпеки необхідно об'єктивно оцінити сучасний стан, специфіку та потенціал розвитку інформаційної зброї й методів її застосування.

Така оцінка є основою для створення зовнішньої та внутрішньої стратегії держави, що включає військові та технічні засоби, здатні попереджати загрози та забезпечувати надійний захист країни. Варто усвідомлювати, що інформаційна війна та кіберзлочинність виступають

інструментами прихованого військово-політичного тиску, які можуть дестабілізувати як регіональну, так і глобальну безпеку.

Саме тому необхідне постійне спостереження за загрозами застосування інформаційної зброї та систематична оцінка ефективності механізмів її нейтралізації. Вирішення проблеми інформаційних загроз сприятиме захисту інтересів держави й суспільства, а також гарантуватиме право громадян на доступ до правдивої та якісної інформації [73]

Сучасні технології, такі як Інтернет, соціальні мережі, штучний інтелект та кібернетика, мають значний вплив на інформаційну війну. Ці технології дозволяють поширювати інформацію на широку аудиторію, маніпулювати громадською думкою та координувати дезінформаційні кампанії.

Розвиток сучасних технологій призвів до зростання потенційних ризиків і викликів, пов'язаних з інформаційною війною. Зокрема, різні види зброї, такі як боти соціальних мереж і цільова реклама, використовуються для впливу на думку ворожого населення під час інформаційної війни. Вплив цих технологій величезний, оскільки вони можуть впливати на медіа та формувати громадську думку, яка часто є основною мішенню в інформаційних війнах. Властивості інформації та інформаційних технологій змінили характер і методи ведення сучасних інформаційних війн, зробивши їх більш прихованими і важко виявленими. Це створює значну проблему для урядів і організацій, яким доручено протидіяти цим загрозам, оскільки вони повинні мати можливість ідентифікувати та пом'якшувати наслідки цих технологій у швидко мінливому ландшафті.

Швидкий розвиток інформаційних технологій кардинально змінив доступність і методи ведення інформаційної війни. Швидкий розвиток інформаційно-комунікаційних технологій приніс значні трансформації в суспільстві та зміни в тому, як люди сприймають світ. З одного боку, ІТ зробили інформацію більш доступною та зручною, дозволяючи людям взаємодіяти та обмінюватися ідеями на величезних відстанях. З іншого боку, все більш

потужним інструментом формування громадської думки стає формування суспільної свідомості за допомогою методів психологічного впливу суб'єктів інформаційної війни. Тому вкрай важливо мати регулярні контрзаходи для боротьби з цим нападом на інформаційну функцію, незалежно від використовуваних засобів.

Однією з найбільш значущих перспектив розвитку інформаційних війн є зростання значення інформаційних технологій. З розвитком Інтернету та платформ соціальних медіа інформаційні війни стали доступнішими та потужнішими, ніж будь-коли раніше.

Ще одна перспектива розвитку інформаційних воєн – все більше використання технологій штучного інтелекту (AI) і машинного навчання (ML). Ці технології можна використовувати для створення високоперсоналізованих і цілеспрямованих кампаній дезінформації, які важко виявити та протидіяти. Оскільки технології штучного інтелекту та машинного навчання продовжують розвиватися, потенціал для того, щоб інформаційні війни ставали ще більш витонченими та ефективними, ймовірно, зростатиме.

Оскільки ми продовжуємо просуватися в майбутнє, надзвичайно важливо враховувати потенційні тенденції інформаційної війни. Феномен інформаційного впливу та його роль у сучасній війні є предметом обговорення вже давно. Із зростанням високотехнологічної інформаційної інфраструктури значення інформації у війні лише зростає. Історія інформаційних війн показала, що це не нова концепція, оскільки вона набула значення в XX столітті [36]. У Стратегії інформаційної безпеки України інформаційна безпека визначається як складова частина національної безпеки, що передбачає захист державного суверенітету, територіальної цілісності, демократичного ладу, а також інших ключових інтересів особистості, суспільства й держави. Її сутність полягає у забезпеченні конституційних прав і свобод громадян на доступ до достовірної інформації, можливість вільного збирання, збереження, використання та поширення інформації. Водночас має функціонувати ефективна система захисту від шкідливих інформаційних впливів, таких як

дезінформація, пропаганда, інформаційні операції, а також від незаконного поширення або спотворення даних з обмеженим доступом.

Питання забезпечення інформаційної безпеки закріплено в Конституції України. Зокрема, стаття 17 визначає, що охорона суверенітету, територіальної цілісності, а також економічної та інформаційної безпеки є пріоритетною функцією держави та спільною справою всього народу [28]. Додатково правові основи у сфері інформаційної безпеки врегульовані Законом України «Про інформацію», який визначає головні принципи функціонування інформаційного простору та гарантії захисту інформаційних прав громадян [22].

Сьогодні одними з найсерйозніших загроз інформаційній безпеці є дезінформація в умовах воєнного стану, ворожа інформаційна політика, маніпуляції у соціальних мережах, а також недостатній рівень медійної культури, медіа- та інформаційної грамотності серед населення, що, на нашу думку, є особливо актуальною проблемою. Фахівці з кібербезпеки підкреслюють, що в умовах війни надзвичайно важливо перевіряти джерела інформації, довіряти лише офіційним повідомленням, а також уникати переходів за підозрілими посиланнями. Ми щоденно зазнаємо впливу потужних медіа- та інформаційних потоків, які формують нашу свідомість. Цифрові технології, хоч і приносять безліч переваг, водночас створюють нові виклики.

Згідно з даними дослідження ГО «Детектор медіа» (2023), третина українців оцінює правдивість інформації інтуїтивно, а кожен четвертий довіряє лише тій інформації, що відповідає його власним переконанням. У цьому контексті навичка медіаграмотності набуває особливої ваги — здатність розпізнавати фейки та відрізняти правду від маніпуляцій стає критично важливою. Критичне мислення, вміння знаходити, аналізувати й ефективно використовувати інформацію є базовими навичками сучасного громадянина. Їх значущість можна порівняти з умінням читати чи рахувати. Для розвитку цих компетентностей фахівці з кіберзахисту пропонують різноманітні освітні

програми, що сприяють підвищенню рівня цифрової культури, медіаграмотності та персональної безпеки в Інтернеті.

Однією з дієвих ініціатив у цій сфері є проєкт «Платформа MRIYA», реалізований Департаментом кіберполіції України. Він спрямований на боротьбу з дезінформацією та протидію російській пропаганді в онлайн-просторі. Актуальні матеріали та практичні поради щодо кіберзахисту доступні на офіційному сайті Кіберполіції України [73]

Отже, у сучасні часи інформаційна війна стала переважно війною сприйняття та впливу, а не фізичного знищення. Дипломатичні зусилля стають все більш важливими для перемоги над ворогом в інформаційній війні. Важливо також зазначити, що використання технологій і платформ соціальних медіа в пропагандистських цілях і надалі залишатиметься основною тенденцією інформаційної війни. Очікується, що хакерські атаки та кібератаки, що фінансуються урядом, також зростатимуть, оскільки країни прагнуть отримати стратегічну перевагу над своїми конкурентами. По мірі того, як ми рухаємося вперед, важливо залишатися пильним і знати про ці нові тенденції, щоб ефективно боротися із загрозами, які створює інформаційна війна.

3.2. Технологічні рішення для боротьби з фейковими новинами

Фейкові новини стали серйозною проблемою сучасного інформаційного суспільства. Вони можуть впливати на громадську думку, політичні процеси, фінансові ринки та навіть безпеку держав. Технологічні рішення відіграють важливу роль у боротьбі з поширенням дезінформації. У цій доповіді розглянуто основні підходи та технологічні інструменти, що використовуються для виявлення та протидії фейковим новинам.

Фейкові новини — ефективний інструмент впливу на громадську думку. Оскільки створювати їх просто і дешево, сьогодні вони в загрозливих обсягах наповнюють інформаційні поля різних країн. «Багато підроблених новин пишуться звичайними людьми. Вони сидять за своїми комп'ютерами,

засвоївши просту формулу: скандальний заголовок плюс неправдива інформація і прибуток... Підроблені новини набагато легше сфабрикувати і поширити, ніж виявити і викрити» [14].

Фейк-нюс фабрикуються таким чином, щоб уже заголовком емоційно вразити користувача та переконати його повірити в них, а потім передати далі. Як стверджує дослідник людської цікавості, автор теорії «інформаційної прогалини» американський психолог Джордж Левенштейн, людину найбільше цікавлять речі, про які вона вже щось знає, але не вважає себе в них експертом. Мінімальний рівень знань є основною умовою залучення його уваги. Якщо користувач нічого про них не знає, значить він досі не виявляв до них інтересу, тому і далі продовжуватиме їх ігнорувати. Складний і незрозумілий заголовок або той, що розкриває надто багато змісту, менш привабливий, ніж заголовки, які дають деяку інформацію і водночас залишають недомовленість чи таємницю.

Фейкова інформація поширюється різними способами, найбільш агресивним з яких є тролінг, який здійснюється інтернет-тролями. Останні, згідно з визначенням австрійської дослідниці тероризму та екстремізму Джулії Ебнер, є «користувачами, які навмисно намагаються впливати на думки, що циркулюють у соціальних мережах» [24]. Найчастіше вони мотивовані політичними цілями і намагаються викликати паніку, дестабілізувати систему, розбурхати суспільство, розпалювати конфлікти, залучаючи до них велику кількість людей. Сутички з тролями особливо тяжкі в часи, коли все більшу роль відіграють платні тролі, навчені відповідним прийомам, що полегшують їм поширення дезінформації, а інтернет-користувачам утруднюють їхнє розпізнавання. Найпоширеніші типи тролів — це люди, які зазнають психологічної потреби завдати шкоди іншим, а також ті, хто вдає когось іншого, ніж є насправді [29].

Для поширення неправдивої інформації часто використовується не лише текст, але також фото чи відео. Йдеться про фейкові новини нового покоління — дипфейки. З розвитком інформаційних технологій стає все важче

відрізняти ці візуальні матеріали, що вводять в оману, від тих, що були зняті в реальності. «Діпфейк — це справжня отрута, якою можуть керувати як окремі люди, так і уряди», — стверджує колишній американський дипломат, а нині — дослідник феномену фейкових новин в Інституті міжнародних досліджень при університеті Міннесота в Дулуті Т. Хенсон [55]. За допомогою інфографіки «Як розпізнати фотографії та відео, що вводять в оману», увагу користувачів звертається на наступне:

— чи є зображення реальним чи виглядає покращеним, змонтованим за допомогою програмного забезпечення для редагування фотографій;

— чи не є зображення/відео, представлене як свідчення з місця події, насправді фрагментом із художнього фільму чи зовсім іншої події;

- Чи не сприяє візуальний матеріал просуванню стереотипів різних груп суспільства – жінок, чоловіків, осіб будь-якої конкретної національності [15].

Важливою складовою технологічних рішень для боротьби з фейковими новинами є аналіз існуючих методів перевірки фактів (fact-checking). Існує кілька основних методів, які застосовуються як вручну, так і з використанням автоматизованих технологій. У Таблиці 1 представлено і порівняно існуючі методи автоматичної перевірки інформації на правдивість.

Таблиця 1. Порівняльний аналіз існуючих способів автоматичного спростування фейкової інформації

Назва продукту	Сфера застосування	Ціль застосування	Методи реалізації ідеї
Fake news guard	Стрічка новин у Facebook або у веб-браузері Google Chrome	Спростування фейкових новин	Часткова автоматизація — порівняння джерела новини із списком сайтів-поширювачів файків, журналістське розслідування
Snopes	Веб-сайт для журналістів, фольклористів та інших читачів	Поширення достовірних і перевірених фактів	Контекстуалізований метод спростування фейків, тобто перевірка інформації

			виключно журналістами
Fakespot	Онлайн магазини (Amazon, Ebay)	Аналіз та обробка відгуків та оглядів продуктів у інтернет магазинах	Технологія аналізу підроблених відгуків шляхом виявлення повторних слів, фраз, схем придбання покупок та інше.
Reviewmeta	Онлайн покупки зі смартфонів, планшетів,	Аналіз оглядів товарів та видалення фейкових	Порівняння вхідного огляду з уже існуючою вибіркою фейкових
Thereviewindex	Інтернет магазини	Аналіз достовірності відгуків про товар	Пошук однакових відгуків на різні товари
FakesRadar (Factology System)	Стрічка новин у Facebook чи розширення веббраузера Google Chrome	Виявлення фейкових новин, боротьба з дезінформацією	Автоматичний аналіз вхідної статті за допомогою NLP

[складено автором].

Отже, кожен спосіб має свої переваги та обмеження. Для забезпечення ефективної перевірки фактів доцільно застосовувати комбінований підхід, який поєднує технологічні рішення з людським аналізом. У майбутньому важливу роль гратиме розвиток етичних стандартів, штучного інтелекту, а також освіта користувачів щодо медіаграмотності.

З метою підвищення поінформованості населення в галузі фейкових експертів, фейкових новин, фрейму, прихованої та замаскованої реклами явищ, що характеризують неякісну і навіть хибну інформацію, ЗМІ Латвії спільно з Британською радою реалізували проект «Голі факти», в інфографіці якого перераховуються основні. У Головній бібліотеці латвійського міста Лімбажі менеджер по комунікацій Stratcom (Центру передового досвіду НАТО в галузі стратегічних комунікацій) виступила на семінаріб з лекцією «Фейкові новини: наскільки реальна наша реальність?», в якій познайомила

бібліотекарів і школярів з тим, чому створюються фальшиві новини, кому це вигідно, як відмінити [43].

Штучний інтелект (ШІ) та машинне навчання (ML) є основними технологіями у боротьбі з фейковими новинами. Вони можуть аналізувати великі обсяги інформації, виявляти закономірності та оцінювати достовірність повідомлень.

ML-алгоритми використовують обробку природної мови (NLP) для:

- Виявлення ключових слів, що часто використовуються у фейкових новинах (емоційні вирази, сенсаційні заголовки).
- Аналізу граматики та стилю (фейки часто мають грубі помилки або непрофесійний стиль викладу).
- Співставлення фактів із перевіреними джерелами.
- Використання комп'ютерного зору для виявлення маніпуляцій у зображеннях.
- Аналіз метаданих (час, місце зйомки, редагування).
- Визначення дипфейків (підроблених відео, створених нейромережами).
- Аналіз поведінки користувачів: автоматичне виявлення ботів, які масово поширюють дезінформацію.
- Ідентифікація підозрілих акаунтів на основі активності (частота публікацій, взаємодія з іншими акаунтами).

Фактчекінгові організації використовують технологічні рішення для перевірки інформації. Автоматизовані платформи фактчекінгу:

- Snopes, PolitiFact, FactCheck.org – аналізують новини та оцінюють їхню достовірність.
- Google Fact Check Explorer – дозволяє користувачам перевіряти твердження через базу даних перевірених фактів.

Також є сьогодні можливість використовувати блокчейну:

- Збереження оригінальних версій статей і відео у незмінному вигляді.

– Верифікація першоджерел через децентралізовані платформи.

Отже, боротьба з фейковими новинами потребує комплексного підходу, що включає машинне навчання, фактчекінг, алгоритмічне регулювання та освітні ініціативи. Технологічні рішення допомагають ідентифікувати та обмежувати поширення дезінформації, але критичне мислення залишається найважливішим інструментом у руках користувачів.

3.3. Вплив сучасних технологій на можливості протидії інформаційним війнам

Розвиток соціальних медіа змінив територію інформаційної війни, полегшивши, ніж будь-коли раніше, маніпулювати більшою кількістю населення та впливати на нього. Соціальні мережі стали інструментом поширення пропаганди та дезінформації, часто з метою створення та управління конфліктними ситуаціями [23]. Використовуючи платформи соціальних медіа, інформацію можна швидко та широко поширювати, щоб охопити мільйони людей по всьому світу. Це дозволило окремим особам і організаціям поширювати неправдиві наративи, сіяти розбрат і маніпулювати громадською думкою в небачених раніше масштабах. Інтернет і соціальні медіа полегшили методи маніпуляції та впливу, дозволивши зловмисникам створювати та поширювати фейкові новини, меми та відео, які виглядають справжніми. Ці маніпуляції часто спрямовані на те, щоб викликати у людей такі емоційні реакції, як гнів, страх і обурення. Таким чином, соціальні медіа стали потужним інструментом для тих, хто прагне впливати на думки та переконання інших. Здатність маніпулювати платформами соціальних мереж також дозволила зловмисникам створювати та посилювати розбіжності в суспільстві, ще більше поляризуючи різні групи та створюючи серйозніші проблеми для вирішення політиками. Однією з таких технологій є TikTok, який використовувався як інструмент інформаційної війни в Україні кремлівськими троями для поширення антиукраїнських наративів, спрямованих на

дискредитацію влади та громадян України в очах міжнародної спільноти [61]. «Фабрика тролів» використовує деякі з найпопулярніших соціальних мереж сьогодення – зокрема, TikTok і Twitter – для поширення кремлівських антиукраїнських наративів за допомогою маніпулятивних технологій вербального впливу [45].

Специфіка дослідження полягала в застосуванні методу системного, семіотичного аналізу та моніторингу контенту в окремих соціальних мережах, таких як TikTok, який було обрано для більш детального аналізу через його популярність в Україні. Кремлівські тролі використовують сучасні технології для маніпулювання соціальними медіа для інформаційної війни, використовуючи вербальні засоби маніпулятивного впливу, такі як пейоративну лексику, для поширення антиукраїнських наративів у соціальних мережах. Нагнітання паніки та повторення інформації також є тактикою, яку використовують кремлівські тролі для маніпулювання соціальними мережами для інформаційної війни. Загалом виявлення та аналіз стратегій, тактик і засобів вербальних маніпуляцій кремлівськими троями в соцмережах є актуальним напрямком досліджень, вкрай важливим для запобігання поширенню антиукраїнської пропаганди в англомовних соціальних мережах. Зрештою, ці події призвели до суттєвих змін у способах ведення інформаційної війни, створивши низку нових викликів для урядів, організацій громадянського суспільства та окремих людей.

Чималу роль у формуванні інформаційної війни через соціальні мережі відіграли алгоритми та таргетована реклама. Платформи соціальних медіа використовують алгоритми для збору даних користувачів і адаптації свого рекламного контенту на основі цих даних. Таким чином, компанії соціальних медіа можуть доставляти персоналізовані повідомлення певним групам людей серед населення. Цей підхід був прийнятий тими, хто прагне вести інформаційну війну, оскільки він дозволяє їм охопити велику кількість людей за допомогою цільових повідомлень. Ці повідомлення часто залишаються непоміченими користувачами, оскільки вони призначені для роботи поза

межами їхньої уваги. Аналізуючи соціальні мережі, актори, задіяні в інформаційній війні, можуть маніпулювати масовою свідомістю, впливаючи на людей і керуючи ними способами, які не відразу помітні. Комунікаційні канали, такі як ЗМІ та Інтернет, використовуються для поширення інформації та пропаганди з метою формування громадської думки. Здатність націлювати пропагандистські матеріали на конкретні групи виявилася потужним інструментом у руках тих, хто прагне підірвати демократичні процеси та інститути. Тому важливо розуміти роль алгоритмів і таргетованої реклами у формуванні інформаційної війни через соціальні мережі та вживати необхідних заходів для протидії цим зусиллям.

В епоху соціальних медіа дезінформація та пропаганда стають все більш поширеними, частково підживлюючись використанням ботів і фейкових акаунтів. Ця тактика дозволила поганим акторам вести інформаційні війни через соціальні мережі, впливаючи на масову свідомість людей і керуючи ними. Вплив цих зусиль часто залишається поза увагою користувача, що означає, що люди можуть отримати неправдиву або оманливу інформацію, не усвідомлюючи цього. Комунікаційні канали в ЗМІ та Інтернеті залучені в інформаційну війну, де боти та фейкові акаунти відіграють значну роль у поширенні дезінформації та пропаганди [63]. Як наслідок, розрізнити правдиву інформацію в Інтернеті від неправдивої стає дедалі важче, що робить ще більш важливим залишатися пильними та критичними під час споживання інформації на платформах соціальних мереж [45].

Зі зростанням складності кібератак існує безліч потенційних ризиків і проблем, пов'язаних з кібервійною. Одним із найбільш значних ризиків є використання «сплячих» вірусів для запуску атак, які можуть залишатися бездіяльними протягом тривалого періоду, перш ніж поширитися на достатню кількість машин. Хакери також можуть використовувати законне програмне забезпечення для поширення вірусів, що ускладнює виявлення та запобігання. Уряди, великі технологічні та телекомунікаційні компанії в різних регіонах, а також окремі особи піддаються ризику кібератак, які можуть призвести до

значних фінансових втрат. Кібервійна також може призвести до компрометації конфіденційної урядової інформації та інфраструктури, створюючи серйозну загрозу національній та міжнародній безпеці. Однією з потенційних проблем у кібервійні є труднощі приписування та відплати, що ускладнює притягнення винних до відповідальності за їхні дії. Між країнами або конкуруючими компаніями можуть відбуватися кібервійни, що призводять до крадіжки або блокування фінансових ресурсів. Кібервійна створює потенційні ризики та виклики для комп'ютерних та інформаційних систем, включаючи системні злами, витік даних, виведення з ладу певних об'єктів та використання інформаційних даних для фальсифікації чи дискредитації. Виведення з ладу об'єктів критичної інфраструктури може мати небезпечні наслідки для населення, а блокування зв'язку та перехоплення розмов також можуть бути потенційними ризиками. Доступ до персональних даних може бути ризикованим, особливо на окупованих територіях. У результаті кібератаки можуть спричинити дестабілізацію роботи, максимальний економічний збиток та психологічну дестабілізацію суспільства. Враховуючи постійну еволюцію кіберзагроз, важливо залишатися пильним і постійно оновлювати заходи кібербезпеки, щоб зменшити потенційні ризики та виклики, пов'язані з кібервійною.

Штучний інтелект (ШІ) все частіше використовується як частина заходів інформаційної війни, спрямованих на поширення сумнівної та неперевіреної інформації та звичайних фейків. Однак відсутність прозорих методів перевірки висновків і рекомендацій систем ШІ створює невизначеність щодо їх точності та практичної цінності [64]. Концепція інформаційної війни рф базується на симбіозі війни в кіберпросторі та інформаційних операцій з механізмами, які активно використовуються в процесі гібридної війни проти України [24]. Традиційні та неортодоксальні стратегії та тактики з використанням цифрових інформаційних технологій все частіше поєднуються та використовуються в інформаційній війні. Тому вкрай важливо створити більш збалансовану та ефективну систему кіберзахисту,

здатну гнучко адаптуватися до змін середовища безпеки, забезпечуючи безпечне функціонування національного сегменту кіберпростору. Для досягнення поставленої мети необхідно провести подальші дослідження щодо визначення в нормативно-правових актах складу, функцій і завдань суб'єктів забезпечення кіберзахисту та розробки відповідної правової та організаційної бази. Проте тенденція кіберзагроз від авторитарних держав і посередників зростає в міру того, як інформаційні технології розвиваються та зближуються з технологіями штучного інтелекту. Як наслідок, впровадження ШІ в інформаційну війну вимагає прозорості та підзвітності, щоб запобігти втраті громадської довіри та завдати шкоди національній безпеці.

Оскільки світ стає все більш цифровим, потенційні наслідки інформаційної війни, керованої ШІ, стають все більш очевидними. Одним із основних застосувань технології ШІ в інформаційних війнах є здатність поширювати сумнівну та неперевірену інформацію. Такі кампанії з дезінформації можуть бути дуже ефективними для впливу на громадську думку та формування політичних наративів. Крім того, технологію штучного інтелекту можна використовувати для генерації дуже переконливого підробленого аудіо- та відеоконтенту, який майже неможливо відрізнити від справжнього. Це полегшує зловмисникам поширення неправдивої інформації та пропаганди, що може мати далекосяжні наслідки. Використання штучного інтелекту в інформаційній війні також може призвести до падіння довіри між окремими особами та установами, оскільки люди дедалі скептичніше ставляться до інформації, яку вони отримують в Інтернеті. Тому дуже важливо, щоб політики та технологічні експерти працювали разом, щоб розробити надійний захист від потенційного зловживання технологією ШІ в інформаційній війні.

Щоб пом'якшити негативний вплив ШІ в інформаційних війнах, можна вжити кілька заходів. По-перше, уряди та організації можуть інвестувати в розробку інструментів на основі ШІ для виявлення та протидії неправдивій інформації. Для цього знадобиться співпраця технологічних компаній і

дослідників для розробки ефективних алгоритмів, які зможуть відрізнити справжню інформацію від підробленої. По-друге, важливо навчати громадськість тому, як розпізнавати неправдиву інформацію та сприяти медіаграмотності. Це допоможе людям краще оцінювати онлайн-контент і запобігатиме поширенню неправдивої інформації. По-третє, уряди можуть запровадити суворіші правила щодо компаній соціальних медіа, щоб вони взяли на себе відповідальність за моніторинг і видалення неправдивої інформації зі своїх платформ. Нарешті, міжнародне співробітництво та угоди можуть бути встановлені для пом'якшення негативного впливу ІІІ в інформаційних війнах. Для цього знадобиться співпраця урядів і організацій для розробки стандартизованого набору правил і норм використання ІІІ в інформаційних війнах. Впроваджуючи ці заходи, ми можемо ефективно пом'якшити негативний вплив штучного інтелекту в інформаційній війні та захистити нашу національну та міжнародну безпеку.

У технологічному світі, який переплетений з інформаційними війнами, ми повинні звернути увагу на те, як використовуються соціальні мережі, штучний інтелект та алгоритми, робити це потрібно з особливою обережністю. Такі соціальні мережі, як TikTok і Twitter, уже використовуються для поширення неправдивої інформації та пропаганди. Алгоритми та таргетована реклама стали інструментами прямого впливу на громадську думку. Такий вплив може призвести до ненавмисних наслідків, зокрема соціальної дестабілізації та ризиків кібербезпеки.

Одним з важливих аспектів цієї ситуації є використання штучного інтелекту для поширення шкідливої інформації та створення віртуального контенту, який є надзвичайно впливовим. Це сприяє широкомасштабній передачі неправдивої інформації. Запобігання цим небезпекам вимагає об'єднаних зусиль технологічних експертів і законодавців для створення ефективних стратегій, щоб уникнути шкідливого використання штучного інтелекту. Ми повинні створити прозорі методи перевірки інформації та надати громадськості засоби для розрізнення фактів і вигадок у цифровій

сфері. Лише спільними зусиллями ми можемо розробити ефективні та стійкі механізми для запобігання маніпуляціям і неправдивій інформації, щоб вони досягли суспільства та завдали шкоди національній безпеці.

Отже, розвиток інформаційної війни тісно пов'язаний із технологічними змінами, удосконаленням систем та адаптацією оперативних методів і організаційних структур, які дозволяють ефективно використовувати нові можливості. У сфері оборони справедливо приділяється значна увага аналізу доктринальних, оперативних і структурних аспектів інформаційної війни. Водночас недостатньо розглядається конкретний вплив цієї сфери на технологічні дослідження та процеси закупівель. Зростання загроз, пов'язаних з інформаційними війнами та ворожими інформаційними впливами, актуалізує питання забезпечення інформаційної безпеки. Законодавство визначає ключові загрози в цій сфері, враховуючи швидкий темп змін та інтенсивність науково-технічного прогресу. Водночас складно очікувати, що будь-який закон може надати вичерпний перелік усіх потенційних викликів. Одним із суттєвих недоліків нормативної бази є відсутність визнання обмеження прав і свобод громадян щодо доступу, поширення та зберігання інформації як серйозної загрози [25].

У результаті проведеного дослідження у межах розділу було з'ясовано, що соціальні мережі виступають одним із головних каналів поширення інформаційних атак, з огляду на їхню масштабність, швидкість розповсюдження контенту, а також широку аудиторію користувачів. Інформаційні атаки в таких середовищах можуть набувати різних форм — від фейкових новин та маніпулятивних наративів до скоординованих кампаній з дезінформації, спрямованих на піддрив довіри, дестабілізацію суспільства або дискредитацію певних осіб чи інституцій.

Ефективна протидія цим загрозам вимагає комплексного підходу, який охоплює як технологічні інструменти, так і організаційні, правові та освітні заходи. З технічної точки зору, одними з найдієвіших засобів протидії є системи штучного інтелекту для автоматичного виявлення фейкових акаунтів,

ботів та поширення неправдивої інформації. Особливу роль відіграють алгоритми машинного навчання, які здатні виявляти патерни дезінформаційної активності та блокувати її поширення на ранніх етапах. Крім того, важливим аспектом є участь самих платформ соціальних мереж у забезпеченні інформаційної безпеки. Багато компаній упроваджують політики модерації контенту, партнерства з фактчекінговими організаціями, інструменти для перевірки джерел та прозорості реклами. Проте ефективність таких заходів часто залежить від політичної волі, доступу до даних і балансу між безпекою та свободою слова. Не менш значущою складовою є підвищення цифрової грамотності користувачів. Освітні кампанії, спрямовані на формування критичного мислення, здатність ідентифікувати фейки, розуміння механізмів маніпуляції — усе це створює умови для більш стійкого до інформаційних атак суспільства.

Таким чином, боротьба з інформаційними атаками у соціальних мережах повинна здійснюватися на кількох рівнях — технічному, правовому, соціальному та освітньому. Лише інтеграція зусиль державних структур, бізнесу, наукової спільноти та громадянського суспільства дозволить створити ефективну систему протидії сучасним інформаційним загрозам у цифровому середовищі.

ВИСНОВКИ

В результаті дослідження мета кваліфікаційної роботи була досягнута, завдання виконані, отже в результаті виконаних завдань було з'ясовано:

1. У результаті виконання завдання було з'ясовано, що соціальні мережі стали невід'ємною складовою сучасного суспільного життя, істотно впливаючи на всі його сфери — від особистісної комунікації до глобальних соціальних процесів. Сутність соціальних мереж полягає в створенні та підтримці зв'язків між людьми, обміні інформацією, формуванні віртуальних спільнот і цифрової ідентичності. Соціальні мережі відіграють ключову роль у трансформації способів комунікації, поширенні знань, формуванні громадської думки, а також у розвитку громадянського суспільства. Вони виступають інструментом соціалізації, самовираження, мобілізації на соціально важливі дії та каналом зворотного зв'язку між владою й громадянами. Значення соціальних мереж полягає також у їхньому впливі на економічні, політичні та культурні процеси. Вони стали потужним засобом маркетингу, інструментом політичної агітації та платформою для кроскультурного обміну. Водночас, використання соціальних мереж супроводжується низкою ризиків: поширенням дезінформації, кібербулінгом, маніпуляцією масовою свідомістю, що зумовлює необхідність формування цифрової культури та медіаграмотності.

Таким чином, соціальні мережі — це багатогранне явище, що одночасно відкриває нові можливості для особистості й суспільства та породжує нові виклики, які потребують комплексного вивчення й осмислення.

2. Інформаційні війни стали новою формою протистояння між державами, в якій ключовими інструментами є медіа, соціальні платформи, кіберпростір і пропагандистські наративи. Цей тип конфлікту не має чітких меж, може вестися без офіційного оголошення війни та впливати на політичні, економічні й соціальні процеси в країнах-цілях. Інформаційні війни спрямовані на деморалізацію населення, послаблення інституцій, створення нестабільності та контроль над інформаційним середовищем. У міжнародних

відносинах це явище дедалі частіше виступає як інструмент «м'якої сили», що дозволяє досягати стратегічних цілей без прямого застосування військової сили.

Інформаційні війни стали важливим компонентом міжнародної політики, використовуючись державами та недержавними акторами для досягнення стратегічних цілей. Вони охоплюють пропаганду, маніпуляцію громадською думкою, поширення фейкових новин та хакерські атаки, що можуть впливати на вибори, конфлікти та міжнародні відносини.

3. У процесі систематизації типології проявів інформаційно-психологічних операцій (ІПСО) в соціальних мережах під час війни визначено сутність інформаційно-психологічних операцій як складової інформаційної війни, що передбачає цілеспрямований вплив на свідомість, емоції, поведінку та оцінки цільової аудиторії з метою досягнення політичних, військових чи ідеологічних цілей. Встановлено, що соціальні платформи є ефективними каналами поширення маніпулятивного контенту завдяки швидкості комунікації, вірусному поширенню інформації, можливості анонімності та використання алгоритмів персоналізації. В процесі систематизації типологій проявів ІПСО в соціальних мережах віднесли основні види: дезінформація (поширення фейкових новин, викривлення фактів, псевдоекспертні коментарі), психологічний тиск (залякування, нагнітання тривожності, створення атмосфери безнадії), маніпуляція громадською думкою (штучне створення інформаційних приводів, використання ботів та тролів, інформаційне повторення), розпалювання внутрішніх конфліктів (поляризація суспільства, міжетнічна чи міжрегіональна ворожнеча), підлив довіри до державних інституцій та армії (дискредитація керівництва, поширення чуток про зраду чи некомпетентність).

Отже, ІПСО мають адаптивний характер і змінюються відповідно до ситуації на фронті, внутрішньої соціальної напруги, актуального порядку денного та реакції населення.

4. У сучасному світі інформація стала не менш важливою зброєю, ніж традиційні військові засоби. Країни дедалі частіше використовують інформаційні інструменти для впливу на політичні процеси, дестабілізації соціуму супротивника, підриву довіри до інституцій та маніпуляції громадською думкою. Ця тенденція свідчить про подальше посилення ролі інформаційних війн у глобальній геополітиці. Штучний інтелект, великі дані, соціальні мережі та інші цифрові інструменти розширюють можливості для ведення інформаційної боротьби. Атаки стають більш точними, цілеспрямованими та складними для виявлення. Наприклад, генерація фейкових відео (deepfake) чи бот-мережі здатні формувати хибну реальність і впливати на масову свідомість.

У майбутньому не лише держави, але й приватні компанії, хакерські угруповання та окремі особи братимуть активну участь у інформаційних війнах. Це ускладнює ідентифікацію джерела атаки, робить інформаційний простір більш вразливим і нестабільним. Протидія інформаційним війнам вимагатиме комплексного підходу, що включатиме розвиток медіаграмотності серед населення, створення ефективних систем кібербезпеки, моніторинг інформаційного простору та міжнародне співробітництво. Особливо важливо навчити громадян критично сприймати інформацію та розпізнавати маніпуляції.

Отже, перспективи розвитку інформаційних війн свідчать про те, що в майбутньому інформація дедалі більше використовуватиметься як стратегічна зброя. Відповідно, ключовим завданням для держав, організацій та окремих громадян стане не лише технічний захист, а й формування критичного мислення, стійкості до маніпуляцій та здатності зберігати інформаційну автономію у глобалізованому світі. Сучасні технології, такі як штучний інтелект, блокчейн, OSINT-аналітика та кібербезпека, відкривають нові можливості для виявлення та нейтралізації інформаційних загроз. Однак, ефективна протидія вимагає комплексного підходу, що поєднує технологічні, правові та освітні заходи.

5. У ході узагальнення було встановлено, що сучасні технології відіграють ключову роль у протидії інформаційним війнам, відкриваючи нові можливості для виявлення, нейтралізації та запобігання інформаційним загрозам. Штучний інтелект та машинне навчання ефективно використовуються для автоматизованого виявлення фейкових новин, бото-активності, маніпулятивного контенту та інформаційних атак. Завдяки цим інструментам значно скорочено час реагування на інформаційні загрози. Аналітика великих даних (Big Data) дає змогу оперативно аналізувати інформаційні потоки в соціальних мережах, виявляючи джерела дезінформації, ключові наративи та тенденції їх поширення. Технології блокчейну можуть забезпечити прозорість і достовірність джерел інформації, сприяючи формуванню довіри до офіційних каналів комунікації. Кібербезпека та інструменти цифрової гігієни є важливою складовою технологічної протидії інформаційним впливам, адже забезпечують захист інформаційної інфраструктури від зовнішніх втручань. Розвиток цифрової грамотності населення, що також базується на використанні технологій (наприклад, онлайн-курсів, мобільних застосунків тощо), підвищує стійкість суспільства до маніпуляцій.

Отже, сучасні технології значно розширюють можливості протидії інформаційним війнам, проте їх ефективність залежить від балансу між безпекою, етикою та свободою. Технологічна перевага сама по собі не гарантує захисту — необхідне поєднання технічних рішень, освітніх програм, законодавчих ініціатив та міжнародного співробітництва. Тільки комплексний підхід забезпечить стійкість до нових форм інформаційної агресії у цифрову епоху.

СПИСОК ВИКОРИСТАНИХ ДЖЕРЕЛ ТА ЛІТЕРАТУРИ

Відео ресурси

1. 24 канал. Погрожує ударами по Німеччині: Соловйов назвав Шольца та Бербок «нацистами» через танки Leopard
URL: https://24tv.ua/solovyov-nazvav-sholtza-berbok-natsistami-cherez-tanki-leopard_n2242962
2. FREEDOM. План по «денацифікації». Чего добивался Путін.
URL: <https://www.youtube.com/watch?v=Aya7KX4SQwM>
3. UAKINO.LU Двоє бійців. [URL:https://uakino.lu/13572-dva-bojca-1943.html](https://uakino.lu/13572-dva-bojca-1943.html)
4. Фотографії Старого Львова. Уривок з пропагандистського кіножурналу «Die Deutsche Wochenschau». URL: <https://www.youtube.com/watch?v=-nmue6FfWUM>

Література

1. «Коммерсант».Путін: ти ж розумієш, Джордж, що Україна — це навіть не держава!. URL: <https://www.unian.ua/politics/108324-putin-ti-j-rozumiesh-djordj-scho-ukrajina-tse-navit-ne-derjava.html> (дата звернення: 03.03.2025).
2. Бельська Т. В. Інформаційно-психологічна війна як спосіб впливу на громадянське суспільство та державну політику держави // Вісник Національного університету цивільного захисту України. 2014. Вип. 1. С. 49–56. URL: http://nbuv.gov.ua/UJRN/VNUCZUDU_2014_1_92014 (дата звернення: 10.05.2025).
3. Бойко Ю. В., Ковальська Л. А. Соціальні мережі як зброя та інструмент впливу в умовах інформаційної війни. URL: <file:///D:/Загрузки/9995-Текст%20статті-19911-1-10-20210507.pdf> (дата звернення: 13.04.2025).

5. Боудіш У. Інформаційна війна: сучасна битва за думки. Київ, 2018. С. 10–68.
6. Бугайчук А. Як голосували «за совєтів». Волинь Post. – 2013. –28 жовтня.
7. Бучин М., Kurus Y. Інформаційна війна Росії проти України: особливості та механізми протидії. Гуманітарні візії 2018;Випуск 4, Номер 1: 55-62.
4. Вересень С. «Злочини УПА» Пізнайте правду /С.Вересень // Кобзар. 2010. Інформаційна війна 1939 року: як Кремль пропагував пакт Молотова-Ріббентроп URL: <http://surl.li/qmxls> (дата звернення: 03.03.2025).
8. Вітюк Н. Особливості дискурсу політичної пропаганди в умовах інформаційно-психологічної війни. Збірник наукових праць: психологія. 2019. № 24. С. 29–38.
5. Войтович Н. О., Кравець Р.К. Сучасна інформаційна війна: Росія проти України. Обрії друкарства. 2014. №1. С. 69-78. URL: http://nbuv.gov.ua/UJRN/obdr_2014_1_9 (дата звернення: 13.03.2025).
9. Горбань О. Ю. Інформаційна війна проти України та засоби її ведення // Вісник Національної академії державного управління при Президентові України. 2015. № 1. С. 136–141.
10. Горбатенко Д. С. Комплексний підхід у сфері захисту інформації. Суми: СумДУ, 2013. С. 3
6. Гулай В. В., Базиліук К. Ф.Інформаційно-психологічна складова гібридної війни російської федерації проти України (2014-2021 рр.): теоретико-медологічні засади дослідження. URL: <http://www.baltijapublishing.lv/omp/index.php/bp/catalog/download/237/6326/13362-1?inline=1> (дата звернення: 15.05.2025).
11. Гуріна Н. Інформаційне протиборство – один з головних напрямків політики сучасних міжнародних відносин. Схід. 2004. № 1. С. 54–57.
7. Гурковський В. І. Особливості застосування інформаційної зброї в умовах глобального інформаційного суспільства // Електронне наукове фахове

видання «Державне 124 управління: удосконалення та розвиток». 2010. № 4.
URL: <http://www.dy.nayka.com.ua/?op=1&z=123> (дата звернення: 03.03.2025).

12. Данько Ю. А. Соціальні мережі як форма сучасної комунікації: плюси і мінуси. Сучасне суспільство. 2012. Вип. 2. С. 179–184., с. 180

13. Дубас О. П. Інформаційна війна: нові можливості політичного протистояння. Освіта регіону: політологія, психологія, комунікації. 2010. № 1. С. 69–72.

14. Задихайло Д. Мобілізаційна стратегія економічного розвитку в контексті правового господарського порядку: постановка питання // Вісник Академії правових наук України. Харків: Право, 2007. № 1 (48). С. 158–168.

8. Закон України «Про інформацію». Відомості Верховної Ради України (ВВР). – 1992. – № 48. – с. 650. – URL: <http://zakon3.rada.gov.ua/laws/show/2657-12> (дата звернення: 03.03.2025).

9. Зіменко О. Є. Інформаційний вплив: поняття та еволюція в сучасній науковій думці. URL: <file:///D:/Загрузки/246728-Текст%20статті-566717-1-10-20211210.pdf> (дата звернення: 14.03.2025).

15. Калетнік В., Калетнік Н. Інформаційна безпека і кіберзахист як сучасна інтелектуальна зброя. Молодий вчений. 2021. № 5 (93). С. 305–311.

16. Качковська Леся, Галина Малеончук, Дмитро Зінюк. «Інформаційний вплив в умовах гібридної війни.» Міжнародні відносини, суспільні комунікації та регіональні студії 3 (14) (2022): 87-102.

17. Клімов А. Д. Інформаційна війна як комунікативна технологія формування та розвитку військово-мобілізаційного потенціалу населення. Київ: К-й. Ін-т. І. Сікорського, 2018. 140 с.

18. Колесніков В. О., Жупінський П. О.1, Тимошенко Р. Р. Актуальність мобілізаційної стратегії розвитку економіки держави в аспекті забезпечення обороноздатності.-Центр воєнно-стратегічних досліджень Національного університету оборони України імені Івана Черняхівського, Київ/Інститут інформаційних технологій Національного університету оборони України імені Івана Черняхівського, Київ. 2016. 8 с.

10. Конституція України. Відомості Верховної Ради України (ВВР). – 1996. – № 30. – с. 141. – URL: <http://zakon5.rada.gov.ua/laws/show/254%D0%BA/96-%D0%B2%D1%80> (дата звернення: 03.03.2025).
19. Кремень Т. В. Політична мобілізація в соціально-медійному вимірі: монографія. Київ: Грамота, 2013. 256 с У 2006 р., с. 65
11. Крисько В. Г. Секрети психологічної війни. Перипетії психологічної війни. URL: <http://www.evartist.narod.ru/text19/011.htm> (дата звернення: 03.03.2025).
20. Куцька О. Агітація, пропаганда, інформаційно-психологічна війна: історія виникнення термінів, їх значення та взаємозв'язок // Наукові праці: серія «Історія». Київ, 2018. 8 с.
12. Лавринцев Н. Що таке ІПСО і як не дати ворогам себе залякати: поради військового психолога. Апостроф. ua: сайт. URL: <https://apostrophe.ua/ua/article/lime/learn/2022-10-11/chto-takoe-ipso-i-kak-ne-datvragam-sebya-zapugat-sovetyi-voennogo-psihologa/48484> (дата звернення: 25.05.2025).
13. Левченко О.В. Еволюція гібридної війни Російської Федерації проти України. URL: <file:///D:/Загрузки/176935-Текст%20статті-398699-1-10-20191004.pdf> (дата звернення: 14.03.2025).
21. Лушагіна Т., Губницька О. Соціальні мережі як інструмент політичних маніпуляцій. Стратегії країн Причорноморського регіону в геополітичному просторі: матеріали міжнар. наук. конференції, м. Миколаїв, 15–18 черв. 2023, Миколаїв, 2023. С. 75–76.
22. Лушагіна Т.В. Особливості комунікації місцевих органів влади щодо відновлення зруйнованих та деокупованих громад. Державне управління та регіональний розвиток, 2024 (24), 565-588. <https://doi.org/10.34132/pard2024.24.11>
23. Лушагіна Т.В. Сучасні технології маніпулювання масовою свідомістю // Ольвійський форум – 2024: стратегії країн Причорноморського

регіону в геополітичному просторі. Актуальні проблеми соціології, політології, філософії : XXI Міжнар. наук. конф. 20–23 черв. 2024 р., м. Миколаїв : тези / М-во освіти і науки України ; ЧНУ ім. Петра Могили ; Нац. акад. наук України ; Півд. наук. центр НАН і МОН України ; Ін-т укр. археографії та джерелознавства ім. М. С. Грушевського НАН України ; Держ. архів Миколаївської обл. ; ДУ «Нац. наук. центр радіаційної медицини НАМН України» ; Донецький нац. медичний ун-т ; Technical University of Moldova (Moldova) ; Jan Dlugosz University in Czestochowa (Poland) ; Adam Mickiewicz University (Poland) ; Leipzig University of Applied Sciences (Germany) ; Rzeszow University of Technology (Poland) ; Ca` Foscari University (Italy). – Миколаїв : Вид-во ЧНУ ім. Петра Могили, 2024. – 44 с.

24. *Лушагіна Т.В., Богуславська Є.* Перспективи розвитку інформаційних війни

25. Маєвський О., Борчук С. Креолізовані тексти на сторінках енциклопедичних видань (на прикладі провідних енциклопедичних проєктів СОСР та російської федерації). Український історичний збірник, Вип. 20, 2018. 12 с.

26. Макаренко Л. П. Еволюція форм та методів ведення інформаційної війни. Науковий огляд Том 4, № 3 (2014).

27. Макаренко Л. П. Сайти соціальних мереж як інструмент ведення сучасної інформаційної війни // Гілея: науковий вісник. 2014. Вип. 84. С. 451–456.

28. Максимович М. Медійні аспекти путінської аудіовізуальної пропаганди. Теле- та радіожурналістика. 2015. Вип. 14. С. 195-202. URL: http://nbuv.gov.ua/UJRN/Tir_2015_14_28 (дата звернення: 24.03.2025).

29. Маркова М. В., Марков А. Р. Інформаційно-психологічна війна як нова загроза здоров'ю населення України: реальність небезпеки та напрями протидії. Здоров'я України. Неврологія. Психіатрія. Психотерапія. 2016. № 1 (36). С. 51- 53.

30. Меренюк С., Меренюк Х. Україно-російська гібридна війна. Україна в умовах трансформації міжнародної системи. Львів, 2019. С. 47–51.
31. Методичний підхід до оцінювання ефективності здійснення інформаційного (психологічного) впливу у соціальних мережах. СО Сідченко, ОВ Ревін, СВ Залкін, КІ Хударковський Системи обробки інформації, 70-82, 2023
32. Молоткіна Ю. Вербальне маніпулювання «фабрики тролів» у контексті антиукраїнської пропаганди кремля в англомовному дискурсі соціальних мереж tiktok та twitter. URL: <https://sdc-journal.com/index.php/journal/article/view/476/387> (дата звернення: 17.03.2025)
33. Музика О.О. Особливості роботи над професійно-орієнтованим завданням з курсу «Загальна психологія» // Професійно-орієнтовані завдання з психології: Навчальний посібник / За ред. О.Л. Музики. – Житомир: Вид-во ЖДУ ім. І.Франка, 2010. – С. 24-51. (з грифом МОН України)
34. Нестеряк Ю. В., Васьківська О. Є. Навчально методичний комплекс із дисципліни «Інформаційні війни». Київ: Національний авіаційний університет, 2020. 11 с.
35. Олександренко А. Інформаційна війна російської федерації проти України. URL: <file:///D:/Загрузки/12711-Текст%20статті-25263-1-10-20221017.pdf> (дата звернення: 14.03.2025).
36. Офіцинський Р.А. Микита Хрущов як викривач сталінізму: ювілейні коментарі з геополітичної межі Захід-Схід. / Р.А. Офіцинський // Україна ХХ ст.: культура, ідеологія, політика. – Вип. 10. – С. 123 – 136.
37. Парута О. Суб'єкт правової ідентичності: загальнотеоретичні аспекти Європейські перспективи. 2013. № 13. С. 12-16.
38. Парфенюк І. М. Інструментарій інформаційних війн: традиційні та новітні засоби // Вісник Книжкової палати. 2019. № 1. С. 7–10.
39. Паршин І. Термін «Мала Русь» у документах XIV століття // Княжа доба: історія та культура. 2019. Вип. 13. С. 215–224.

40. Патаркін Є.Д. Педагогічний дизайн соціальної мережі Scratch. Освітні технології і суспільство (Education Technology & Society). 2013. Т. 16. № 2. С. 505–528.
41. Патлашинська І.В. Сучасна російсько-українська інформаційна війна: завдання, методи та особливості використання. URL: <http://www.regionalstudies.uzhnu.uz.ua/archive/28/15.pdf> (дата звернення: 14.05.2025).
42. Печерський А. ІПСО в українському інфопросторі: як розпізнати? АрміяInform. URL: <https://armyinform.com.ua/2022/08/05/ipso-v-ukrayinskomu-infoprostor-i-yak-rozpiznaty/> (дата звернення: 14.03.2025).
43. Платформа прав людини. ЗМІ і війна: особливості поширення інформації та фото під час воєнного стану. URL: <https://ppl.org.ua/zmi-i-vijna-osoblivosti-poshirennya-informacii-ta-foto-pid-chas-voennogo-stanu.html> (дата звернення: 16.03.2025).
44. Політичний терор і тероризм в Україні. XIX – XX ст. історичні нариси. – К.: Наукова думка., 2002. – 950 с.
45. Присяжнюк М., Жарков Я. Аналіз засобів ведення інформаційної боротьби з використанням інформаційних технологій, форм і способів їх застосування. Вісник Національного технічного університету України «Київський політехнічний інститут». Філософія. Психологія. Педагогіка. 2011. № 3. С. 70-74.
46. Путін о 5-й ранку оголосив про початок операції на Донбасі // Радіо Свобода URL: <https://www.radiosvoboda.org/a/31719676.html> (дата звернення: 18.04.2025).
47. Салата О. О. Інформаційне протистояння між Німеччиною та СРСР в історіографії // Київські історичні студії. Вип. 1(6). Київ: Київ. ун-т ім. Б. Грінченка, 2018. С. 52–62.
48. Свідницька І. В. Соціально-комунікативні технології в умовах інформаційно-психологічних війн (на прикладі TikTok) URL:

<file:///D:/Загрузки/9983-Текст%20статті-19887-1-10-20210506.pdf>

(дата

звернення: 15.03.2025).

49. Семен О.Д., Зелінська О.В. «Вплив інформаційних технологій на захист населення під час війни». Матеріали I Міжнародної науково-практичної конференції, 15.12.2022.

50. Січкаренко Г., Овсієнко А., Яременко С. Особливості інформаційно-комунікаційних практик в соціальних мережах сьогодні. Наукові інновації та передові технології. 2022. № 8(10).

51. Скіцько, П. Складаний, Р. Ширшов, М. Гуменюк, М. Ворохоб. Загрози та ризики використання штучного інтелекту. URL: <https://csecurity.kubg.edu.ua/index.php/journal/article/view/520/408> (дата звернення: 13.03.2025).

52. Субота, Є. (2020). Вплив телебачення та соціальних мереж на формування медіа реальності. Український інформаційний простір, (1(5), 243–252. [https://doi.org/10.31866/2616-7948.1\(5\).2020.206132](https://doi.org/10.31866/2616-7948.1(5).2020.206132) (дата звернення: 14.05.2025).

53. Турчин А.В. Класифікація соціальних мереж. Актуальні задачі та досягнення у галузі кібербезпеки: матеріали Всеукраїнської науковопрактичної конференції 23 – 25 листопада 2016 р., м.Кропивницький. URL: <https://core.ac.uk/download/pdf/84825408.pdf> (дата звернення 10.11.2023 (дата звернення: 15.05.2025).

54. Федонюк С.В. Інформаційні війни: Робоча навч. прогр.- Луцьк: РВВ «Вежа» ВНУ ім. Лесі Українки, 2008. 28 с.

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

56. Фролова Н. В. Особливості використання соціальних мереж у діяльності органів публічної влади. Публічне адміністрування: теорія та практика, 2019. Вип. 1(21). URL: [http://www.dridu.dp.ua/zbirnik/2019-01\(21\)/12.pdf](http://www.dridu.dp.ua/zbirnik/2019-01(21)/12.pdf) (дата звернення 29.11.2023), с. 5 (дата звернення: 12.03.2025).

57. Холод Г. Я. Інформаційне протистояння в друкованих ЗМІ на прикладі газети «Кіно» та «Кіно-газети» (1930). Соціальні комунікації: теорія і практика, 2016. Т. 3. С. 188–198.
58. Христенко В. Є. Маніпулювання свідомістю в умовах гібридної війни: психологічний аспект. URL: http://repositsc.nuczu.edu.ua/bitstream/123456789/5929/1/Khrystenko_monogr.pdf (дата звернення: 13.03.2025).
59. Чмир Я. І. Інформаційна війна як ключова загроза демократичному державотворенню України. Державноуправлінські студії. 2019. № 10. С. 1–11.
60. Шептицька Л., Ременяк, О., Захарчин, Н. Досвід інформаційних війн в історії та сучасності як об'єкт досліджень сучасної науки та освіти. 2024. Українські історичні студії, 35-43
61. Шмаленко Ю. І. Використання інформаційно-психологічних операцій (ІПСО) у сучасній війні в Україні // Європейські орієнтири розвитку України в умовах війни та глобальних викликів ХХІ століття: синергія наукових, освітніх та технологічних рішень : у 2 т. : матеріали Міжнар. наук.-практ. конф. (м. Одеса, 19 травня 2023 р.) / за заг. ред. С. В. Ківалова. Одеса, 2023. Т. 1. С. 226-229.
62. Шумка А. В. Черник П. П. Інформаційно-мережева війна – нова форма міждержавного протиборства початку ХХІ ст. Військово-науковий вісник. 2013. Вип. 19. С. 243-255.
63. Шумка А. В., Черник П. П. Теоретичні аспекти інформаційних війн та національна безпека. Грані. 2015. №9. С. 10-16. URL: http://nbuv.gov.ua/UJRN/Grani_2015_9_4 (дата звернення: 13.03.2025).
64. Ягупов В. Морально-психологічне забезпечення. URL: <http://medbib.in.ua/psihologichni-viyni-operatsiji-yakskladovi36879.html> (дата звернення: 13.04.2025).
65. Anderson-Butcher, D., Ball, A., Brzozowski, M., Lasseigne, A., Lehnert, M., & McCormick, B. L. (2010). Adolescent Weblog Use: Risky or Protective? Child and Adolescent Social Work Journal, 27 (1), 63–77. <https://doi.org/10.1007/s10560-010-0193-x> [in English].

66. Barnes J. A. Class and committees in a Norwegian island parish. URL: <http://garfield.library.upenn.edu/classics1987> (дата звернення: 21.12.2023)
67. Beyond Facebook: A look at social network history. The economic times. 19 May 2012. URL:
68. Bryan Frederick, Mark Cozad, Alexandra Stark Understanding the Risk of Escalation in the War in Ukraine. RAND Corporation, 2023, p 12.
69. Chernobrov D., Briant E. L. Competing propagandas: How the United States and Russia represent mutual propaganda activities. Politics. URL: <https://doi.org/10.1177/0263395720966171>
70. Countering disinformation with facts - Russian invasion of Ukraine. URL: https://www.international.gc.ca/world-monde/issues_developpement-enjeux_developpement/response_conflict-reponse_conflits/crisis-crisis/ukraine-fact-fait.aspx?lang=eng (дата звернення: 13.03.2025).
71. Cox L. Planning for psychological operations: a proposal / Air Command and Staff College, Maxwell Air Force Base, Montgomery, Alabama, 1997. 89 p.
72. Frizell J. War and modern taxation. Global Taxation. 2022. Vol. 1. P. 43–66.
73. Jerome Gavin Information and Misinformation in the Russia Ukraine war. URL : <https://www.visionofhumanity.org/information-and-misinformation-in-the-russia-ukraine-war/> (дата звернення: 30.12.2023)
74. Kornieiev V., Ryabichev V., Glushkova T. Fake News and Content Manipulation Under Russian Information Aggression. Przegląd Strategiczny. 2023. No. 15. P. 187–209.
75. Libicki M. C. What is information warfare? : National Defense University, Institute for National Strategic Studies, 1995.
76. Macdonald S. Propaganda and Information Warfare in the Twenty-First Century: Altered Images and Deception Operations. Taylor & Francis Group, 2007. 220 p.

77. Ryzhuk O. Providing information security of Ukraine during the hybrid war. *Politicus*. 2018. Vol. 2. P. 147–150.

78. Sheldon, P. (2008). The Relationship Between Unwillingness-to-Communicate and Students' Facebook Use. *Journal of Media Psychology Theories Methods and Applications*, 20 (2), 67–75. <https://doi.org/10.1027/1864-1105.20.2.67> (дата звернення: 13.03.2025).

79. SPRAVDI 10 фіаско російської пропаганди у 2022 році. URL:<https://spravdi.gov.ua/10-fiasko-rosijskoyi-propagandy-u-2022-roczy/> (дата звернення: 13.03.2025)

80. Turns D. Cyber Warfare and the Notion of Direct Participation in Hostilities. *Journal of Conflict and Security Law*. 2012. Vol. 17, no. 2. P. 279–297.

81. Viacheslav Gusarov The Russians came Pt.2 How much does the Russian information war cost?. URL: <https://web.archive.org/web/20171222052510/http://sprotyv.info/en/news/kyiv/russians-came-pt2-how-much-does-russian-information-war-cost>. WaybackMachine (дата звернення: 13.05.2025).

82. War of the Waves: Radio and Resistance During World War II / S. Gagliarducci et al. SSRN Electronic Journal. 2019. URL: <https://doi.org/10.2139/ssrn.3170796> (дата звернення: 23.04.2025).