

МІНІСТЕРСТВО ОСВІТИ І НАУКИ УКРАЇНИ
Харківський національний університет імені В.Н. Каразіна
Навчально-науковий інститут «Інститут державного управління»

До захисту

Завідувач кафедри публічної політики д.держ.упр., проф.

Дзюндзюк В.Б.

/Підпис/

**ВИКОРИСТАННЯ СОЦІАЛЬНИХ МЕРЕЖ У ГІБРИДНІЙ ВІЙНІ ТА
ЇХ ВПЛИВ НА ГРОМАДСЬКУ ДУМКУ**

Кваліфікаційна робота на здобуття освітнього ступеня «магістр»

281 Публічне управління та адміністрування

28 Публічне управління та адміністрування

Виконавець

здобувач 2 курсу, гр. ППГЗ-2-23

М. С. Коваленко

Науковий керівник

д.держ.упр., проф.

О.В. Орлов

Харків – 2024

ЗМІСТ

ВСТУП.....	3
РОЗДІЛ 1. ТЕОРІЯ ТА МЕТОДОЛОГІЯ ВИКОРИСТАННЯ СОЦІАЛЬНИХ МЕРЕЖ У ГІБРИДНІЙ ВІЙНІ.....	8
1.1. Стан наукової розробки проблеми використання соціальних мереж у гібридній війні.....	8
1.2. Концептуальні підходи та зарубіжний досвід використання соціальних мереж у гібридній війні.....	13
1.3. Сутність явища "Використання соціальних мереж у гібридній війні".....	16
РОЗДІЛ 2. СУЧАСНИЙ СТАН ВИКОРИСТАННЯ СОЦІАЛЬНИХ МЕРЕЖ У ГІБРИДНІЙ ВІЙНІ ЩОДО УКРАЇНИ ТА УКРАЇНСЬКОГО СУСПІЛЬСТВА.....	20
2.1. Організаційні, правові, функціональні та інші аспекти використання соціальних мереж у гібридній війні.....	20
2.2. Оцінка стану використання соціальних мереж у гібридній війні.....	37
2.3. Суперечності у розвитку використання соціальних мереж у гібридній війні: аналіз і шляхи вирішення.....	43
Розділ 3. Шляхи розвитку Використання соціальних мереж у гібридній війні.....	50
3.1. Тенденції розвитку, можливі інструменти та механізми використання соціальних мереж у гібридній війні.....	50
3.2. Організаційно-управлінські та правові заходи використання соціальних мереж у гібридній війні.....	52
3.3. Рекомендації щодо використання соціальних мереж у гібридній війні.....	56
ВИСНОВКИ.....	6

СПИСОК ВИКОРИСТАНИХ ДЖЕРЕЛ.....	66
---------------------------------	----

ВСТУП

Проблема використання соціальних мереж у гібридній війні є надзвичайно актуальною та активно досліджується як у міждисциплінарному, так і в спеціалізованому аспектах. вченими з різних галузей знань: політології, соціології, комунікацій, психології та інших. Вчені вивчають це явище в контексті інформаційної війни, психологічного впливу, дезінформації, кібербезпеки, соціальної психології та політичних наук.

Останні роки спостерігається значний прогрес у розумінні цього феномену, проте залишається багато невирішених питань.

Актуальність цієї теми полягає в тому, що українські державні органи мають великий потенціал як для використання соціальних мереж. Аналіз воєнних дій та збройних конфліктів XX століття та на початку XXI століття веде до висновку, що сучасна епоха є епохою гібридних війн Соціальні мережі є ключовим елементом гібридної війни, оскільки вони забезпечують швидкий доступ до аудиторії та можливість маніпулювати громадською думкою. Методологія їх використання включає розробку інформаційних кампаній, автоматизоване поширення контенту, експлуатацію алгоритмів платформ і психологічний вплив. Для зменшення їх негативного впливу необхідно впроваджувати комплексні заходи, спрямовані на підвищення обізнаності, вдосконалення технологій і зміцнення співпраці між урядом, громадськістю та міжнародними партнерами.

Проблема використання соціальних мереж у гібридній війні активно досліджується як у міждисциплінарному, так і в спеціалізованому аспектах. [11] Вчені вивчають це явище в контексті інформаційної війни, психологічного впливу, дезінформації, кібербезпеки, соціальної психології та політичних наук, а впровадження цих технологій набуває вирішального значення для безпеки та розвитку держави. Вивчення концептуальних підходів до гібридної війни і її компонентів займає значне місце в сучасних міжнародних та внутрішніх

академічних дискусіях [1, 2. 5. 9, 10, 14]. Визнані аналітики зі США, як-от F. Hoffman [94], Michael Rühle, Clare Roberts. [97], здобули репутацію як провідні теоретики у цій галузі. Водночас, на тлі безпосереднього впливу російської гібридної агресії проти України, українські вчені такі як Є. Магда [47], В. Горбулін[16], С. Грабовський [17], Я. Деркаченко [19], М. Дзюба [21] активно долучилися до дослідження цієї проблематики, пропонуючи глибокий аналіз ситуації на основі безпосереднього досвіду. Теорія гібридної війни викладена в працях вітчизняних і зарубіжних науковців. На особливу увагу заслуговують публікації О. Курбана [38, 39, 40], В. Бебіка [2], Л. О.Саєнко [65] та інших дослідників специфіки феномена «гібридної війни». Певна група вчених вважає, що як класичне можна використовувати визначення гібридної війни Френка Хоффмана, який вважає, що гібридна війна включає різноманітні методи ведення конфлікту, зокрема традиційні військові операції, дії нерегулярних збройних груп, терористичні акти, беззаконня та неправомірне застосування насильства й примусу. Таку війну можуть вести як державні, так і недержавні суб'єкти.

Основні напрямки досліджень можна розділити на декілька основних напрямків: Аналіз методів маніпуляції в соціальних мережах, такі як поширення фейкових новин, створення бот-ферм, використання тролів, таргетована реклама тощо. Дослідження впливу на різні групи населення, коли Особлива увага приділяється вивченню того, як різні групи населення (за віком, освітою, політичними поглядами) сприймають інформацію в соціальних мережах та наскільки вони вразливі до маніпуляцій. Вивчення психологічних механізмів впливу, а саме, як соціальні мережі впливають на емоції, когнітивні процеси та поведінку людей. Розробка методів виявлення та протидії дезінформації метою яких є створення інструментів для автоматичного виявлення фейкових новин, ботів та інших ознак маніпуляцій.

Незважаючи на високий науковий інтерес, питання комплексного підходу до використання соціальних мереж у гібридній війні ще не вирішені. Тому необхідні

подальші дослідження, щоб зрозуміти, як найкраще адаптувати ці технології до потреб українського суспільства та перш за все до проблем безпеки.

Метою дослідження є аналіз можливостей, викликів та ризиків використання соціальних мереж у гібридній війні та розробка рекомендацій щодо використання соціальних мереж для забезпечення перемоги у війні.

Для досягнення цієї мети було визначено такі завдання:

1. Проаналізувати світовий досвід використання соціальних мереж у гібридній війні та їх вплив на громадську думку.
2. Визначити основні переваги та можливі ризики, що несуть соціальні мережі у гібридній війні.
3. Оцінити поточний стан використання соціальних мереж у гібридній війні України та дослідити бар'єри, що стримують його розвиток.
4. Розробити рекомендації щодо ефективного використання соціальних мереж у гібридній війні з урахуванням історичного контексту.
5. Дослідити потенційний вплив соціальних мереж на громадську думку.

Об'єктом дослідження є інформаційна політика у гібридній війні.

Предметом дослідження є використання соціальних мереж у гібридній війні та їх вплив на громадську думку.

У цьому дослідженні використано низку методів для комплексного аналізу питання застосування штучного інтелекту в державному управлінні:

1. Аналіз і синтез – вивчення наукової літератури, законодавства та практичних прикладів впливу соціальних мереж на громадську думку в різних країнах. Ці методи дозволили систематизувати наявні знання та узагальнити досвід світової практики.
2. Порівняльний аналіз – для вивчення різних моделей розвитку соціальних мереж та їх впливів на громадську думку в інших країнах та їх адаптації до українських реалій. Цей метод допоміг виявити сильні та слабкі сторони різних підходів.

3. Експертне опитування- зібрано думки експертів у сфері ІТ та державного управління щодо можливостей та ризиків використання соціальних мереж у гібридній війні та їх вплив на громадську думку. Це дозволило врахувати думки експертів.

4. Аналіз великих даних – для оцінки потенційного впливу соціальних мереж на перебіг гібридної війні та їх вплив на громадську думку, зокрема з точки зору оптимізації ресурсів та підвищення ефективності розподілу державних ресурсів.

5. Методи моделювання – для прогнозування наслідків реголювання соціальних мереж та їх вплив на громадську думку в українське державне управління, що допомогло визначити можливі економічні та соціальні наслідки цього процесу.

6. Системний підхід, який комплексно досліджує взаємозв'язки між технологічними змінами, управлінськими процесами та суспільними потребами.

Практичне значення отриманих результатів полягає в тому, що вони можуть бути використані для вдосконалення управлінських процесів шляхом врахування впливу соціальних мереж на громадську думку.

Основними аспектами практичної цінності результатів дослідження є:

1. Підготовка рекомендацій органам державної влади щодо використання соціальних мереж у гібридній війні та посилення їх впливів на громадську думку. Ці рекомендації стануть основою для створення програм цифрової трансформації та модернізації державних органів.

3. Підвищення якості інформаційної політики – що враховує роль соціальних мереж у гібридній війні та їх вплив на громадську думку, позитивно впливаючи на рівень довіри до державних органів.

4. Оцінка потенційних ризиків та розробка стратегій для їх мінімізації – результати досліджень можуть допомогти спрогнозувати ризики (наприклад,

кіберзагрози та етичні проблеми), пов'язані з використанні соціальних мереж у гібридній війні, та створити механізми для їх уникнення або зменшення.

5. Потенціал для використання в навчальних закладах для підготовки фахівців у сфері державного управління та інформаційних технологій – отримані результати сприятимуть розбудові спроможності у сфері цифрової трансформації державного управління.

Таким чином, результати цього дослідження є корисними не лише для науковців та практиків у сфері державного управління та інформаційних технологій, а й для органів державної влади та державних службовців.

Апробація результатів. Робота містить результати проведених досліджень, спрямованих на обґрунтування положень в галузі державного управління, які розкривають нові можливості для розв'язання проблем запровадження державних механізмів забезпечення безпеки України.

Інформаційною базою дослідження є законодавчі та нормативно–правові акти, що визначають порядок функціонування соціальних мереж в Україні, аналітичні матеріали; вітчизняні та зарубіжні літературні джерела, фактологічна інформація державних органів влади, матеріали офіційних органів України, матеріали та звіти міжнародних організацій. Використано також дані інформаційно–аналітичних бюлетенів та оглядів, довідкову літературу та періодичні видання, матеріали міжнародних і всеукраїнських науково–практичних конференцій, офіційні Інтернет–ресурси.

Структура і обсяг роботи. Магістерська робота складається зі вступу, трьох розділів, дев'яти підрозділів, висновків та переліку використаних джерел. Загальний обсяг роботи становить 78 сторінок Магістерська робота містить 4 рисунка, 4 таблиці, перелік використаних джерел налічує 107 найменувань.

РОЗДІЛ 1. ТЕОРІЯ ТА МЕТОДОЛОГІЯ ВИКОРИСТАННЯ СОЦІАЛЬНИХ МЕРЕЖ У ГІБРИДНІЙ ВІЙНІ

1.1. Стан наукової розробки проблеми використання соціальних мереж у гібридній війні

Соціальні мережі стали важливим інструментом гібридної війни, оскільки вони дозволяють впливати на громадську думку, мобілізувати підтримку, поширювати дезінформацію та підривати довіру до державних інституцій. Їх використання базується на певних теоретичних концепціях і стратегічних підходах. Соціальні мережі є основним середовищем для поширення інформації, яка може впливати на емоції, поведінку та рішення аудиторії.

У рамках гібридної війни коли, інформація використовується як зброя для дестабілізації суспільства або впливу на політичні процеси. Стає вкрай важливим контроль за темами, які обговорюються в суспільстві – Agenda-setting, або представлення подій або проблем у певному контексті для формування бажаної інтерпретації – Framing. Має місце використання соціальних мереж для створення враження підтримки певної думки та ізоляції альтернативних точок зору – Spiral of silence. Вплив через повторення меседжів, використання емоційних тригерів, створення "ефекту присутності" (наприклад, через ботів або фейкові акаунти). Використання принципу "соціального доказу" (якщо багато людей підтримують певну позицію, то вона сприймається як правильна і, таким чином впливаючі на психологічний стан суспільства, що веде до поляризації думок через алгоритми платформ, які підсилюють "інформаційні бульбашки").

2. Використання соціальних мереж у гібридній війні використовує розвинуту методологію створення і розповсюдження контенту, фейкові новини та дезінформація, поширення недостовірної інформації для маніпуляції фактами.

Використання простого та зрозумілого контенту для емоційного впливу – меми та візуальний контент або технології створення відео, де люди виглядають або говорять те, чого не було насправді – дипфейки. Використання ботів і тролів, що автоматизують поширення контенту, задля створення ілюзії підтримки певної позиції. Координація тролів, як механізм організація активності для атак на опонентів, залякування або створення інформаційного шуму.

Створення та підтримка "інформаційних бульбашок", коли алгоритми соціальних мереж надають користувачам контент, який відповідає їхнім інтересам, що підсилює поляризацію суспільства, поширення односторонніх поглядів у вузьких спільнотах для радикалізації їхніх членів.

Планування та проведення скоординованих інформаційних операцій, спрямованих на досягнення стратегічних цілей (наприклад, вплив на вибори, підриг довіри до влади).

Залучення звичайних користувачів до поширення певних меседжів через заохочення, маніпуляцію або ідеологічний вплив. Вплив соціальних мереж на громадську думку та формування суспільного дискурсу коли соціальні мережі визначають порядок денний, які теми обговорюються та які позиції домінують та ведуть до поляризації суспільства – посилення протистояння між різними групами населення через поширення екстремальних позицій та ідеологій.

Можливість маніпуляції виборцями через таргетовану рекламу або дезінформаційні кампанії призводять до підригу довіри до інституцій, зокрема до дискредитації органів державної влади. [49]

Значна увага в методології використання соціальних мереж у гібридній війні направлена на психологічний вплив, що посіяти страх, тривогу та розгубленість, які виникають через масове поширення негативної інформації.

Це перш за все: Поширення фейкових новин, створення та розповсюдження неправдивої інформації з метою маніпуляції громадською думкою. Створення ботферм, автоматизовані акаунти, які використовують для масового поширення

інформації та коментарів. Тролінг – провокування конфліктів та емоційних реакцій у мережі. Таргетована реклама – показ реклами, яка відповідає інтересам та поглядам конкретних користувачів. Генерація deepfake – створення реалістичних, але фальшивих відео та аудіозаписів.

Разом з тим отримують і свій розвиток методи протидії використанню соціальних мереж у гібридній війні, розвиток медіаграмотності – навчання населення розпізнавати дезінформацію та критично аналізувати контент.

Використання технологій штучного інтелекту для виявлення ботів та фейкових акаунтів, впровадження законодавчих заходів для зобов'язання платформ відповідати за поширення дезінформації поширення достовірної інформації, яка спростовує фейки та пропаганду.

Важливим також є обмін досвідом та координація дій між країнами для протидії інформаційним загрозам.

Таким чином, соціальні мережі є ключовим елементом гібридної війни, оскільки вони забезпечують швидкий доступ до аудиторії та можливість маніпулювати громадською думкою. Методологія їх використання включає розробку інформаційних кампаній, автоматизоване поширення контенту, експлуатацію алгоритмів платформ і психологічний вплив. Для зменшення негативного впливу необхідно впроваджувати комплексні заходи, спрямовані на підвищення обізнаності, вдосконалення технологій і зміцнення співпраці між урядом, громадськістю та міжнародними партнерами.[42]

Проблема використання соціальних мереж у гібридній війні активно досліджується як у міждисциплінарному, так і в спеціалізованому аспектах. Учені вивчають це явище в контексті інформаційної війни, психологічного впливу, дезінформації, кібербезпеки, соціальної психології та політичних наук. Розглянемо основні напрямки розвитку наукової думки.

1.1. Інформаційна війна та дезінформація – напрямок вивчення механізмів поширення фейкових новин через соціальні мережі, їхнього впливу на громадську думку та формування політичних уподобань.

Дослідження алгоритмів роботи платформ (Facebook, X (Twitter), YouTube), які сприяють розповсюдженню маніпулятивного контенту. Аналіз ефективності методів контрпропаганди та фактчекінгу.

1.2. Соціальна психологія та поведінкові аспекти має на меті дослідження механізмів маніпулювання емоціями та переконаннями аудиторії через соціальні мережі. Вивчення феноменів поляризації суспільства, створення "інформаційних бульбашок" та радикалізації громадян.

1.3. Кібербезпека та інформаційні технології включає до себе аналіз кіберзагроз, пов'язаних із використанням соціальних мереж у гібридних конфліктах. Розробка технологій для виявлення ботів, тролів, автоматизованих кампаній і дипфейків. Вивчення блокчейн-технологій та штучного інтелекту як засобів захисту інформаційного простору.

1.4. Роль соціальних мереж у політиці та міжнародних відносинах, у виборчих процесах і політичній мобілізації. Дослідження геополітичних стратегій, які включають інформаційні операції в соціальних мережах. Аналіз міжнародних зусиль щодо регулювання дезінформації.

Для аналізу цих напрямків вчені використовують наступні основні дослідницькі підходи

Кількісний аналіз: Використання великих даних (Big Data) для аналізу динаміки поширення інформації, соціальних графів і активності ботів. Дослідження статистичних залежностей між типами контенту та їхнім впливом на аудиторію.

Якісний аналіз: Контент-аналіз повідомлень у соціальних мережах для ідентифікації ключових меседжів, стилів подачі інформації та наративів. Інтерв'ю та фокус-групи для вивчення сприйняття дезінформації різними соціальними групами.

Моделювання та симуляції: Використання комп'ютерного моделювання для симуляції впливу інформаційних кампаній на суспільство. Застосування мережевих моделей для аналізу структур інформаційного впливу.

Інтердисциплінарний підхід: Поєднання методів соціальної психології, комп'ютерних наук, політології та медіазнавства для комплексного аналізу явища.

Теорія та методологія використання соціальних мереж у гібридній війні приділяють велику увагу як закордонні так і вітчизняні вчені. Серед них слід згадати Cass Sunstein (США) з його дослідженням інформаційних каскадів і "інформаційних бульбашок". Shoshana Zuboff (США) [101] та його концепцію "капіталізму спостереження", яка пояснює, як цифрові платформи використовують дані для маніпуляцій.[94] Philip N. Howard (Оксфордський університет): вивчення "кібер-військових кампаній" у соціальних мережах.[107]

З українських вчених, слід відзначити зокрема з Національного інституту стратегічних досліджень та Київського національного університету ім. Т. Шевченка, зосереджені на аналізі використання соціальних мереж у контексті війни з Росією.[80] Праці аналітиків Центру стратегічних комунікацій та інформаційної безпеки України.[81]

Разом з тим існують і актуальні проблеми та прогалини в дослідженнях, що зумевленні здебільшого недостатністю емпіричних даних. Багато досліджень обмежується аналізом окремих кейсів без доступу до великих масивів даних через конфіденційність інформації. Технології, такі як дипфейки та автоматизовані алгоритми, розвиваються швидше, ніж розробляються методи їх виявлення. Досі відсутній міжнародний консенсус щодо механізмів контролю та відповідальності платформ за дезінформацію.

Проведений аналіз дозволяє окреслити перспективи подальших досліджень, які мають бути спрямовані на аналіз нових технологій впливу, вивчення можливостей штучного інтелекту для створення контенту та його використання в інформаційних війнах.

Також потребує подальшого розвитку роботи, що пов'язані з підвищенням ефективності заходів протидії використанню ворогом соціальних мереж у гібридній війні. Аналізу ефективності державних і приватних ініціатив щодо боротьби з дезінформацією (наприклад, фактчекінг).

Цікавим може стати напрям визначення етики використання соціальних мереж, розробка етичних стандартів для платформ і урядів у сфері використання даних та маніпуляції громадською думкою. Інтеграція кібербезпеки та соціальної інженерії, поєднання технічних і соціальних аспектів для більш ефективного захисту інформаційного простору.

Таким чином стан наукової розробки проблеми використання соціальних мереж у гібридній війні перебуває на етапі активного розвитку. Попри значний прогрес у розумінні механізмів маніпуляції та впливу, існує низка викликів, які вимагають міждисциплінарного підходу, міжнародної співпраці та розробки нових методів аналізу й протидії. Соціальні мережі залишаються не лише інструментом, а й самостійним полем сучасних конфліктів.

1.2. Концептуальні підходи та зарубіжний досвід використання соціальних мереж у гібридній війні

Соціальні мережі у гібридній війні використовуються як потужний інструмент для ведення інформаційних операцій, поширення дезінформації, формування громадської думки та дестабілізації суспільств. Зарубіжний досвід демонструє різноманітність стратегій та тактик, що застосовуються в цьому контексті.

Гібридна війна — це поєднання військових, економічних, інформаційних та кібератак для досягнення стратегічних цілей без прямого збройного конфлікту.

Соціальні мережі є ключовим елементом гібридної війни, оскільки дозволяють працювати з великими аудиторіями, швидко поширювати інформацію та маніпулювати громадською думкою.

Створення та поширення контенту, що дестабілізує суспільство або дискредитує політичні інститути. Використання соціальних мереж для "м'якої сили" (soft power), тобто ненасильницького впливу на аудиторію з метою зміни її поведінки або світогляду.

Маніпуляція громадською думкою, формування порядку денного (Agendasetting), поширення інформації, яка привертає увагу до певних проблем або подій. Фреймінг (Framing) – контекстуалізація подій у певному наративі. Створення напруги між різними групами суспільства – їх поляризація.[42]

Збільшення ролі цифрових інструментів гібридної війни, використання ботів, тролів, дипфейків, автоматизованих платформ для генерації контенту. Залучення методів таргетованої реклами для впливу на конкретні групи населення.

Розглянемо зарубіжний досвід використання соціальних мереж.

Наприклад, Росія активно використовує соціальні мережі для інформаційних атак як частину своєї "доктрини Герасимова". Ця доктрина, названа на честь генерала Валерія Герасимова, передбачає поєднання військових і невійськових засобів впливу, де інформаційна війна займає центральне місце. У цьому контексті соціальні мережі стали основним інструментом для дезінформації, психологічного впливу та дестабілізації.

При цьому вона активно використовує тактики дезінформаційних кампаній через фабрики тролів, як-от "Агентство інтернет-досліджень" (Санкт-Петербург). Використання фейкових акаунтів у Facebook та X (Twitter) для втручання у вибори (наприклад, у США в 2016 році). Розповсюдження фейкових новин і пропаганди щодо подій в Україні. [43]

Китай застосовує соціальні мережі для просування державних наративів і придушення опозиційних голосів. Забезпечує координацію кампаній у X (Twitter) і

Facebook для зміцнення наративу про ефективність китайського уряду, та використовує "50 Cent Army" — урядових коментаторів, які поширюють пропаганду в інтернеті. На державному рівні здійснюється заборона західних платформ у Китаї та створення альтернатив (WeChat, Weibo) для контролю над внутрішньою інформаційною сферою.

У США застосовується стратегія використання соціальних мереж для боротьби з тероризмом і контрпропаганди. Розробляються програми моніторингу активності терористичних угруповань у X (Twitter) і Facebook. Впровадження кампаній для протидії радикалізації, таких як "Think Again Turn Away" (Держдеп США). Використання соцмереж для збору розвідданих у рамках кібербезпеки. [48]

Європейський Союз застосовує створення платформи East StratCom Task Force для викриття дезінформації в країнах Східної Європи, кампанії підвищення медіаграмотності серед населення. Законодавчі ініціативи, спрямовані на прозорість реклами та боротьбу з фейковими новинами.

2.5. Близький Схід.

Мабуть вперше відбулось широке використання соціальних мереж як засобу впливу в умовах конфліктів і революцій – під час "Арабської весни" соціальні мережі використовувалися як інструмент мобілізації протестів. Терористичні угруповання, такі як ІДІЛ, застосовували платформи для рекрутування та поширення пропаганди. [48]

Таким чином приходимо до висновку, що соціальні мережі дозволяють охоплювати мільйони людей у режимі реального часу, що робить їх ідеальним інструментом для інформаційних атак. Їх глобальна доступність дозволяє проводити операції на міжнародному рівні без фізичної присутності.

Навіть після закінчення інформаційної кампанії її наслідки можуть впливати на суспільство протягом тривалого часу, а використання штучного інтелекту, алгоритмів і автоматизації значно підвищує ефективність інформаційних операцій.

Тобто, Україні необхідно активно враховувати зарубіжний досвід для зміцнення інформаційної безпеки та протидії гібридним загрозам. Вести власні розробки національної стратегії використання соціальних мереж для боротьби з дезінформацією. Здійснювати інтеграцію міжнародних стандартів регулювання діяльності соціальних платформ, а також спрямовувати зусилля на створення власних цифрових платформ і підвищення медіаграмотності населення.

Соціальні мережі залишаються ключовим елементом сучасних конфліктів, і їх ефективне використання або протидія вимагає комплексного підходу на основі світового досвіду.

1.3. Сутність явища "Використання соціальних мереж у гібридній війні"

Використання соціальних мереж у гібридній війні — це стратегія застосування цифрових платформ для ведення інформаційних операцій, що поєднують військові та невійськові методи впливу. Соціальні мережі стають полем бою, де сторони конфлікту впливають на аудиторії, поширюючи дезінформацію, пропаганду, маніпуляції та інші форми інформаційного тиску.

Основні характеристики явища: швидкість поширення інформації, соціальні мережі забезпечують миттєву доставку контенту мільйонам користувачів; доступність, кожен користувач може стати учасником інформаційного впливу; анонімність, легкість створення фейкових акаунтів дозволяє приховувати справжніх ініціаторів інформаційних атак; висока таргетованість, алгоритми соціальних платформ дозволяють ефективно впливати на конкретні групи людей; двостороння взаємодія, соціальні мережі дають змогу отримувати зворотний зв'язок, адаптуючи інформаційні кампанії в реальному часі.

Цілі використання соціальних мереж у гібридній війні: дестабілізація суспільства, поширення паніки, провокація конфліктів, розкол у суспільстві;

дискредитація державних інституцій, зниження довіри до уряду, армії, правоохоронних органів; формування альтернативної реальності, створення викривленого уявлення про події чи ситуації; вплив на громадську думку, маніпулювання думкою для досягнення політичних, економічних або військових цілей.

Вплив на громадську думку, передбачає перш за все:

1. Поширення дезінформації. Дезінформація — це свідоме поширення фейкових новин, що викривляють реальність.

Приклад: Фейкові новини про події на Донбасі або "утиски російськомовного населення" в Україні.

2. Дезорієнтація населення, формування помилкових переконань, підвищення рівня недовіри до офіційних джерел інформації.

3. Поляризація суспільства, використання соціальних мереж для розпалювання конфліктів між різними групами населення.

Приклад: Посилення суперечок між прихильниками різних політичних поглядів або етнічних груп. Що призводить до зниження соціальної згуртованості, провокації протестів, конфліктів, зростання радикальних настроїв.[56]

4. Маніпуляція емоціями, поширення емоційного контенту (шокуючих відео, мемів, провокаційних постів), щоб викликати страх, ненависть, співчуття чи обурення. Формування стереотипів, підвищення емоційної напруги.

Приклад: Використання фотографій або відео з інших конфліктів, виданих за актуальні події.

5. Зміна порядку денного (Agenda-setting), використання алгоритмів платформ для просування певних тем або новин. Відволікання уваги від реальних проблем. Вплив на політичні рішення. Привертання уваги до "зовнішніх ворогів" замість внутрішніх проблем.

6. Легітимізація дій агресора, використання соціальних мереж для виправдання агресивних дій, наприклад, окупації територій. Зміна сприйняття

міжнародної спільноти щодо конфлікту. Мобілізація власного населення на підтримку війни. Приклад: Російська пропаганда про "захист населення Криму".[63]

7. Рекрутинг та радикалізація. Використання платформ для залучення нових учасників до військових або екстремістських організацій. Розширення мережі підтримки терористичних чи військових угруповань. Зростання кількості екстремістів. Приклад: Кампанії ІДІЛ у соцмережах для вербування молоді.

Найбільш відомі приклади впливу використання соціальних мереж у гібридній війні в реальному світі:

1. Російська агресія проти України: Масштабні кампанії у Facebook, X (Twitter) та YouTube для виправдання окупації Криму та агресії на Донбасі.

Поширення фейкових відео та фотографій, що викликають ненависть до української влади.

2. Втручання у вибори в США (2016, 2020). Створення сотень фейкових акаунтів, які поширювали провокаційні матеріали, поляризуючи суспільство.

3. Арабська весна (2011) Соціальні мережі використовувалися як платформа для мобілізації протестів, але також і для дезінформації та дискредитації учасників протестів.

Таким чином використання соціальних мереж у гібридній війні стало невід'ємною частиною сучасних конфліктів. Їхній вплив на громадську думку проявляється через поширення дезінформації, поляризацію, маніпуляції та мобілізацію. Для протидії цим загрозам важливо: Розвивати критичне мислення та медіаграмотність. Підвищувати стійкість державних інституцій до інформаційних атак. Впроваджувати міжнародні механізми регулювання діяльності соціальних платформ.

РОЗДІЛ 2. СУЧАСНИЙ СТАН ВИКОРИСТАННЯ СОЦІАЛЬНИХ МЕРЕЖ У ГІБРИДНІЙ ВІЙНІ ЩОДО УКРАЇНИ ТА УКРАЇНСЬКОГО СУСПІЛЬСТВА

2.1. Організаційні, правові, функціональні та інші аспекти використання соціальних мереж у гібридній війні.

Гібридна війна, що поєднує військові, економічні, політичні та інформаційні інструменти, активно використовує соціальні мережі як ключовий засіб впливу. В контексті російсько-української війни соціальні платформи стали полем битви за суспільну думку як в Україні, так і за її межами. Це включає активну пропаганду, дезінформацію, мобілізацію аудиторій та створення маніпулятивних інформаційних кампаній.

Соціальні мережі стали критично важливим інструментом у гібридній війні завдяки їх здатності швидко поширювати інформацію та впливати на широкий спектр аудиторій. У контексті гібридних конфліктів, включаючи російськоукраїнську війну, вони використовуються для інформаційних атак, маніпуляцій громадською думкою, мобілізації ресурсів та дезінформації.

Дивлячись на організаційні аспекти використання соціальних мереж у гібридній війні, можна констатувати, що Росія використовує централізовані структури, такі як "Агентство інтернет-досліджень" (відоме як "фабрика тролів"), що координує масові кампанії в соціальних мережах, тоді як в Україні задіяно численні волонтерські організації, які допомагають протидіяти інформаційним атакам та організовувати кампанії підтримки.

Станом на січень 2018 року, згідно звіту *Digital in 2018* міжнародного агентства *We are social*, в Україні 58 % населення користуються Інтернетом (22,59 млн осіб), 29 % – соціальними мережами (13 млн) [45]. Найбільшу популярність на сьогодні отримав *Facebook*. За даними внутрішньої статистики сервісу на січень 2018 року *Facebook* користується 11 млн українців. За останній рік кількість українських користувачів соцмережі зросла на 67 % [77], що пов'язано з міграцією користувачів з російських ВКонтакте и Одноклассники, доступ до яких був

обмежений українськими провайдерами згідно підписаного у травні 2017 р. Президентом України указу № 133/2017 [74]

Для подальшого дослідження важливим є те, як розподілено інформаційний простір в Україні. Також необхідно буде дослідити не тільки загальний стан розподілу інформаційного простору, але й те, як цей розподіл змінювався під час гарячої фази російсько-української війни.

Щодо медіаспоживання українців в умовах повномасштабної війни ґрунтовне дослідження на замовлення ГО ОПОРИ проводив Київський міжнародний інститут соціології з 3 до 26 травня 2022 року. Методом телефонних інтерв'ю з використанням комп'ютера (computer-assisted telephone interviews, CATI) на основі випадкової вибірки мобільних телефонних номерів (із випадковою генерацією телефонних номерів та подальшим статистичним зважуванням) опитано 2009 респондентів, що мешкають у всіх регіонах України (крім АР Крим). Опитування проводилося серед дорослих (у віці 18 років і старше) громадян України, які на момент опитування проживали на території України (у межах, які контролювала влада України до 24 лютого 2022 року). До вибірки не увійшли жителі територій, тимчасово не підконтрольних владі України до 24 лютого 2022 року (АР Крим, м. Севастополь, окремі райони Донецької та Луганської областей), а також громадяни, які виїхали за кордон після 24 лютого 2022 року. Польовий етап тривав з 19 до 24 травня 2022 року. [76] Дослідження опубліковано 1 червня 2022 року.

Всього опитано 2009 респондентів у віці 18 років і старше, які мешкають у всіх регіонах України (крім АР Крим).

Статистична похибка вибірки (з імовірністю 0,95 і з врахуванням дизайнефекту 1,1) не перевищує: 2,4% для показників, близьких до 50%, 2,1% — для показників, близьких до 25%, 1,5% — для показників, близьких до 10%.

Соціологічне дослідження показало, що серед українців найпопулярнішим джерелом інформації за останні два місяці є соцмережі, які випередили телебачення. Для отримання інформації соцмережі використовують 76,6% українців, а телебачення – 66,7%. 61,2% українців читають новини з інтернету без використання соцмереж. Найменше респонденти обирали радіо, його слухають близько 28,4% громадян України, а друковані ЗМІ читають лише 15,7% опитаних.

ТРАВЕНЬ 2022

Соціальні мережі

(Viber, Telegram, Youtube, Tik-Tok, Facebook, Twitter, Instagram)

76,6%

Телебачення

66,7%

Інтернет, не включаючи соціальні мережі

(Viber, Telegram, Youtube, Tik-Tok, Facebook, Twitter, Instagram тощо)

61,2%

Радіо

28,4%

Друковані ЗМІ

15,7%

Рис. 2.1. Розподіл джерел отримання інформації на початку гарячої фази війни (травень 2022 р.)

Соціологи виявили відмінності у виборі джерел інформації за віком. Понад 92% людей від 18 до 39 років читають новини у соцмережах, так само як і понад 64% споживачів від 40 до 69 років. Люди старші за 60 років надають перевагу телебаченню як джерелу інформації – 78% та радіо – 36%. Інтернет без соцмереж для отримання новин використовують понад 60% користувачів від 30 до 59 років, а друковані ЗМІ – понад 20% користувачів від 60 років. Водночас найбільше українці довіряють інформації з телевізора (60,5%), соцмережам довіряють 54% опитаних, а інтернет-джерелам без врахування соціальних мереж – 49%.

Найменше довіри респонденти мають до радіо (34%) та друкованих ЗМІ (23%), а 5% відповіли, що не довіряють жодному з джерел інформації.

Таблиця 2.1. Які соціальні мережі найбільше поширені серед українців для отримання інформації?

Telegram	65,7%,
YouTube	61,2%
Facebook	57,8
Viber	48%
Instagram	29,1%
TikTok	19,5%
Twitter	8,9%
WhatsApp, Signal тощо	2%

Зокрема, чоловіки частіше звертаються за новинами до YouTube (67,2%), Telegram (63%) та Facebook (54,8%), а найрідше – до TikTok (19,5%) і Twitter (11,8%), тоді як для жінок більш авторитетними є Telegram (68%), Facebook (62,1%) та YouTube (56%), найменше жінки звертаються як до джерела новин до TikTok (19,5%) та Twitter (6,5%). Через Viber та Instagram новини отримують 44,5% та 24,6% чоловіків та 51,1% і 32,9% жінок відповідно.[76]

Але, через два роки інформаційний простір України зазнав значних змін. Це можна довести спираючись на дослідження, що було проведено 3-12 березня 2024 року Фондом «Демократичні ініціативи» ім. Ілька Кучеріва спільно з Центром політичної соціології на замовлення медіамережі «Вікно Відновлення» (UA Recovery Window Media Network).

Як свідчать результати цього дослідження, значно скоротилася доля телебачення, радіо та друкованих ЗМІ.



Рис 2.2. Розподіл джерел отримання щоденної інформації громадянами України у 2024 р.

(Дані опитування, що проведеного 3-12 березня 2024 року Фондом «Демократичні ініціативи» ім. Ілька Кучеріва спільно з Центром політичної соціології на замовлення медіамережі «Вікно Відновлення» (UA Recovery Window Media Network))

Нові дослідження показали, що найпопулярнішим джерелом інформації про війну для українців вже є Telegram (53%). На другому та третьому місцях –

міжособистісні контакти (42%) та YouTube (40%). Телемарафон як джерело новин використовують 37% опитаних.

Найбільшою популярністю Telegram-канали користуються серед людей віком до 30 років (73%). Чим старша група респондентів, тим вищий у ній відсоток використання телемарафону "Єдині новини". У найстаршій віковій групі він є домінуючим (64%).

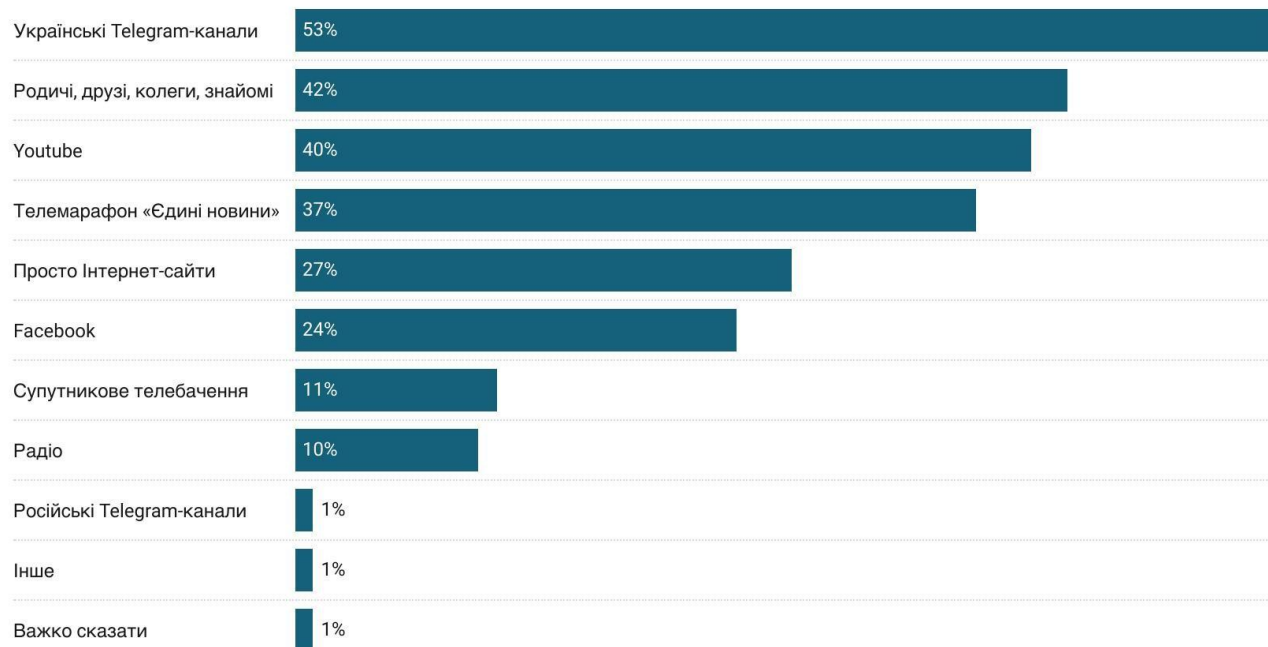


Рис 2.3. Розподіл джерел отримання інформації про події війни громадянами України у 2024 р.

Опитування показало, що у південних та східних регіонах Telegram-канали є однозначними лідерами (68% та 58%), у той час як у західних та центральних областях число користувачів становить менше половини жителів (48% та 49%). популярний на Півдні та Сході, але на Заході та в Центрі на нього також орієнтується менше половини населення.

У містах популярність Telegram-каналів трохи вища, ніж у селах. Друге та третє місця за популярністю серед міських жителів займають канали міжособистісного спілкування та YouTube (43%), а серед

сільських – канали міжособистісного спілкування та телемарафон "Єдині новини" (40-41%).

Дослідження також показало, що вибір джерел інформації залежить рівня освіти. Так, люди із середньою чи неповною середньою освітою переважно орієнтуються на телемарафон (49%) та спілкування з іншими людьми (48%), із середньою спеціальною освітою — Telegram-канали (53%) та канали міжособистісного спілкування (45%), а з високим рівнем освіти – Telegram-канали (61%) та YouTube (45%). Відсоток використання телемарафону зменшується із підвищенням рівня освіти.

Щодо довіри українців до інформації, що надходить від органів влади, більшою чи меншою мірою їм довіряють 39% опитаних, проте про повну довіру заявили лише 6%. У західних та центральних регіонах зафіксовано вищі показники довіри до повідомлень органів влади про війну (41–42%). На Півдні та Сході рівень довіри становить 31–32%. За даними опитування, рівень недовіри до інформації про війну з офіційних джерел вищий серед більш забезпечених громадян (39%) порівняно з 25–30% у групах із меншим рівнем достатку.

Щодо рівня освіти, особи із загальною або неповною середньою освітою частіше довіряють повідомленням органів влади (44%), тоді як відповідний показник серед осіб із середньою спеціальною або вищою освітою становить 36–38%. Також повідомляється, що даними від держорганів схильні довіряти жінки (41%), ніж чоловіки (35%).

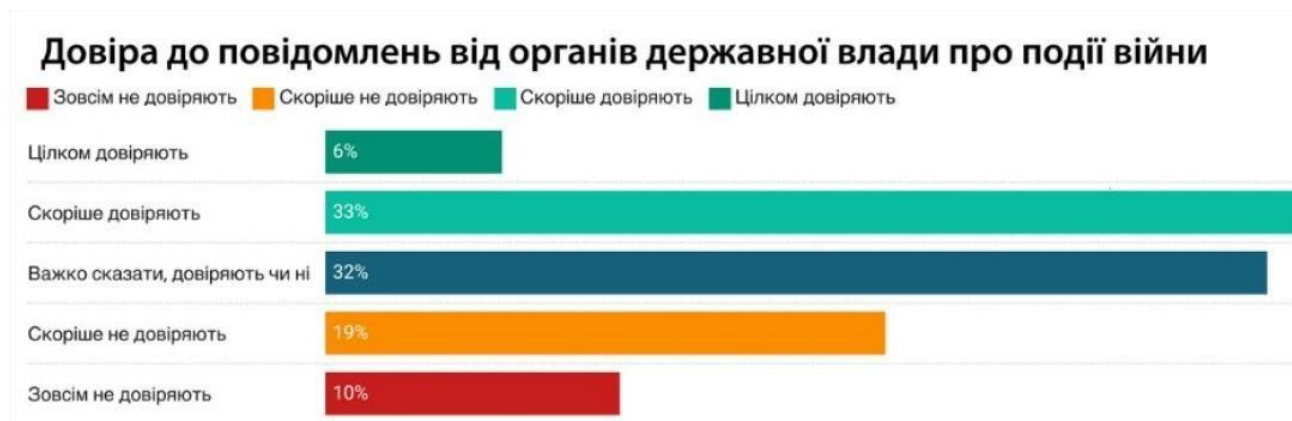


Рис2.4. Рівень довіри до інформації від органів влади в Україні

Нагадаємо, 18 квітня у Центрі протидії дезінформації повідомили про блокування ряду каналів у соціальній мережі TikTok, які використовувалися для поширення пропаганди Російської Федерації

Саме на ці соціальні мережі й націлені пропагандистські кампанії Росії, яка активно використовує соціальні мережі для поширення пропаганди, зокрема:

- Звинувачення України у "нацизмі" та "громадянській війні" на Донбасі.
- Зображення українських військових як агресорів.
- Використання фейкових новин для дискредитації українського уряду та міжнародної підтримки України.

Пропагандистські кампанії Росії не зупиняються лише на створенні пропагандистського контенту, але, для підсилення ефекту, активно використовує «армію» Ботів та тролів.

Бот-мережі (бот-ферми) це автоматизовані облікові записи, що поширюють дезінформацію, підтримуючи наративи, вигідні Росії.

Тролі – це акаунти, контрольовані реальними людьми, що беруть участь у дискусіях, щоб посіяти розкол, посилити напругу або дискредитувати українські позиції.

Пропагандистські кампанії Росії можна розділити на декілька напрямів.

Кампанії по дезінформації

- Цілеспрямоване поширення фальшивих новин, таких як вигадані "злочини" українських військових.
- Фейкові відео та фото для створення емоційного резонансу.
- Маніпуляції фактами для впливу на міжнародну громадську думку.

Поляризація суспільства

□ Поширення інформації, яка підсилює протиріччя між різними регіонами України, мовними або етнічними групами.

□ Зростання внутрішньої напруги через маніпулятивні пости про складну економічну чи військову ситуацію.

Росія намагається представити Україну як неспроможну державу.

Разом з тим соціальні мережі використовуються для поширення як позитивного, так і негативного іміджу України за кордоном: Українські активісти та уряд використовують соцмережі для інформування світу про російську агресію, зокрема через кампанії на платформах, таких як Twitter, Facebook, Instagram. Завдяки соцмережам українські користувачі отримують змогу об'єднуватися для волонтерської допомоги, пошуку правдивої інформації та підтримки армії. Соцмережі є потужним інструментом мобілізації громадян, наприклад, через кампанії збору коштів для армії або протестні акції.

Водночас не тільки пряма дезінформація, але й політичні суперечки, яка створюються в самому українському середовищі можуть викликати недовіру до влади, Збройних Сил України або міжнародних партнерів.

Україна використовує відео, щоб висвітлювати героїзм військових, масштаби руйнувань від російської агресії, залучаючи емоційну підтримку міжнародної спільноти, тоді як Росія поширює фейкові відео, часто створені за допомогою deepfake технологій, щоб дискредитувати українське керівництво.

Telegram став однією з ключових платформ у російсько-українській війні.

Українські волонтерські канали інформують громадян про евакуацію, гуманітарну допомогу тощо.

Проросійські канали поширюють паніку, дезінформацію або заклики до дестабілізації.

Українське суспільство активно використовує гумор як засіб протистояння. Мем-культура не лише піднімає бойовий дух, але й викликає симпатії у міжнародних аудиторій.

Алгоритми соціальних мереж (Facebook, TikTok, YouTube) сприяють поширенню емоційно зарядженого контенту, що робить їх ідеальним інструментом для маніпуляцій. [27]

Російські маніпулятори створюють контент, який максимально привертає увагу, тоді як українські користувачі намагаються протидіяти, поширюючи реальні історії та факти.

4. Протидія маніпуляціям у соціальних мережах це перш за все Фактчекінг та боротьба з дезінформацією. Українські та міжнародні організації створюють платформи для перевірки фактів, такі як StopFake. Соціальні мережі (Facebook, Twitter) починають маркувати підозрілий контент або видаляти дезінформацію.

Українські IT-фахівці та кібервійська працюють над захистом інформаційного простору від російських атак. Використання штучного інтелекту для виявлення та блокування фейкових акаунтів.

В Україні впроваджуються програми для навчання громадян критично оцінювати інформацію. Активісти та освітяни працюють над підвищенням обізнаності про ризики інформаційних маніпуляцій.

Таким чином соціальні мережі є одним із головних інструментів у сучасній гібридній війні. Їх вплив на громадську думку щодо України є величезним, як у позитивному, так і негативному контексті. Для ефективного захисту свого інформаційного простору Україна повинна продовжувати співпрацю з міжнародними партнерами, розвивати технології для протидії дезінформації, а також підвищувати рівень медіаграмотності серед своїх громадян.

Згідно з чинним законодавством, медіа несуть відповідальність не лише за поширення російської пропаганди, але й за багато інших порушень. Завдяки цьому, а також внутрішній саморегуляції, жодне ЗМІ не може безкарно публікувати

«джинсу», наклепи, немарковану рекламу і тому подібне. Об'єктивне і неупереджене висвітлення подій, баланс думок, відокремлення суджень від фактів, перевірка інформації – все це не порожні гасла, а важливі принципи, відмова від яких миттєво перетворює медіа на помийницю. Правила працюють насамперед на користь аудиторії, закладаючи обов'язкові для медій і журналістів стандарти.

Розвиток інтернету і поява нових технологічних можливостей призвели до того, що мільйони людей отримали можливість створювати власний контент. Але поряд зі «старими медіа» з'явилися «нові»: соціальні мережі, інтернет-радіо, Youtube-канали, телеграм-канали тощо. Вони стали джерелом інформації для величезних аудиторій: наприклад, сьогодні більшість українців дізнається новини з Youtube, Telegram-каналів, Facebook. «Нові медіа» фактично перебрали функцію «старих», проте не взяли на себе зобов'язань щодо дотримання відповідних правил роботи. [21]

Через це у світі почалися дискусії про необхідність регуляції «нових медій». Особливо гостро це питання постало після виборів у США у 2016-му році, під час яких Росія активно впливала на суспільну думку американців через соціальні платформи. Згодом закони, що регулюють соціальні медіа, були ухвалені у Німеччині, Австралії, Канаді та низці інших країн. З того часу будівництво правової екосистеми, покликаної регулювати нові медіа, не зупиняється. Так, влітку 2022 року у Євросоюзі було прийнято Закон про цифрові послуги (Digital Services Act, DSA) та Закон про цифрові ринки (Digital Markets Act, DMA), які регламентують діяльність технологічних компаній на європейському ринку, а також закривають деякі лазівки для поширення фейків.

На жаль, регуляція спрацьовує не завжди. Коли у 2017 році в Україні заблокували російські соцмережі «ВКонтакте» та «Однокласники», а також низку інших інтернет-ресурсів, частина суспільства сприйняла це негативно – як обмеження свободи. Проте цей крок був вимушений, адже дані ресурси були не лише майданчиком для пропаганди, але й джерелом персональних даних для

російських спецслужб про українців. Сьогодні доведено, що й надзвичайно популярний месенджер Telegram несе низку цілком реальних загроз. Він пов'язаний з РФ фінансово і технологічно, а також дуже подобається російським спецслужбам, які можуть, наприклад, отримувати доступ навіть до видаленого листування у месенджері. Звідси – й обговорення ідеї блокування Telegram, які, на жаль, часто подаються як «наступ на свободу слова» чи навіть як спроба наслідувати приклад тоталітарної Росії. [4]

Проте називати блокування певних інтернет-майданчиків ознакою «диктатури» – відверта маніпуляція. Наприклад, Сполучені Штати годі вважати диктатурою. Проте на початку березня 2024 року Палата представників підтримала законопроект, який відкриє шлях до блокування TikTok. Передбачається, що компанія ByteDance, якій належить сервіс, буде зобов'язана продати його не китайському власнику протягом шести місяців, інакше TikTok буде заблокований у США. Таке рішення зaledве можна назвати популярним, адже сервісом користується близько 150 млн американців, в середньому проводячи у TikTok майже годину на день. Але законотворці керуються міркуваннями безпеки: додаток TikTok може використовуватись для збору даних і маніпулювання суспільною думкою в інтересах китайського уряду.

Отож, регуляція онлайн-майданчиків вже давно є нормальною світовою практикою і продиктована вона об'єктивними потребами безпеки та інтересами аудиторії. На жаль, «абсолютна свобода інформації», в яку вірили інтернетентузіасти минулого століття, виявилась ілюзією. Показовим прикладом є те, що сталося з соціальною мережею X (Twitter), відколи Ілон Маск почав змінювати політику платформи відповідно до принципу «безумовної свободи слова». Згідно з дослідженням Єврокомісії, руйнування стандартів безпеки призвело до того, що X стала набагато комфортнішою для російської пропаганди. Аналітичний центр DFRLab також зафіксував активне зростання підписників

китайських та іранських пропагандистських ресурсів. Навряд чи це має хоч якесь відношення до справжньої свободи слова.

Інформаційна агресія – не метафора, а об’єктивна і загрозлива дійсність. Тому регуляція інтернет-простору, а часом і заходи обмежувального характеру, є вимушеною необхідністю. Так само важливим є унормування діяльності ресурсів, які по факту виконують роль медій. Швидкі та прості рішення тут неможливі, проте іншого шляху немає – лише так можна захистити інтереси споживачів інформації й убезпечити їх від непрофесіоналізму та недобросовісності новітніх акторів медіапростору. За роки свого існування месенджер Telegram став важливою частиною життя багатьох українців. Під час повномасштабної війни його популярність ще більше зросла завдяки зручності, невибагливості до якості інтернет-зв’язку та оперативності популярних каналів.

Telegram є беззаперечним лідером у своєму сегменті: згідно з дослідженням Kantar, у другій половині 2023 року додатком користуються 88% українців. На другому місці Viber, який у 2022-му випереджав конкурента майже на 10%. [96]

В умовах війни Telegram для українців став головним джерелом новин в інтернеті, помітно випередивши інформаційні сайти та інші соцмережі. Такий стан справ було зафіксовано ще минулого року. У поточному – ситуація залишилася незмінною.

На популярність месенджера вимушені зважати не лише споживачі, а й постачальники новин: свої канали відкривають посадовці, державні органи та більшість українських медіа.

Втім, Telegram – це не лише зручний месенджер. Увагу суспільства і держави на небезпеку, які створює користування цим додатком, намагаються привернути експерти з інформаційної та кібербезпеки.

Центр стратегічних комунікацій та інформаційної безпеки зібрав пояснення фахівців, у чому саме небезпека месенджера Telegram.

Зауваження експертів можна розділити на чотири групи.

1. Зв'язок з путінською Росією

Засновником Telegram є росіянин Павло Дуров, який у 2006 створив соцмережу «Вконтакте» (VK). У 2013-2014 роках він продав її – нібито під тиском російської влади, та переключився на новий проєкт – Telegram. Разом з командою розробників, яка перед цим працювала з Дуровим над VK.

До 2021 року власником контрольного пакета акцій VK були структури путінського олігарха Алішера Усманова. Сьогодні VK опосередковано належить «Газпрому».

Хоча Дуров неодноразово робив заяви про свою опозиційність, Telegram продовжує мати не лише російського засновника та розробників, а й російських інвесторів. У 2017 і 2021 роках Дурову вдалося залучити 2,7 млрд доларів інвестицій. Серед інвесторів він називав Сергія Солоніна (засновник платіжної системи Qiwi), Романа Абрамовича та Давида Якобашвілі (співзасновник «ВіммБілл-Данн»). У 2022 році Україна наклала на Якобашвілі санкції за підтримку путінського режиму.

У березні 2021 року російські державний VTB Capital та приватні Aton і «Альфа-Капітал» викупили облігації Telegram на загальну суму 1 млрд доларів. Завдяки цьому Дуров зміг погасити борги компанії, які становили 684 млн доларів.

З 2018 року російська влада вдавала вигляд, що намагається заблокувати Telegram у РФ. Та й сам Дуров заявляв під час блокування, як і під час продажу «Вконтакте», про тиск з боку російських спецслужб та небажання передавати їм дані користувачів.

Але у 2020-му епопея з блокуванням завершилася, а головний ворог месенджера – Роскомнадзор – навіть завів у месенджері власний канал. Тому зняття питань російської влади до Telegram може свідчити про досягнення певних домовленостей між розробником і спецслужбами. Хоча при цьому офіційна позиція Telegram – «жодних угод, які б сприяли розблокуванню соцмережі в Росії, не укладалося».

Згідно з російським законодавством РФ, під час збору персональних даних оператор зобов'язаний забезпечити їх запис, систематизацію, накопичення, зберігання, уточнення, вилучення, використовуючи бази даних, що перебувають на території РФ. Станом на квітень 2022 сайт telegram.org хостився на російському ІР.[12]

Сервери, через які Telegram передає повідомлення, належать російській компанії GlobalNet із головним офісом у Москві. Частина цих серверів фізично розташовують на території РФ. Інформація про ці сервери опублікована на офіційному сайті компанії.

Під час встановлення застосунків запитує дозволи на доступ до камери, мікрофону, документів, зображень, контактів. Політика Telegram передбачає зберігання всіх цих даних на серверах. Тому нема жодних підстав вірити запевненням Telegram у забезпеченні безпеки ваших даних. А отже на ці сервери, які перебувають на території РФ, можуть потрапляти не лише файли, переслані під час листування, а взагалі весь вміст вашого смартфона.

. Існує чимало доказів того, що російські спецслужби мають доступ до приватного листування користувачів Telegram і використовують отриману інформацію проти них.

Telegram позиціонується як безпечний месенджер, який підтримує шифрування даних. Втім «не все так однозначно». Функцію наскрізного шифрування та обмін повідомленнями напряму, без залучення проміжних серверів, передбачено лише для секретних чатів. Але опція за замовчуванням є вимкненою, а доступ до неї в актуальних версіях застосунку є ускладненим. До того ж зовнішнього аудиту цієї системи, на відміну від деяких конкурентів, Telegram не проводив. Отже, жодних гарантій, що заявлена опція дійсно працює, немає. Про те, що секретні чати Telegram працюють не зовсім коректно, свідчить наявність багу: якщо розлогінітися або реінстальювати застосунок, ви втратите доступ до секретних

чатів. Але не ваші співрозмовники, які можуть продовжувати писати туди, не знаючи, що повідомлення вже недоступні для адресата.

Telegram запрошує доступ до геолокації пристрою для активації опції «Люди поруч». З одного боку, зручно. З іншого – застосунок має можливість не лише збирати інформацію про ваші маршрути і навіть офлайн-зустрічі з іншими користувачами Telegram, а й відстежувати переміщення в режимі реального часу.

Використання соціальних мереж у гібридній війні часто порушує норми міжнародного права, зокрема стосовно кібератак, пропаганди війни та втручання у внутрішні справи інших держав.

Наразі відсутні універсальні правові механізми для регулювання цього виду агресії.

Україна. Прийнято закони, спрямовані на боротьбу з пропагандою, кіберзлочинами та дезінформацією, включаючи блокування платформ, що підтримують агресора. 3 березня Верховна Рада ухвалила законопроект №5101 щодо заборони виготовлення та поширення інформаційної продукції, спрямованої на пропагування дій держави-агресора. Цей документ був зареєстрований у парламенті 18 лютого 2021 року. Його ініціаторами виступила група народних депутатів. 15.03.2022 р. Президент Володимир Зеленський підписав закон (законопроект №5101) про заборону виготовлення та розповсюдження інформаційної продукції, спрямованої на пропагування дій Росії. [74]

Так, відповідно до закону, друкованим ЗМІ, телебаченню та радіо заборонено виправдовувати, визнавати правомірною та заперечувати збройну агресію РФ проти України, яка триває з 2014 року. Зокрема, заборонено представляти російську агресію проти України як "внутрішній конфлікт", "громадянський конфлікт", "громадянська війна", заперечувати тимчасову окупацію частини української території.

Також заборонено прославляти заяви та дії осіб, які здійснюють збройну агресію Росії проти України. Йдеться про:

- осіб, які здійснювали збройну агресію Росії проти України,
- представників збройних формувань країни-агресора,
- нерегулярних незаконних збройних формувань,
- озброєних банд та груп найманців, створених, підпорядкованих, керованих та фінансованих РФ,
- представників окупаційних адміністрацій,
- представників підконтрольних Росії самопроголошених органів, називаючи їх "повстанцями", "ополченцями", "ввічливими військовими людьми".

Крім того, закон передбачає санкції, а саме припинення в Україні діяльності партій, релігійних та громадських організацій, діяльність яких спрямована на ліквідацію незалежності, зміну конституційного ладу, порушення її суверенітету чи територіальної цілісності України, пропаганду війни чи виправдання дій РФ як країни-агресора.

Державне бюро розслідувань зібрало необхідні докази для оголошення російського пропагандиста Володимира Соловйова у міжнародний розшук та передасть його закордонним колегам.

Офіс генпрокурора повідомив про підозру російському співаку Миколі Баскову за пропаганду війни, яку Росія розпочала на території України. Підозру у посяганні на територіальну цілісність України оголошено також російській ведучій Тіні Канделаки. У вчиненні низки злочинів проти України звинувачується також російська пропагандистка Маргарита Симоньян, яку ОГПУ хоче оголосити у міжнародний розшук.

В тому ж напрямку діє й Постанова Верховної Ради України від 01.12.2022 № 2798-IX Про прийняття за основу проекту Закону України про внесення змін до деяких законів

України щодо заборони використання джерел інформації держави-агресора або держави-окупанта в освітніх програмах, в науковій та науково-технічній діяльності [59]

З токи зору інституційного забезпечення боротьби з російською пропагандою важливцу роль має зіграти Наказ від 25.07.2023 № 399, Про затвердження Положення про Експертну комісію Українського інституту національної пам'яті з питань реалізації норм Закону України «Про засудження та заборону пропаганди російської імперської політики в Україні і деколонізацію топонімії» Чинний, від 15.09.2023,[58]

Законодавче забезпечення охорони українського медіапростору є тим більш актуальним у зв'язку з тим, що російське законодавство активно використовує цензуру та інші інструменти для придушення альтернативних думок і посилення інформаційної монополії.

Великою, ще не вирішеною проблемою є боротьба за інформаційний вплив на міжнародному інформаційному просторі. Наприклад, за даними ЗМІ, китайські державні медіа висвітлюють війну в Україні як вимушені кроки Путіна, який захищає оточену ворожими західними країнами Росію. При цьому наративу про націоналізм у китайських медіа не чути, також журналісти КНР осуджують створення гуманітарних проблем.

Міжнародні соціальні мережі (Meta, Google, Twitter) мають політики боротьби з фейковими новинами, але ефективність їх впровадження залишається обмеженою через складність і масштабність проблеми. Масове поширення неправдивої інформації з метою дискредитації урядів, зниження довіри до інститутів влади та формування негативного іміджу. Використання "deepfake" технологій для створення фейкових відео та зображень. Соціальні мережі використовуються для координації протестів, збору гуманітарної допомоги, організації волонтерських ініціатив.

2.2. Оцінка стану використання соціальних мереж у гібридній війні

Соціальні мережі перетворилися на ключовий інструмент у гібридних війнах завдяки їхній здатності швидко охоплювати мільйони користувачів, впливати на їхню думку, формувати наративи та координувати дії. В умовах сучасних конфліктів, таких як російсько-українська війна, оцінка цього феномену є необхідною для розуміння його наслідків та пошуку ефективних шляхів протидії.

Соціальні мережі стали потужним інструментом формування вигідних наративів для зміцнення підтримки серед власного населення та міжнародної аудиторії. Дискредитація супротивника через дезінформацію, пропаганду та маніпуляцію фактами. Створення конфліктів у суспільстві через поляризацію думок та поширення фейкових новин. Використання емоційного контенту для підриву довіри до влади чи ключових державних інституцій. Координація кібератак, протестних рухів або диверсійних груп. Залучення симпатиків для підтримки через фінансову допомогу, поширення меседжів чи участь у цифрових кампаніях.

Поширення вигідних меседжів через створення бот-мереж, груп у Telegram, вірусних відео в TikTok та YouTube. Використання deepfake для створення фальшивого візуального контенту. Використання технологій штучного інтелекту для автоматичного створення фейкових новин. Поширення спотворених фактів з метою підриву довіри до офіційної інформації. Цілеспрямовані атаки на ключові групи, таргетинг аудиторій за інтересами, мовою, регіоном проживання.

Використання рекламних інструментів соціальних мереж для досягнення максимальної ефективності. Упакування пропаганди у формат гумору для легшого сприйняття широкою аудиторією. Створення мемів, що швидко поширюються серед молоді.

Щоб оцінити масштаб дезінформаційного впливу, достатньо звернутися до таблиці 2.1. в який наведено далеко неповний перелік фейків, які за останні 10 років поширювалися російською пропагандою.

Навіть поверхневий аналіз цієї таблиці призводить до висновку, що пропаганда в Росії поставлена на індустріальну основу. Не рідше чим раз на місяць, і так вже протягом десяти років, в інформаційний простір вкидується новий фейк, на супровід якого працюють всі російські ЗМІ як в середині самої Росії так назовні.

Разом з тим необхідно вказати й на позитивні аспекти використання соціальних мереж у захисті від гібридної війни

Це протидія дезінформації. Українські медіа та громадські організації, такі як StopFake, активно спростовують фейкові новини. Розширення програм медіаграмотності серед населення. Інформування міжнародної спільноти. Використання платформ для поширення правдивої інформації про війну. Кампанії в соцмережах для залучення гуманітарної допомоги та міжнародної підтримки.

Таблиця 2.1. Основні фейки про Україну, що використовувала Росія у період 2014-2024 р.р.

«КИШЕНЬКОВИЙ ІДІЛ»	– Жителі захоплених територій не зможуть скористатися безвізом
«В Україні діють табори ІДІЛ».	Україна ніколи не стане повноправним членом ЄС
«Джихадисти ІДІЛ отаборились в Україні»	Загроза українських мігрантів..
«Україна і 500 джихадистів».	Українська промисловість втрачає найбільший ринок збуту
Кремль: «ІДІЛ постачає нафту до України»	КРИМСЬКА ІНФОРМАЦІЙНА ВІЙНА
Переслідування кримських татар	146% підтримки приєднання Криму до Росії
та «Хізб ут-Тахрір», як поплічників ІДІЛ	Одноставність голосування за приєднання Криму
Пов'язування добровольчих батальйонів та української армії з ІДІЛ.	Загадковий з'їзд українських діаспор
Фейки про батальйон Дудаєва..	Крим ніколи не повернеться до складу України
ІДІЛ окупанта Басуріна.	Крим ніколи не був українським?..
ІДІЛ та «Правий сектор»	Україна змирилася з втратою Криму.
Фейки про добровольців батальйону «Азов»	Міжнародна спільнота незацікавлена у поверненні Криму Україні
Українська армія на боці ІДІЛ?	«Офіційні делегати» з інших країн, які відвідали Крим

«Україна постачає зброю ІДІЛ»	Фіни та кримський безвіз.
Кремль: «Українці постачають хімічну зброю бойовикам в Сирію»..	– Крим і «українські туристи».
Російський посол: «Україна постачає до ІДІЛ тони зброї»	У ПОШУКАХ УКРАЇНСЬКОЇ ЗБРОЇ
Україна постачає терористам зенітноракетний комплекс «Печора»	Україна постачає зброю супротивникам ЄС та США..
Україна продає ІДІЛ китайські ПЗРК.	РФ – перший імпортер української зброї.
Україна – ціль терористичних атак з боку ІДІЛ..	Україна та північнокорейські двигуни.
Джихад проти «Ліги чемпіонів»	Українська зброя в Сирії..
ЗЛОЧИНИ ЗСУ ТА МІНСЬКІ	Нелегальна торгівля з Африкою
	Несправна українська зброя.

ДОМОВЛЕНOSTІ	
ЗСУ, Нацгвардія та добровольці «знищують» населення Донбасу	Таїланд відмовляється від українського танку «Оплот»
Обстріли «мирних жителів Донбасу» українськими «карателями»	Індонезії та Іраку не потрібні українські БТР-4.
ЗСУ обстрілює «ополченців» снарядами з пропагандою	– Хорватія, Україна та несправні МиГ-21
«Карателі» з ЗСУ: розіпнений хлопчик та інші фантазії російської пропаганди.	США використовують Україну та її зброю для протидії Росії.
Українські добровольці – мародери, гвалтівники та вбивці.	Американська зброя на передовій
Геноцид населення Донбасу..	Кремль проти «Джавелінів»
Фейкові фотографії із зони АТО	Росія не є спонсором тероризму?
Україна зриває виконання Мінських домовленостей	Війна на Донбасі – не «громадянський конфлікт»
Західні лідери та спостерігачі звинувачують Україну у порушенні Мінських домовленостей.	Бойовики знайшли зброю у шахтах
Росія: «ОБСЄ ігнорує обстріли української сторони».	Україна порушує Мінські домовленості.
ЗСУ готується до штурму Донецька.	Україна – спонсор тероризму?.
РЕЙС МН-: ВІД КАРЛОСА – ДО РОСІЙСЬКОГО «БУКА»	#Кримнаш або на території півострова немає переслідувань.
Диспетчер Карлос та його військові винищувачі.	Росія не дискримінує кримських татар?.
Диспетчер «Карлос» звинувачує Україну	Українські інвестори легалізували анексію Криму

Українські сили хотіли збити літак Путіна	«Нафтогаз» програв «Газпрому»
Українці знищили літак заповнений трупами	Європейцям не потрібна українська ГТС
Малайзійський літак знищило ЦРУ..	Фейкова перемога «Газпрому»
Малайзійський Боїнг збив винищувач Су-25	УКРАЇНА – «FAILED STATE»..
Кейс Волошина	Україна – несаможиттєва держава, яка розпадається на частини
Кремлівський фіктивний свідок	Україна перебуває під зовнішнім управлінням Заходу
Український “Бук”..	Україна на межі розпаду, а західні союзники зрадили.
Бук був українським?.	«Україна не може забезпечити своє населення базовими благами»
Фейки «Алмаз-Антей».	Українська економіка не виживе без торговельних зв'язків із Росією
Україна – співучасник вбивства	Українська економіка стагне і розвалюється.
– Україна не закрила повітряний простір.	Населення голодує, замерзає, вмирає та тікає
	з України
НЕВИДИМІ ПІДРОЗДІЛИ ЗАХІДНИХ КРАЇН В УКРАЇНІ	«Другий Чорнобиль» в Україні через американське ядерне паливо
Україна – де-факто передній край військ НАТО.	«Україна – країна майданів та розгулу радикалів»
Війська НАТО беруть участь у конфлікті на Донбасі	Україна – країна нестабільності та революцій
Втрати військ західних країн на Донбасі.	Після «Євромайдану» Україна стала полігоном для націоналізму та радикальних рухів.
Україна – полігон для випробувань зброї НАТО	ШИЗОФРЕНІЯ ОКУПАНТА: МІЖ ЗОРЯНОМ ТА ШКІРЯКОМ
Приватні військові компанії в АТО	«Правосек» з Німеччини, який виступає за федералізацію.
Американські найманці з Blackwater та Greystone	Арсеній Яценюк – чеченський бойовик..
Невидима війна польських найманців на Донбасі	Древні укри викопали Чорне море
БІЙ ЗА ЄС	Геноцид проросійських снігурів
Україні не потрібна Угода про асоціацію.	Любов українців до нацистської символіки..
ЄС змусить Україну приймати мігрантів	Двоє рабів та клаптик землі.

ЄС витіснятиме українську продукцію та знищуватиме виробництво	Оплата сіллю за проїзд в Мелітополі
Європейці не нададуть/скасують безвізовий режим..	Зорян і Шкіряк – замовники вбивства «Гіві».
Нідерланди проти асоціації..	Вимоги до Монголії через зруйнування Києва ханом Батиєм
Європейці проти безвізової лібералізації	Дегуманізація ВСУ
Безвіз: хвороби та сексуальне рабство	

Соціальні мережі стали платформою для збору коштів, організації волонтерської допомоги та координації дій громадян. Цифровий активізм. Громадяни та активісти використовують соцмережі для прямої комунікації з владою, допомоги армії та боротьби з ворогом в інформаційному просторі.

Відсутність критичного мислення серед частини населення робить їх вразливими до впливу пропаганди, викликає складнощі у відрізненні правдивої інформації від фейків. Алгоритми платформ, таких як Facebook або TikTok, часто сприяють поширенню емоційно зарядженого контенту, включаючи дезінформацію. Вірусність маніпулятивного контенту значно перевищує поширення правдивих новин.

Соціальні мережі намагаються боротися з фейками (маркування контенту, видалення акаунтів), але масштаб проблеми перевищує їхні можливості. Не сприяють цьому й географічні обмеження – певні країни блокують доступ до частини платформ, створюючи "інформаційні бульбашки".

Завдяки соціальним мережам Україна отримала безпрецедентну підтримку від міжнародної спільноти. Соціальні мережі об'єднують громадян для протидії агресору, сприяють мобілізації ресурсів.

Російські інформаційні кампанії формують спотворене уявлення про причини та наслідки війни.

Таким чином необхідно розробити програми щодо Розвитку національних інформаційних стратегій, до яких має бути включені напрямки Удосконалення механізмів виявлення та нейтралізації дезінформації, посилення співпраці з

платформами соцмереж для блокування маніпулятивного контенту, використання штучного інтелекту для моніторингу інформаційного простору та залучення кібербезпекових команд до захисту від ворожих атак.

Створення глобальних коаліцій для боротьби з дезінформацією. Удосконалення правових норм щодо відповідальності за інформаційні атаки.

Соціальні мережі стали важливим інструментом у гібридній війні, але їхня роль залежить від того, як вони використовуються. Для ефективної протидії загрозам Україна повинна продовжувати розвивати власну інформаційну стратегію, підвищувати технологічні можливості та посилювати міжнародну співпрацю. Водночас акцент на медіаграмотність суспільства є критично важливим для зміцнення інформаційної стійкості.

2.3. Суперечності у розвитку використання соціальних мереж у

гібридній війні: аналіз і шляхи вирішення

Соціальні мережі у гібридній війні є інструментом і викликом водночас. Для ефективного використання їх потенціалу у захисті державних інтересів і мінімізації ризиків необхідно впроваджувати як локальні, так і міжнародні рішення. Врахування вітчизняного досвіду та адаптація найкращих практик зарубіжних країн дозволить підвищити інформаційну безпеку та посилити стійкість суспільства до маніпуляцій.

Використання соціальних мереж у гібридній війні супроводжується значними суперечностями, які виникають через їхній двоїстий характер: ці платформи є потужними засобами для інформаційного впливу, але одночасно створюють серйозні виклики для безпеки, довіри суспільства і правового регулювання. Аналіз досвіду України та зарубіжних країн дозволяє виявити ключові протиріччя та шляхи їх розв'язання.

Використання соціальних мереж для боротьби з пропагандою викликає питання обмеження свободи слова. Одні країни вводять жорсткі обмеження на контент, тоді як інші бояться зловживань владою. Останнім часом влада в Україні розмірковує над тим, щоб заборонити месенджер або, ймовірно, зробити його більш підконтрольним. Для цього, зокрема, у Києві зажадали від адміністрації платформи відкрити офіс в Україні, а також інформувати про розташування серверів компанії.

Зокрема, зазначається, що через Telegram Росія активно розповсюджує свої ІПСО та пропагандистські інформаційні кампанії. І це правда. Але, з іншого боку, саме Телеграм є основним альтернативним джерелом інформації для українців. І деякі вбачають у всьому цьому спробу наступу на свободу слова. Влада має вжити заходів для регулювання Telegram. Зокрема, пропонують такі кроки:

- Зробіть видимими власників анонімних каналів. Це, змусить їх нести відповідальність за контент, що поширюється, і підвищить довіру до Telegramканалів.

- Створити реєстр суб'єктів медіадіяльності у Telegram. Це дозволить чітко визначити, які канали є медіа, а які ні, та застосовувати до них відповідні норми.

- Деанонімізувати власників каналів, щоб можна було встановити, хто замовляє шкідливий контент.

- Відкрити в Україні представництво Telegram. Це дозволить українській владі ефективніше співпрацювати з месенджером.

Інший пласт суперечностей пов'язано із існуючим законодавчим розривом. Це й відсутність єдиних міжнародних стандартів регулювання соціальних мереж, що дозволяє платформам і агресорам використовувати прогалини у законодавстві різних країн. Алгоритми соціальних мереж сприяють поширенню маніпулятивного контенту через орієнтацію на емоційність і вірусність. Соціальні мережі гарантують анонімність користувачам, що полегшує створення бот-мереж і поширення

dezінформації. Платформи часто затримують реалізацію заходів безпеки через загрозу втрати аудиторії та прибутків.

Для вирішення цих суперечностей слід планувати наступні кроки:

1. Розробка міжнародних стандартів. Встановлення глобальних норм регулювання соцмереж під егідою ООН чи інших міжнародних організацій для боротьби з пропагандою.

2. Розширення співпраці між державами. Законодавче забезпечення спільних дій в рамках НАТО чи ЄС для протидії гібридним загрозам, включаючи інформаційні атаки в соцмережах.

3. Підвищення прозорості шляхом зобов'язання платформ розкривати інформацію про джерела фінансування політичної реклами та механізми роботи алгоритмів.

4. Розвиток технологій і освіти, інвестування в розробку штучного інтелекту для автоматичного виявлення фейків, масштабні освітні програми з медіаграмотності для суспільства.

5. Законодавчі ініціативи. Посилення відповідальності за поширення дезінформації як для фізичних осіб, так і для організацій.

6. Роль громадянського суспільства, шляхом активного залучення незалежних фактчекінгових організацій та неурядових ініціатив.

На цьому шляху вже існують приклади успішних рішень:

□ ЄС: Впровадження Digital Services Act, – Регламент (ЄС) 2022/2065 Європейського Парламенту та Ради від 19 жовтня 2022 року про єдиний ринок цифрових послуг і внесення змін до Директиви 2000/31/ЄС (Закон про цифрові послуги), який зобов'язує платформи зменшувати поширення шкідливого контенту.

□ Україна: Блокування російських платформ, таких як ВКонтакте та Однокласники, що використовувалися для поширення дезінформації та збору даних.

Однак ще на використані такі можливості у поглиблення шляхів вирішення як:

□ Розробка локалізованих механізмів реагування, що включає розширення національних платформ для виявлення дезінформації (наприклад, ініціативи України, такі як StopFake, ЦПД) та посилення співпраці між урядом і громадянським суспільством для швидкої перевірки та реагування на інформаційні атаки.

□ Підтримка демократичного контролю над соцмережами, запровадження громадських рад, які аналізують дії соцмереж у регіонах, найбільш уразливих до інформаційних загроз та регулярний аудит діяльності платформ незалежними міжнародними організаціями.

□ Вдосконалення санкційних механізмів за рахунок розширення міжнародних санкцій проти платформ, що не реагують на випадки використання їхніх сервісів для розпалювання конфліктів. Замороження активів або обмеження комерційної діяльності технологічних компаній, які співпрацюють із державами-агресорами.

□ Розробка механізмів протидії новим формам маніпуляції. Розробка технологій для боротьби з deepfake та іншими інструментами підробки відео та аудіоконтенту. Створення національних баз даних для аналізу походження маніпулятивних матеріалів.

□ Інтеграція штучного інтелекту, шляхом використання нейронних мереж для моніторингу трендів дезінформації в реальному часі. Автоматизація процесу маркування неправдивих новин у стрічках соцмереж.

Нові виклики та інструменти пов'язані зі зростаючою роллю месенджерів.

□ Такі платформи, такі як Telegram і WhatsApp, стають осередком поширення фейкових новин через відсутність прозорих механізмів модерації.

□ Перспективними вважаються використання технологій блокчейн для перевірки контенту. Блокчейн може забезпечити прозорість у процесах верифікації новин і виявлення джерел маніпуляцій.

□ Краудсорсингові підходи сприяють залученню широкого кола користувачів до перевірки інформації через ігрові механізми та спеціалізовані додатки.

Вже існує низка практичних прикладів подолання суперечності у розвитку використання соціальних мереж у гібридній війні

Так Україна запровадила блокування російських соцмереж, таких як "ВКонтакте" і "Однокласники", стало ефективним кроком у скороченні доступу до каналів пропаганди, а ініціатива StopFake забезпечує оперативний розбір маніпулятивного контенту.

Європейський Союз проводить багаторічну системну роботу по протидії поширенню дезінформації. Черговим кроком на цьому шляху стало запровадження Code of Practice on Disinformation, який закликає технологічні компанії добровільно боротися з дезінформацією. [104]

Кодекс щодо протидії дезінформації 2022 року спрямований на встановлення ширшого спектру зобов'язань і заходів для протидії дезінформації в Інтернеті.

Підписанти зобов'язалися вжити заходів у кількох сферах, таких як; демонетизація поширення дезінформації; забезпечення прозорості політичної реклами; розширення можливостей користувачів; посилення співпраці з фактчекерами; і надання дослідникам кращого доступу до даних.

Посилений Кодекс практики містить 44 зобов'язання та 128 конкретних заходів у наступних сферах.

Демонетизація: скорочення фінансових стимулів для розповсюджувачів дезінформації. Посилений Кодекс спрямований на те, щоб розповсюджувачі дезінформації не отримували прибутків від рекламних доходів.

Прозорість політичної реклами. Визнаючи важливість політичної реклами у формуванні суспільного життя, посилений Кодекс зобов'язує підписантів запроваджувати більш суворі заходи прозорості, дозволяючи користувачам легко розпізнавати політичну рекламу за допомогою ефективнішого маркування, зобов'язуючись розкрити спонсора, витрати на рекламу та період показу. Крім того, підписанти зобов'язуються створити ефективні та доступні для пошуку рекламні бібліотеки для політичної реклами.

Забезпечення цілісності послуг. Кодекс посилить заходи щодо зменшення маніпулятивної поведінки, яка використовується для поширення дезінформації (наприклад, фейкові облікові записи, посилення, кероване ботами, видавання себе за іншу особу, зловмисні глибокі фейки), і встановлює тіснішу співпрацю між підписантами для боротьби з проблемами, пов'язаними з такими методами.

Підписанти домовляться про міжсервісне розуміння недозволеної маніпулятивної поведінки та практики поширення дезінформації. Вони також повинні будуть періодично переглядати перелік тактик, методів і процедур (ТТР), які застосовуються зловмисниками, і впроваджуватимуть чітку політику, яка охоплюватиме діапазон виявлених видів поведінки та практик.

Розширення можливостей користувачів. Користувачі будуть краще захищені від дезінформації за допомогою розширених інструментів для розпізнавання, розуміння та позначення дезінформації, доступу до авторитетних джерел та за допомогою ініціатив з медіаграмотності. Зокрема, Кодекс забезпечить впровадження безпечних практик проектування для обмеження поширення дезінформації та забезпечення більшої прозорості їхніх систем рекомендацій, адаптуючи їх для обмеження поширення дезінформації.

Кодекс передбачає, що онлайн-платформи надають кращу підтримку дослідженням дезінформації. Дослідники матимуть кращий і ширший доступ до даних платформ. Це означає забезпечення автоматизованого доступу до неособистих, анонімних, зведених або явно оприлюднених даних, а також роботу

над створенням структури управління для спрощення доступу до даних, які потребують додаткової перевірки.

Новий Кодекс розширить охоплення перевірки фактів на всі країни-члени ЄС і мови, а також гарантує, що платформи будуть більш послідовно використовувати перевірку фактів у своїх службах. Крім того, Кодекс спрямований на забезпечення справедливого фінансування роботи перевіряючих в і кращого доступу перевіряючих до інформації, що полегшує їхню щоденну роботу.

Центр прозорості, доступний для всіх громадян, дозволить легко переглядати виконання заходів Кодексу, забезпечуючи прозорість та регулярне оновлення відповідних даних.

Кодекс містить надійну систему моніторингу, включаючи індикатори рівня обслуговування для вимірювання впровадження Кодексу в усьому ЄС та на рівні держав-членів.

Підписанти Кодексу зобов'язалися співпрацювати та координувати свою роботу під час виборів, коли загроза дезінформаційних кампаній є особливо високою. Як передбачено Кодексом, Підписанти створили систему швидкого реагування, щоб забезпечити швидку та ефективну співпрацю між платформами, організаціями громадянського суспільства та особами, які перевіряють факти, під час виборів, яка запрацює на виборах до Європейського парламенту в червні 2024 року.[104]

Таким чином, використання соціальних мереж у гібридній війні є складним явищем із численними суперечностями регуляції та протидії загрозам. Вирішення цих питань потребує комплексного підходу, який включає координацію між державами корпораціями та громадянським суспільством із залученням інноваційних технологій., регулювання діяльності платформ і підвищення обізнаності суспільства.

РОЗДІЛ 3. ШЛЯХИ РОЗВИТКУ ВИКОРИСТАННЯ СОЦІАЛЬНИХ МЕРЕЖ У ГІБРИДНІЙ ВІЙНІ

3.1. Тенденції розвитку, можливі інструменти та механізми використання соціальних мереж у гібридній війні

Алгоритми соціальних мереж дедалі частіше сприяють поширенню маніпулятивного контенту, оскільки вони налаштовані на максимізацію залучення користувачів. Це дає змогу дезінформації та пропаганді швидше знаходити аудиторію. Разом з тим відмічається зростання популярності закритих платформ у Telegram, Discord, та приватні групи у WhatsApp, що дедалі все більше використовуються для поширення дезінформації через високу анонімність та відсутність модерації. TikTok і YouTube стали основними платформами для поширення відеоматеріалів, які емоційно впливають на аудиторію, що робить їх потужними інструментами в гібридній війні. Використання таргетованого контенту, що враховує культурні, мовні та регіональні особливості аудиторії. Це робить пропаганду більш переконливою для різних груп населення.

Значного розвитку набувають можливі інструменти та механізми як створення, так і протидії інформаційного впливу через Автоматизація боти, що дозволяють проводити масове створення фейкових акаунтів, які можуть генерувати і поширювати маніпулятивний контент у великих масштабах. Це може бути посилене за рахунок мікротаргетингу, який дозволяє використовувати будьякі платформи для пошуку вразливих груп і націлювання на них з урахуванням їхніх інтересів, страхів і переконань.

Для посилення ефекту можна створювати дезінформаційні мережі, що здійснюють координацію дій кількох платформ одночасно для поширення єдиного наративу. Це створює ілюзію достовірності інформації через її повторення з різних джерел. Більш того, останні роки спостерігається цілеспрямоване впровадження потрібних наративів безпосереднє через пошукову систему Яндекс, коли відповіді на пошукові запити формуються по заздалегідь сформованим темникам.

Поширенням та дієвим стає також напрямок, що пов'язано зі створенням "фабрик тролів" – наймання людей, які цілеспрямовано беруть участь у дискусіях, поширюють пропаганду або дискредитують альтернативні погляди.

До новітніх технологій слід також віднести Deepfake-контент, що створюється за допомогою штучного інтелекту. Застосування технологій штучного інтелекту дозволяє створювати такі фейкові відео, фото та тексти, які складно відрізнити від справжніх.

Таким чином, можемо спрогнозувати основні тенденції щодо розвитку використання соціальних мереж у гібридній війні:

Зростання ролі штучного інтелекту: Інструменти штучного інтелекту дозволяють швидше аналізувати настрої аудиторії та адаптувати дезінформацію для досягнення максимальної ефективності.

Децентралізація платформ: Зростання популярності менш контрольованих платформ, таких як децентралізовані соціальні мережі або месенджери.

Поєднання інформаційних кампаній з кібератаками для створення комплексного впливу на об'єкти інфраструктури та громадську думку.

Використання ігрових елементів, щоб залучати аудиторію до створення або поширення контенту. Наприклад, заохочення лайків, репостів чи участі в "челенджах", які непомітно просувають пропагандистські меседжі. Пропагандисти часто використовують меми для популяризації дезінформації, бо вони швидко розповсюджуються та легко запам'ятовуються, особливо серед молоді.

Наймання популярних блогерів чи впливових осіб для ненав'язливого поширення маніпулятивних ідей серед їхніх підписників.

Розробка стратегій, де контент спочатку запускається на одній платформі, а потім просувається через інші, щоб досягти максимального охоплення.

Запровадження правових вимог для платформ, зокрема обов'язкової перевірки джерел контенту та алгоритмів, які поширюють маніпулятивні матеріали.

Уряди стають більш активно співпрацювати з платформами, такими як Facebook, Twitter, YouTube, щоб своєчасно виявляти та видаляти дезінформацію.

Використання штучного інтелекту та великих даних для автоматичного виявлення фейкових акаунтів, ботів і дезінформації.

Об'єднання зусиль між країнами для обміну досвідом і створення єдиних стандартів боротьби з дезінформацією.

Вдосконалення алгоритмів для розпізнавання дезінформації стикається з проблемою обробки величезних обсягів даних.

Разом з тим, надмірне втручання у діяльність платформ викликає суперечки щодо обмеження свободи слова.

Постійно зростає кількість платформ і інструментів, що ускладнює контроль над інформаційними потоками.

Для реалізації ефективних механізмів впливу та протидії потрібна синергія між державними, приватними та міжнародними структурами.

3.2. Організаційно-управлінські та правові заходи використання соціальних мереж у гібридній війні.

Для упорядкування використання організаційно-управлінські заходів щодо використання соціальних мереж у гібридній війні слід вживати наступні заходи:

Формування державних органів або міжвідомчих центрів для моніторингу соціальних мереж і координації інформаційної безпеки. Необхідно і далі розвивати аналітичні центри, які спеціалізуються на вивченні інформаційних загроз. Такі як Центр протидії дезінформації при РНБО, який займається збором і аналізом дезінформаційних кампаній або Центр стратегічних комунікацій та інформаційної безпеки України, який займається протидією дезінформації. [74]

Поглиблення співпраці між органами державної влади (Міноборони, МЗС, СБУ) для ефективного управління інформаційною політикою та оперативного реагування на інформаційні атаки.

Участь технологічних компаній, таких як Meta, Twitter або Google, для видалення маніпулятивного контенту та закриття фейкових акаунтів.

Застосування алгоритмів для автоматизованого моніторингу інформаційних потоків, аналізу контенту та виявлення ботів або координованих кампаній.

Запровадження законів щодо регуляція контенту, що зобов'язують соціальні платформи видаляти дезінформацію та пропагандистські матеріали. Наприклад, у ЄС діє Акт про цифрові послуги (Digital Services Act), який вимагає від платформ боротьби з нелегітимним контентом.

Прийняття законодавчих норм щодо криміналізація дезінформації, введення кримінальної відповідальності за створення та поширення фейкових новин, особливо під час воєнного стану.

Внесення змін до законодавства для захисту цифрового простору, запобігання кібератакам та поширенню шкідливих програм через соціальні мережі. Встановлення правових механізмів, що регулюють діяльність ботів, обмежують автоматизацію контенту та вимагають прозорості щодо використання штучного інтелекту.

Підписання угод із міжнародними структурами, такими як НАТО чи ЄС, для обміну досвідом у протидії інформаційним загрозам.

Разом з тим, всі заходи, що ведуть до обмеження обміном інформацією породжують відповідні проблеми та виклики. Це й проблема балансу між свободою слова і необхідністю обмеження дезінформації. Технічні складнощі в ідентифікації та видаленні дезінформаційного контенту. Глобальний характер соціальних мереж, який ускладнює національне регулювання.

Можна навести приклади вдалої реалізації програм та заходів на фронтах інформаційної війни:

Закриття понад 2,000 проросійських Telegram-каналів, зокрема тих, що поширювали паніку під час активної фази війни у 2022 році. (Україна)

Введення санкцій проти RT (Russia Today) та Sputnik, які поширювали дезінформацію через соціальні платформи. (ЄС) [91]

Програма CISA (Cybersecurity and Infrastructure Security Agency) для протидії пропаганді та кіберзагрозам. (США)

Ефективність таких заходів залежить від поєднання технічних інновацій, міжвідомчої співпраці та активного залучення суспільства.

Участь у глобальних коаліціях протидії дезінформації, таких як *EUvsDisinfo*, яка підтримується Європейським Союзом, для обміну знаннями та найкращими практиками.

З погляду на правові аспекти, в першу чергу необхідно здійснити законодавчі ініціативи, які дозволяють блокувати платформи або контент, що сприяють поширенню пропаганди чи розпалюють конфлікти. Так ще в 2021 Рада національної безпеки і оборони України ухвалила рішення від 11 березня 2021 року Про створення Центру протидії дезінформації, яке було введено в дію Указом Президента України від 19 березня 2021 року № 106/2021. В подальшому було створено Електронну петицію на Офіційному інтернет-представництві Президента України №22/130114-еп в яка мала наступний зміст:

«Протидія дезінформації в Україні. Проєкт Закону України "Про внесення змін до деяких законодавчих актів України щодо протидії дезінформації". На сьогодні проблема створення й поширення дезінформації є загрозою для національної безпеки України, інтересів фізичних та юридичних осіб, їх прав на достовірну та об'єктивну інформацію. Тож, розробивши відповідний законопроект, пропонуємо розглянути питання щодо вдосконалення законодавства України задля встановлення реальної відповідальності для осіб, що спричиняють шкоду суспільним інтересам, уводячи населення в оману.» На жаль за неї було зібрано лише 21 підпис з 25000 необхідних.

Разом з тим, ще 31 січня 2020 року з'явилась повідомлення про те, що Моніторингова місія ООН з прав людини розкритикувала новий законопроект про протидію дезінформації, який ініціювало Міністерство культури, молоді та спорту. В тексті її заяви зазначалось наступне: «Закликаємо українську владу утриматися від встановлення непотрібних обмежень для роботи медіа. Ми поділяємо обурення медіа-спільноти та громадянського суспільства щодо того, що нинішній проект закону про дезінформацію не відповідає міжнародним стандартам прав людини, може підривати свободу ЗМІ та призвести до самоцензури»,

Як повідомляли провідні ЗМІ ще в квітні 2024 р. В Україні готують законопроект про регулювання дезінформації та пропаганди у медіа та соцмережах. Зокрема, він має контролювати роботу Telegram, TikTok та YouTube. Над розробкою документа працюють із кінця березня. Влада зобов'язана вжити заходів для регулювання Telegram. Зокрема, необхідні такі кроки:

Зробить видимими власників анонімних каналів. Це, змусить їх нести відповідальність за контент, що поширюється, і підвищить довіру до Telegramканалів.

Створити реєстр суб'єктів медіадіяльності у Telegram. Це дозволить чітко визначити, які канали є медіа, а які ні, та застосовувати до них відповідні норми.

Боротьби з рекламою – деанонімізувати власників каналів, щоб можна було встановити, хто замовляє таку рекламу.

Відкрити в Україні представництво Telegram, що дозволить українській владі ефективніше співпрацювати з месенджером.

Про це повідомив голова Центру протидії дезінформації при РНБО Андрій Коваленко в інтерв'ю Forbes. Проект закону розробляють спільно РНБО, СБУ та Верховна Рада.

Зазначається, що на підставі майбутнього закону влада зможе вимагати від соціальних мереж і платформ блокувати той чи інший канал. Станом на 19 квітня в Україні вже заблоковано 200 YouTube-каналів та 24 акаунти в TikTok.

Також передбачається запровадження обов'язкової реєстрації рекламних кампаній у соціальних мережах для ідентифікації джерел фінансування (наприклад, подібно до законів у США, які регулюють політичну рекламу в соцмережах) та відповідну відповідальність платформ. Уряди примушують соціальні мережі до відповідальності за поширення дезінформації, зокрема, через штрафи або блокування платформ, які не дотримуються стандартів (законопроекти в Німеччині, Закон про цифрові послуги в ЄС).

Деякі компанії, такі як Meta, мають штаб-квартири за межами країн, які страждають від дезінформації. Це ускладнює юридичний процес.

Зловмисники використовують дедалі складніші інструменти, як-от deepfake та генеративний ШІ, для створення контенту, який складно відрізнити від справжнього. Жорсткі закони можуть бути використані для обмеження свободи вираження поглядів, якщо вони неправильно застосовуються.

Наприклад, у Німеччині діє Закон NetzDG (2017 р.), що вимагає від платформ видаляти незаконний контент протягом 24 годин після отримання скарги. Так саме і у США діють відповідні програми боротьби з іноземним втручанням у вибори, що включають перевірку реклами на Facebook і Twitter. [98]

Ці заходи демонструють, як країни адаптуються до нових викликів і використовують різні підходи для захисту інформаційного простору в умовах гібридних загроз.

3.3. Рекомендації щодо використання соціальних мереж у гібридній війні

Системний підхід до використання соціальних мереж у гібридній війні базується на координації інформаційних, технологічних, управлінських і правових компонентів для досягнення стратегічних цілей. Гібридна війна вимагає використання як військових, так і невійськових методів, а соціальні мережі стають основним інструментом впливу через свою доступність, масовість і здатність

формувати громадську думку. У табл. 3.1. ми зробили спробу виокремити основні системні компоненти щодо використання соціальних мереж у гібридній війні.

Таблиця 3.1. Основні компоненти системного підходу щодо використання соціальних мереж у гібридній війні

Складові стратегії	Сутність системних складових
1. Стратегічне планування	Використання соціальних мереж у гібридній війні є частиною комплексної інформаційної стратегії. Це передбачає: Створення та поширення ключових наративів, які підтримують політичні чи військові цілі. Вибір цільової аудиторії (наприклад, молодь, політичні опоненти, міжнародна спільнота) для максимального впливу. Використання алгоритмів платформ для підвищення видимості контенту.
2. Технологічні інструменти	Бот-мережі : автоматизовані акаунти для масового поширення інформації. Алгоритмічні маніпуляції : адаптація контенту під тренди та емоційні реакції. Deepfake і AI : створення контенту для дискредитації осіб або створення ілюзії громадської підтримки. Кібератаки : втручання у функціонування платформ або цільових акаунтів.
3. Інформаційні операції	Пропаганда : підтримка офіційних позицій або створення позитивного образу агресора. Дезінформація : поширення фейків для маніпуляції громадською думкою. Психологічний тиск : створення паніки чи невпевненості серед населення.
4. Моніторинг і аналіз	Системний підхід включає регулярний моніторинг активності в соціальних мережах: Виявлення трендів і контенту, який може бути шкідливим.
	Використання аналітичних платформ для відстеження поширення інформації. Оцінка ефективності кампаній впливу.

5. Правове забезпечення	У багатьох країнах розробляються закони для регулювання використання соціальних мереж у контексті гібридної війни: Блокування або обмеження доступу до платформ, що поширюють дезінформацію. Зобов'язання платформ видаляти шкідливий контент. Відповідальність за використання бот-мереж.
6. Міжнародне співробітництво	Соціальні мережі глобальні за своєю сутністю, тому міжнародна співпраця критично важлива: Спільні ініціативи щодо боротьби з фейками та пропагандою. Обмін досвідом і технологіями між країнами. Розробка загальних стандартів прозорості для соціальних мереж.
7. Медіаграмотність	Захист від використання соціальних мереж у гібридній війні включає навчання громадян критичному мисленню: Кампанії з підвищення обізнаності про дезінформацію. Впровадження медіаграмотності у шкільну та вищу освіту.

У російсько-українській війні Росія активно застосовує бот-мережі для створення ілюзії громадської підтримки, deepfake для дискредитації українських лідерів і дезінформацію для підризу міжнародної довіри до України. Водночас Україна відповідає стратегією прозорої комунікації, мобілізацією суспільства та залученням міжнародної підтримки для протидії дезінформації. Системний підхід до використання соціальних мереж дозволяє максимально ефективно впливати на інформаційний простір і захищати національні інтереси.

Таблиця 3.2. Рекомендації щодо використання соціальних мереж у гібридній війні

Напрями діяльності	Зміст діяльності
Для громадян	
Моніторинг та	Використання систем моніторингу соціальних мереж
аналітика:	для ідентифікації загроз і дезінформації. Інтеграція штучного інтелекту для автоматичного аналізу великого обсягу даних і виявлення ворожих інформаційних кампаній.

Створення центрів стратегічних комунікацій:	Координація міждержавних зусиль для розробки спільних наративів, які протидіють дезінформації. Пропагування офіційної позиції через створення та активне ведення урядових акаунтів у соціальних мережах.
Співпраця з технологічними компаніями:	Залучення платформ до зусиль із видалення фейкових акаунтів і контенту, що підриває національну безпеку. Забезпечення прозорості алгоритмів і впровадження політик щодо перевірки фактів.
Навчання громадян:	Організація інформаційних кампаній для підвищення медіаграмотності серед населення. Включення курсів з аналізу медіаконтенту в освітню програму.
Для Збройних сил:	
Оперативна протидія ворожим кампаніям:	Впровадження інформаційно-психологічних операцій, які запобігають паніці серед населення. Використання соціальних мереж для поширення правдивої інформації під час активних бойових дій.
Використання кібервійськ:	Ідентифікація та нейтралізація ворожих ботів і координованих кампаній дезінформації.
Для громадянського суспільства	
Фактчекінг:	Створення незалежних платформ для перевірки фактів, таких як <i>StopFake</i> . Активне поширення достовірної інформації у соціальних мережах.
Партнерство з державними органами:	Обмін інформацією щодо підозрілих акаунтів або ворожих кампаній.
Для соціальних платформ:	
Автоматичне виявлення фейків:	Використання алгоритмів для відстеження координованих атак і пропагандистських матеріалів.
Підтримка прозорості:	Відкриття інформації про джерела фінансування рекламних кампаній. Обмеження доступу до інструментів таргетингу, які можуть бути використані для розпалювання конфліктів.
Механізми реалізації:	

Поширення позитивних наративів:	Акцент на історіях успіху, об'єднавчих ідеях для підняття морального духу.
Протидія ботам:	Використання штучного інтелекту для ідентифікації та блокування автоматизованих акаунтів.
Розробка спільних стандартів протидії дезінформації:	Співпраця з країнами-членами для запровадження єдиних правил виявлення та боротьби з пропагандистськими кампаніями в соціальних мережах. Підтримка таких ініціатив, як <i>NATO StratCom COE</i> (Центр передового досвіду стратегічних комунікацій НАТО), який займається вивченням впливу соцмереж на безпеку.
Фінансування проєктів медіаграмотності:	Інвестиції у глобальні програми з підвищення рівня медіаграмотності серед населення. Організація конференцій, семінарів і тренінгів для урядів і громадянського суспільства.
Технічна допомога:	Надання країнам, які є об'єктом гібридної агресії, ресурсів для розвитку кібербезпеки та створення ефективних систем моніторингу інформаційного простору.
Для бізнесу та технологічних компаній	
Розширення політик модерації контенту:	Розробка та впровадження інструментів, які блокують пропаганду і фейкові новини ще на етапі їх поширення.
Вдосконалення алгоритмів виявлення дезінформації:	Інвестиції в технології штучного інтелекту для автоматизованої перевірки фактів і аналізу мережових взаємозв'язків.
Підтримка прозорості таргетованої реклами:	Забезпечення доступу користувачів до інформації про джерела фінансування та цільову аудиторію рекламних кампаній.
Захист персональних даних:	Посилення політики захисту приватності, щоб мінімізувати використання персональних даних у деструктивних цілях.
Тенденції майбутнього розвитку	

Інтеграція технологій штучного інтелекту (ШІ):	ШІ може використовуватись як для ідентифікації фейкових новин і ботів, так і для їх створення. Зростає важливість розробки етичних стандартів і регуляцій для використання ШІ у соцмережах.
Боротьба з deepfake-технологіями:	Зростає популярність використання deepfake для створення візуально переконливих маніпулятивних матеріалів. Розробка інструментів для автоматичного виявлення таких матеріалів є важливою.
Реалізація комплексного підходу:	Жодна окрема ініціатива не може повністю протидіяти використанню соцмереж у гібридній війні. Необхідна взаємодія урядів, технологічних компаній і громадянського суспільства.
Оцінка ефективності заходів	Регулярний аналіз впливу запроваджених ініціатив для їх вдосконалення.

Для подолання негативних наслідків соціальних мереж у гібридній війні, слід системно запроваджувати використання систем моніторингу соціальних мереж для ідентифікації загроз і дезінформації. Цьому має сприяти інтеграція штучного інтелекту для автоматичного аналізу великого обсягу даних і виявлення ворожих інформаційних кампаній та координація міждержавних зусиль для розробки спільних наративів, які протидіють дезінформації. З іншого боку держава має прикладати зусилля для пропагування офіційної позиції через створення та активне ведення урядових акаунтів у соціальних мережах. Залучення платформ до зусиль із видалення фейкових акаунтів і контенту, що підриває національну безпеку та забезпечення прозорості алгоритмів і впровадження політик щодо перевірки фактів.

Впровадження активних інформаційно-психологічних операцій, які запобігають паніці серед населення. Використання соціальних мереж для поширення правдивої інформації під час активних бойових дій і, одночасно, ідентифікація та нейтралізація ворожих ботів і координованих кампаній дезінформації.

Розширення мережі незалежних платформ для перевірки фактів, таких як *StopFake* – активне поширення достовірної інформації у соціальних мережах.

Обмін інформацією щодо підозрілих акаунтів або ворожих кампаній та Використання алгоритмів для відстеження координованих атак і пропагандистських матеріалів.

Ці рекомендації можуть стати основою для розробки стратегії протидії ворожим кампаніям у соціальних мережах, спрямованим як проти держави, так і проти суспільства в цілому.

ВИСНОВКИ.

Таким чином в роботі було проведено комплексне дослідження та аналіз можливостей, викликів та ризиків використання соціальних мереж у гібридній війні зроблені конкретні пропозиції та розроблені рекомендації щодо використання соціальних мереж для забезпечення перемоги.

Під час роботи було:

1. Проаналізовано світовий досвід використання соціальних мереж у гібридній війні та їх вплив на громадську думку. Визначено що стан наукової розробки проблеми використання соціальних мереж у гібридній війні перебуває на етапі активного розвитку. Попри значний прогрес у розумінні механізмів маніпуляції та впливу, існує низка викликів, які вимагають міждисциплінарного підходу, міжнародної співпраці та розробки нових методів аналізу й протидії. Констатовано, що соціальні мережі залишаються не лише інструментом, а й самостійним полем сучасних конфліктів.

2. Визначені основні переваги та можливі ризики, що несуть соціальні мережі у гібридній війні. Вони дозволяють охоплювати мільйони людей у режимі реального часу, що робить їх ідеальним інструментом для інформаційних атак. Їх глобальна доступність дозволяє проводити операції на міжнародному рівні без фізичної присутності.

Навіть після закінчення інформаційної кампанії її наслідки можуть впливати на суспільство протягом тривалого часу, а використання штучного інтелекту, алгоритмів і автоматизації значно підвищує ефективність інформаційних операцій.

Тобто Україні необхідно активно враховувати зарубіжний досвід для зміцнення інформаційної безпеки та протидії гібридним загрозам. Вести власні розробки національної стратегії використання соціальних мереж для боротьби з дезінформацією. Здійснювати інтеграцію міжнародних стандартів регулювання

діяльності соціальних платформ, а також спрямовувати зусилля на створення власних цифрових платформ і підвищення медіаграмотності населення.

Соціальні мережі залишаються ключовим елементом сучасних конфліктів, і їх ефективне використання або протидія вимагає комплексного підходу на основі світового досвіду.

3. Проведена оцінка поточного стану використання соціальних мереж у гібридній війні Україні та досліджені бар'єри, що стримують розвиток використання соціальних мереж у гібридній війні. Їхній вплив на громадську думку проявляється через поширення дезінформації, поляризацію, маніпуляції та мобілізацію. Для протидії цим загрозам важливо розвивати критичне мислення та медіаграмотність, підвищувати стійкість державних інституцій до інформаційних атак, впроваджувати міжнародні механізми регулювання діяльності соціальних платформ.

4. Розроблені рекомендації щодо ефективного використання соціальних мереж у гібридній війні з урахуванням історичного контексту. Для ефективної протидії загрозам Україна повинна продовжувати розвивати власну інформаційну стратегію, підвищувати технологічні можливості та посилювати міжнародну співпрацю. Водночас акцент на медіаграмотність суспільства є критично важливим для зміцнення інформаційної стійкості.

5. Досліджено потенційний вплив соціальних мереж на громадську думку. Використання соціальних мереж у гібридній війні є складним явищем із численними суперечностями у регуляції та протидії загрозам. Вирішення цих питань потребує комплексного підходу, який включає координацію між державами, корпораціями та громадянським суспільством із залученням інноваційних технологій, регулювання діяльності платформ і підвищення обізнаності суспільства. Для реалізації ефективних механізмів впливу та протидії потрібна синергія між державними, приватними та міжнародними структурами.

Зроблені рекомендації можуть стати основою для розробки стратегії протидії ворожим кампаніям у соціальних мережах, спрямованим як проти держави, так і проти суспільства в цілому

СПИСОК ВИКОРИСТАНИХ ДЖЕРЕЛ

1. Андрієвський Т. Концептуалізація поняття гібридної війни: політологічний вимір, Сучасне суспільство. 2017, Випуск 1 (13). URL: <http://surl.li/lthyd> (дата звернення: 24.07.2023).
2. Бебик В. М. Інформаційний простір як театр військових дій: війська, зброя, розвідка, контррозвідка. / В. М. Бебик // Міжнародні відносини. Політичні науки №18. – 2018. – [Електронний ресурс] — Режим доступу: http://journals.iir.kiev.ua/index.php/pol_n/arti...
3. Бернейс Едвард. Пропаганда. / Едвард Бернейс. – К.: Видавничий дім «Сварог», 2022. – 128 с.
4. Белєсков М. Сучасний російський спосіб ведення війни: теоретичні основи і практичне наповнення: аналіт. доп. – К.: НІСД, 2021. – 29 с. URL: <https://niss.gov.ua/sites/default/files/2021-02/analitichna-dopovid.pdf> (дата звернення: 29.06.2023).
5. Близнюк А. Гібридна війна ХХІ століття. Пропаганда як основна складова у політичних, соціальних та етнічних протистояннях / А. Близнюк // Intermarum: історія, політика, культура. – 2015. – Вип. 2. – С. 390-399. – Режим доступу: http://nbuv.gov.ua/UJRN/inhpc_2015_2_32.
6. Веселова Л.Ю. Кібербезпека в умовах гібридної війни: адміністративно-правові засади: монографія. – Одеса: Видавничий дім «Гельветика», 2020. – 488 с.
7. Війна Росії проти України. Російська пропаганда як складова «гібридної війни» – [Електронний ресурс] – Режим доступу: <http://socialscience.com.ua/article/1392>.
8. Гібридна війна як форма сучасного міжнародного конфлікту

[Електронний ресурс]. – Режим доступу:

http://journals.iir.kiev.ua/index.php/pol_n/arti...

9. Гібридна війна: in verbo et in praxi : монографія / Донецький національний університет імені Василя Стуса / під. заг. ред. проф. Р.О. Додонова.

– Вінниця : ТОВ «Нілан- ЛТД», 2017. – 412 с.

10. Гібридна війна: сутність та структура феномену [Електронний ресурс].

– Режим доступу: http://journals.iir.kiev.ua/index.php/pol_n/arti...

11. Гібридні загрози Україні і суспільна безпека. Досвід ЄС і Східного партнерства. Аналітичний документ. – К.: © Центр глобалістики «Стратегія ХХІ», 2018. – 17-20 с. URL: https://www.civic-synergy.org.ua/wpcontent/uploads/2018/04/blok_XXI-end_0202.pdf (дата звернення: 21.05.2023).

12. Гітінз Еліот. Ми – Bellingcat. Онлайн-розслідування міжнародних злочинів та інформаційна війна з Росією / пер. з англ. Орина Ємельянова. – К.: Наш Формат, 2022. – 240 с.).

13. Голопатюк Л., Тимошенко Р. Визначення та аналіз особливостей складових сучасних воєнних конфліктів / Збірник наукових праць Центру воєнностратегічних досліджень Національного університету оборони України імені Івана Черняхівського. – 2017. – № 1. URL: <http://znp-cvsvd.nuou.org.ua/article/view/125468> (дата звернення: 29.04.2021).

14. Горбань Ю. О. Інформаційна війна проти України та засоби її ведення / Ю. О. Горбань // Вісник Національної академії державного управління при Президентові України. – 2015. – № 1. – С. 136-141. – Режим доступу: http://nbuv.gov.ua/UJRN/Vnadu_2015_1_21.

15. Горбенко В.І. Кібервійни та кібербезпека в сучасному світі. URL:

https://moodle.znu.edu.ua/pluginfile.php/483537/mod_resource/content/1/%D0%BB%D0%B5%D0%BA%D1%86%D1%96%D1%8F%202.pdf (дата звернення: 19.12.2023).

16. Горбулін В., Бадрак В. Над прірвою. 200 днів російської війни. – К. : Брайт Букс, 2023. 275 с.
17. Грабовський С. «Гібридна війна»: історія і сутність. До постановки питання / С. Грабовський // Вісник КНУ імені Тараса Шевченка. Українознавство. – 2016. – Вип. 1. – С. 19-22. – Режим доступу : http://nbuv.gov.ua/UJRN/VKNU_ukr_2016_1_7.
18. Дем'єн ван Пуївелде «Гібридна війна – чи вона взагалі існує?» – [Електронний ресурс] – Режим доступу : <https://www.nato.int/docu/Review/2015/Also-in-20....>
19. Деркаченко Я. Інформаційно-психологічні операції як сучасний інструмент геополітики / Я. Деркаченко // Глобальна організація союзницького лідерства. – 2016. – [Електронний ресурс] – Режим доступу: <http://goalint.org/informacijno-psixologichni-o....>
20. Джолос О. Захист інформаційного простору / журнал «Україна до НАТО»; Ukraine to NATO. URL: <https://ukrainetonato.com.ua/bezpeka/zakhystinformatsiynoho-prostoru/> (дата звернення: 14.08.2023).
21. Дзюба Т. М. Механізм інформаційно-психологічного впливу на психіку людини у гібридній війні / Т. М. Дзюба, Н. М. Волошина, І. В. Пампуха // Збірник наукових праць Військового інституту Київського національного університету імені Тараса Шевченка. – 2016. – Вип. 51. – С. 91-99. – Режим доступу: http://nbuv.gov.ua/UJRN/Znpviknu_2016_51_14.
22. Доктрина Військ зв'язку та кібербезпеки Збройних Сил України. URL: <https://drive.google.com/file/d/1IUbl25aEZ1NX1AHc8KIEEyD6AifekcrJ/view> (дата звернення: 21.01.2024).
23. Доповідь щодо ситуації з правами людини в Україні 1 серпня 2021 – 31 січня 2022. URL: <https://www.ohchr.org/sites/default/files/202204/33rdReportUkraine-ua.pdf> (дата звернення: 25.07.2022).

24. Дубровинський Г. Р. Особливості взаємодії масової комунікації та психологічного впливу / Г. Р. Дубровинський, А.Ю. Ділай // Актуальні проблеми соціології, психології, педагогіки. – 2014. – Вип. 2. – С. 68-74. – Режим доступу: http://nbuv.gov.ua/UJRN/apspp_2014_2_11 .

25. Є. Магда. Гібридна війна: внутрішній фронт – [Електронний ресурс] – Режим доступу: <https://site.ua/evgen.magda/1170/>

26. Євроінтеграційний вектор розвитку та реалізація національних інтересів України : монографія / [Д. В. Карамишев, Н. В. Мирна, Л. Ю. Величко та ін.] ; за заг. ред. д.держ.упр., проф. Д. В. Карамишева. – Х. : Вид-во ХарПІ НАДУ «Магістр», 2021. – 204 с. URL: https://ipa.karazin.ua/wpcontent/themes/education/filesforpages/science/Karamyshev_2021.pdf (дата звернення: 19.01.2024).

27. ЗМІ як інструмент політичного PR – [Електронний ресурс] – Режим доступу: <http://social-science.com.ua/article/818>

28. Зубарева М.А. Аналіз інформаційної війни між Росією та Україною в інформаційному суспільстві / М. А. Зубарева // Інформаційне суспільство. – 2015. – Вип. 21. – С. 6-11. – Режим доступу: http://nbuv.gov.ua/UJRN/is_2015_21_3.

29. І. Ляльков «Гібридна війна» Росії за створення «Русского міра». Як це відбувається і що робити. – [Електронний ресурс]. – Режим доступу: <http://ukrnationalism.com/publications/3092-hibr...>

30. Ільченко Л. Експерти Давоса вперше поставили дезінформацію на перше місце серед світових ризиків / Сайт «Економічна правда». 2024, 10 січ. URL: <https://www.epravda.com.ua/news/2024/01/10/708604/> (дата звернення: 12.01.2024).

31. Капнік О. Кремль рекордно збільшив оборонний бюджет для продовження війни – аналітики ISW / ТСН. 2023, 29 лист. URL: <https://tsn.ua/svit/kreml-rekordno-zbilshiv-oboronniy-byudzheth-dlya-prodovzhennyaviyni-analitiki-isw-2460451.html> (дата звернення: 26.01.2024).

32. Кехейн Адам. Взаємодія з ворогом. Як працювати з людьми, які не викликають ні довіри, ні симпатій / пер. з англ. Дмитро Кожедуб. – 3-тє вид. – К.: Лабораторія, 2022. – 160 с.
33. Кобільник Б.Ю. Роль інформаційно-психологічних впливів у інформаційній війні / Б.Ю. Кобільник, А.І. Гізун // Матеріали науково-практичної конференції, 23–25.11.2016. – Кропивницький: Філіал НАУ, 2016. – С. 28–29.
34. Когут Ю.І. Гібридна війна нового типу як загроза національній безпеці держав / Ю.І. Когут. К.: Консалтингова компанія «СІДКОН»; ВД «ДАКОР» 2023. 348 с.
35. Косоков О. М. Інформаційний простір як об'єкт управління в системі державної інформаційної політики / О. М. Косоков // Збірник наукових праць Харківського університету Повітряних Сил. – 2016. – Вип. 3. – С. 54-56. – Режим доступу: http://nbuv.gov.ua/UJRN/ZKhUPS_2016_3_14.
36. Костилєва С. Становлення і функціонування національного інформаційного простору України (90-ті рр. XX ст.) у світлі вітчизняних досліджень / Світлана Костилєва – [Електронний ресурс] — Режим доступу: http://history.org.ua/JournALL/graf/graf_2002_11/15.pdf.
37. Кукін І.В. Державне управління інформаційною безпекою особистості : монографія / І.В. Кукін [наук. ред. В.С. Нікіфоренко]. К.: ВД «Дакор», 2023. 416 с. : іл.
38. Курбан О. В. Сучасна гібридна війна та її інформаційна складова / О. В. Курбан // Бібліотекознавство. Документознавство. Інформологія. – 2016. – № 4. – С. 88. – Режим доступу: http://nbuv.gov.ua/UJRN/bdi_2016_4_12.
39. Курбан О. В. Сучасні інформаційні війни в мережевому он-лайн просторі [Текст]: навчальний посібник / О.В.Курбан. – Київ: ВІКНУ, 2016. – С. 43. – Режим доступу: http://www.mil.univ.kiev.ua/files/222_1044284240.pdf
40. Курбан О.В. Сучасні інформаційні війни в мережевому он-лайн просторі [Текст]: навчальний посібник / О.В. Курбан. – Київ: ВІКНУ, 2016. – 286 с.

URL: <http://www.interinf.chnu.edu.ua/res//interinf/Inf%20vijny.pdf> (дата звернення: 06.06.2023).

41. Лазоренко О. А. Інформаційний складник гібридної війни Російської Федерації проти України: тенденції розвитку / О. А. Лазоренко // Стратегічні пріоритети. – 2015. – № 3. – С. 124-133. – Режим доступу: http://nbuv.gov.ua/UJRN/spra_2015_3_19.

42. Латишев К. Стратегія непрямих дій Б.Г. Ліддела Гарта: вчення «алхіміка війни» з Туманного Альбіону / Сайт «Пломінь», 2018, 29 верес. URL: <https://plom.in.club/strategy-indirect-approach-liddell-hart/> (дата звернення: 20.01.2024).

43. Литвиненко О. Інформаційна складова у сучасній гібридній війні проти України: виклики й загрози / О. Литвиненко // Українознавчий альманах. – 2016. – Вип. 19. – С. 171-174. – Режим доступу: http://nbuv.gov.ua/UJRN/Ukralm_2016_19_42.

44. Лідери НАТО затвердили нову Стратегічну концепцію / Сайт НАТО. 2022, 29 червня. URL: https://www.nato.int/cps/uk/natohq/news_197281.htm (дата звернення: 01.07.2022).

45. Лише 58% українців користуються Інтернетом – дослідження [Електронний ресурс] // Економічна правда. – 2018. – 31 січня. – Режим доступу: <https://www.epravda.com.ua/news/2018/01/31/633590/>

46. Лужницький Г. Українська церква між сходом і заходом : нарис історії
64. Малик І. Р. Інформаційні війни в Україні: історія, сучасний стан та перспективи / І. Р. Малик // Видавництво Львівської політехніки. – 2011. – [Електронний ресурс] – Режим доступу до ресурсу: <http://ena.lp.edu.ua:8080/bitstream/ntb/19137/1/...>

47. Магда Є.М. Гібридна війна: сутність та структура феномену. URL: <http://surl.li/osyym> (дата звернення: 30.12.2023).

48. Макфейт Шон. Нові правила війни. Перемога в епоху тривалого хаосу / пер. з англ. Ігор Бігун. – К. : Наш Формат, 2023. – 256 с. ISBN 978-617-8120-98-6 (паперове видання).

49. Марутян Р. Інформаційна складова гібридної війни проти України: сучасні виклики та загрози / Рена Марутян. – 2017. – [Електронний ресурс] – Режим доступу до ресурсу: <https://matrix-info.com/2017/04/13/informatsijna...>

50. Національна стійкість України: стратегія відповіді на виклики та випередження гібридних загроз: національна доповідь / ред. кол. С. І. Пирожков, О. М. Майборода, Н. В. Хамітов, Є. І. Головаха, С. С. Дембіцький, В. А. Смолій, О. В. Скрипнюк, С. В. Стоєцький / Інститут політичних і етнонаціональних досліджень ім. І. Ф. Кураса НАН України. Київ, 2022. 552 с. URL: https://ipend.gov.ua/wp-content/uploads/2022/05/nats_dopovyid.pdf (дата звернення: 21.06.2023).

51. Пожуєв В. І. Осмислення місця і ролі інформації у сучасному суспільстві / В. І. Пожуєв // Гуманітарний вісник Запорізької державної інженерної академії. – 2010. – Вип. 42. – С. 4-13. – Режим доступу: http://nbuv.gov.ua/UJRN/znpgvzdia_2010_42_3.

52. Положення про Міністерство цифрової трансформації України / Урядовий портал. URL: <https://www.kmu.gov.ua/npas/pitannya-ministerstvacifrovoyi-t180919> (дата звернення: 18.04.2023).

53. Положення про Національний координаційний центр кібербезпеки, затверджено Указом Президента України від 07 червня 2016 р. № 242/2016 (зі змінами). URL: https://ips.ligazakon.net/document/U242_16?an=11 (дата звернення: 30.05.2023).

54. Понад 140 країн на Генасамблеї ООН підтримали українську формулу миру / ІА «УКРІНФОРМ». 2023, 23 лют. URL: <https://www.ukrinform.ua/rubricpolitics/3674324-genasamblea-oon-uhvalila-ukrainsku-rezoluciu-sodo-neobhidnostidosagnenna-spravedlivogo-miru.html> (дата звернення: 10.02.2024).

55. Попович К.В. Гібридна війна як сучасний спосіб ведення війни: історичний та сучасний виміри / К.В. Попович. // Науковий вісник Ужгородського університету. – 2016. – С. 75–79. – [Електронний ресурс] – Режим доступу: <https://dspace.uzhnu.edu.ua/jspui/bitstream/lib/13747/1/%D0%93%D0%86%D0%91%D0%A0%D0%98%D0%94%D0%9D%D0%90%20%D0%92%D0%86%D0%99%D0%9D%D0%90%20%D0%AF%D0%9A%20%D0%A1%D0%A3%D0%A7%D0%90%D0%A1%D0%9D%D0%98%D0%99%20%D0%A1%D0%9F%D0%9E%D0%A1%D0%86%D0%91%20%D0%92%D0%95%D0%94%D0%95%D0%9D%D0%9D%D0%AF%20%D0%92%D0%86%D0%99%D0%9D%D0%98.pdf>

56. Почепцов Г.Г. Когнитивные войны в соцмедиа, массовой культуре и массовых коммуникациях/Георгий Почепцов; худож.-оформитель М.С. Мендор. – Харьков: Фолио, 2019, – 314 с. – (Современные технологии).

57. Приборкати Гідру: Як протистояти інформаційній агресії Кремля? // Ukraine World. – 2018. – [Електронний ресурс] — Режим доступу: <https://ukraineworld.org/ua/articles/infowars/hydra>.

58. Про основні засади забезпечення кібербезпеки України: Закон України від 05 жовт. 2017 р. № 2163-VIII. URL: <https://zakon.rada.gov.ua/laws/show/216319#Text> (дата звернення: 09.03.2024).

59. **Про** рішення Ради національної безпеки і оборони України від 15 жовтня 2021 року «Про Стратегію інформаційної безпеки»: Указом Президента України від 28 груд. 2021 р. № 685/2021. URL: <https://www.president.gov.ua/documents/6852021-41069> (дата звернення: 12.05.2024).

60. Про телебачення та радіомовлення Україні Верховна Рада України; Закон від 23.05.2017 р. №2054-VIII (2054-19) – [Електронний ресурс] – Режим доступу: <http://zakon5.rada.gov.ua/laws/show/2782-12> class="hcphplink"><http://zakon5.rada.gov.ua/laws/show/2782-12>

61. Про електронні довірчі послуги: Закон України від 05.10.2017 № 2155-VIII // База даних «Законодавство України» / Верховна Рада України. URL: <https://zakon.rada.gov.ua/laws/show/2155-19> (дата звернення: 07.04.2023).
62. Рева Т. Гібридні загрози та гібридні війни: сутність та аспекти взаємодії, Вісник Львівського університету. Серія філос.-політолог. студії. 2022. Випуск 40, с. 186–191. URL: http://fps-visnyk.lnu.lviv.ua/archive/40_2022/24.pdf (дата звернення: 26.06.2023).
63. Різун В. Методологія виявлення і дослідження масовокомунікаційного впливу [Текст] / В. Різун // Вісник Київського національного університету ім. Т. Шевченка / відп. ред. В. В. Різун. – Київ : Київський ун-т, 2013. – Вип. 1(20): Журналістика. – С. 42-57.
64. Сабрі К.Н. Інформаційно-іміджевий аспект гібридної війни / Молодий вчений. – 2018 р. – № 5 (57). – С. 209. URL: <http://molodyvcheny.in.ua/files/journal/2018/5/51.pdf> (дата звернення: 31.08.2023).
65. Саєнко О. Г. Механізм інформаційно-психологічного впливу в умовах гібридної війни / О. Г. Саєнко. // Вісник Національної академії Державної прикордонної служби України. Серія : Психологія. – 2015. – Вип. 1. – Режим
66. Світова гібридна війна: український фронт : монографія / за заг. ред. В.П. Горбуліна. – К: НІСД, 2017. – 496 с.
67. Севрук В. Рецепт приготування інформаційної війни – [Електронний ресурс] – Режим доступу: http://mymedia.org.ua/articles/infowars/recept_p....
68. Селезньова О.М. Теоретико-методологічне трактування окремих засадничих категорій інформаційного права / О. М. Селезньова // Вісник Асоціації докторів філософії України. Спецвипуск «ІТ право». — Львів, 2016. — [Електронний ресурс] — Режим доступу: <http://aphd.ua/publication-164/>
69. Сили ППО вночі знищили усі 18 російських ракет, серед них – шість «Кинджалів» / Українське національне інформаційне агентство «Укрінформ». 2023,

16 трав. URL: <https://www.ukrinform.ua/rubric-ato/3709737-sipi-ppo-vnociznisili-usi-18-rosijskih-raket-sered-nih-sist-kinzaliv.html> (дата звернення: 16.05.2023).

70. Смола Л. Є. Аспекти ведення інформаційної та гібридної війни в контексті застосування комунікаційних технологій / Л. Є. Смола // S.P.A.C.E. Society, Politics, Administration in Central Europe : електронний науковопрактичний журнал / редкол.: Д. В. Яковлев (голов. ред.), К. М. Вітман (заст. голов. ред.), Д. Ю. Дворніченко (відп. секр.) [та ін.] ; НУ «ОЮА». – Одеса, 2016. – Вип. 1. – С. 48-53.

71. Соколова К. В. Меми як засіб комунікації в інтернет-середовищі / К. В. Соколова // Гуманітарний часопис. – 2012. – № 1. – С. 118-123. – Режим доступу: http://nbuv.gov.ua/UJRN/gumc_2012_1_17.

72. Стратегія і тактика гібридних війн в контексті військової агресії Росії проти України / Борисфен Інтел [Електронний ресурс] – Режим доступу: <http://bintel.com.ua/uk/article/gibrid-war/>.

73. Уизер. Смысл гибридной войны. URL: <http://connectionsqj.org/ru/article/smysl-gibridnoy-voyny> (дата звернення: 29.06.2023).

74. Указ Президента України «Про рішення Ради національної безпеки і оборони України від 28 квітня 2017 року «Про застосування персональних спеціальних економічних та інших обмежувальних заходів (санкцій)» від 15 травня 2017 року № 133/2017 [Електронний ресурс]. – Режим доступу: <http://www.president.gov.ua/documents/1332017-21850>

75. Український медіаландшафт – 2015: аналітичний звіт / За ред. В. Іванова. – К.: ФКА, АУП, 2015.

76. Український медіаландшафт – 2017: аналітичний звіт / За ред. В. Іванова. – К.: Представництво Фонду Конрада Аденауера в Україні, Академія української преси, 2017.

77. У Facebook вже 11 млн українців [Електронний ресурс] / Watcher. – 2018. – 23 січня. – Режим доступу: <http://watcher.com.ua/2018/01/23/u-facebookvzhe-11-mln-ukrayintsiv>
78. Феськов І. Основні методи ведення гібридної війни в сучасному інформаційному суспільстві. URL: <http://surl.li/gmhmn> (дата звернення: 28.06.2023).
79. Франчук А. Б., Пухкал В.С. Забезпечення інформаційної безпеки в умовах євроінтеграції України: правовий вимір. Київ: ТОВ «Видавничий дім «АртЕк», 2018. 422 с..
80. Центр протидії дезінформації. URL: <http://surl.li/hlxsf> (дата звернення: 30.05.2023).
81. Центр стратегічних комунікацій та інформаційної безпеки при Міністерстві культури та інформаційної політики України. URL: <https://mkip.gov.ua/content/centr-strategichnih-komunikaciy-ta-informaciynoi-bezpekipri-ministerstvi-kulturi-ta-informaciynoi-politiki.html> (дата звернення: 30.05.2023).
82. Черновол К. У 2023 році росіяни завдали по Україні десятки тисяч ударів: інфографіка / ІА УНІАН. 2024, 02 січ. URL: <https://www.unian.ua/war/u-2023-roci-rosiyani-zavdali-po-ukrajini-desyatki-tisyach-udariv-infografika12500187.html> (дата звернення: 05.02.2024).
83. Шамрай В.В. Конституційне право в умовах глобалізації та міждержавної інтеграції: теоретико-методологічний аспект: монографія / В.В. Шамрай – Одеса: Фенікс, 2018. – 360 с.
84. Шарре Пол. Невидима армія. Автономна зброя та майбутнє війни/Пол Шарре; пер. з англ. Н. Мочалової. – К.: Форс Україна, 2023. – 448 с.
85. Шутов Р. Пропаганда та маніпуляції / Р. Шутов // Медіадрайвер – [Електронний ресурс] – Режим доступу: http://mediadriver.online/manipuliatsiyi_ta_prop...

86. By Lieutenant General James N. Mattis, U.S. Marine Corps, and Lieutenant Colonel Frank Hoffman, U.S. Marine Corps Reserver (Retired). Future Warfare: The Rise of Hybrid Wars / U.S. Naval Institute. November 2005. URL: <https://www.usni.org/magazines/proceedings/2005/november/future-warfare-risehybrid-wars> (дата звернення: 03.10.2023).

87. Cognitive Warfare: Beyond Military Information Support Operations / NATO Allied Command Transformation. May 9, 2023. URL: <http://surl.li/mqaer> (дата звернення: 22.11.2023).

88. Cyberwarfare: Information Operations in a Connected World (Jones & Bartlett Learning Information Systems Security & Assurance Series) Paperback – Illustrated, 15 Aug. 2014

89. Daniel Kurtz-Phelan. How to Avoid a Great-Power War A Conversation With General Mark Milley / Foreign Affairs. May 2, 2023. URL: <http://surl.li/iogyj> (дата звернення: 27.06.2023).

90. Diego A. Ruiz Palmer. NATO's engagement in Afghanistan, 2003-2021: a planner's perspective / NATO REVIEW. 20 June 2023. URL: <https://www.nato.int/docu/review/articles/2023/06/20/nato-s-engagement-inafghanistan-2003-2021-a-planners-perspective/index.html> (дата звернення: 27.06.2023).

91. ENISA / An official website of the European Union. URL: <https://www.enisa.europa.eu/about-enisa/regulatory-framework> (дата звернення: 22.12.2023).

92. Events that changed America in the twentieth century / edited by John E. Findling & Frank W. Thackeray. p. cm. – (Greenwood Press «Events that changed America».

93. FT Interactive Graphics: The Age of Surveillance Capitalism by Shoshana Zuboff. Abgerufen am 8. August 2024 (britisches Englisch).

94. Hoffman F. G. Hybrid Threats: Reconceptualizing the Evolving Character of Modern Conflict / Frank G. Hoffman // Strategic Forum / Institute for National Strategic Studies National Defense University. – No. 240. – April. 2009.

[Electronic resource] – Mode of access: <http://www.ndu.edu/inss>.

95. Hybridwarfare. [Electronic resource] – Mode of access: http://en.wikipedia.org/wiki/Hybrid_warfare/.

96. LikeWar: The Weaponization of Social Media P.W. SINGER, EMERSON T. BROOKING National Defense, Vol. 103, No. 779 (October 2018), pp. 18-19 (2 pages)

97. Michael Rühle, Clare Roberts. Enlarging NATO's toolbox to counter hybrid threats / NATO Review. 19 March 2021. URL: <http://surl.li/clpqx> (дата звернення: 19.12.2023).

98. NetzDG Transparency Report від 21.01.2021. Режим доступу: <https://about.fb.com/de/wp-content/uploads/sites/10/2021/01/Facebook-NetzDG-Transparency-Report-January-2021.pdf>. Дата звернення 27.04.2021 р., сс. 6-8.

99. Rear Admiral John W. Tammen. NATO's Warfighting Capstone Concept: anticipating the changing character of war / NATO REVIEW. 09 July 2021. URL: <http://surl.li/clvqc> (дата звернення: 19.12.2023).

100. Robots, Junk News Operations, and Political Operatives. Yale University Press, 2020. ISBN 9780300250206

101. Shoshana Zuboff. Harvard Business School, abgerufen am 14. Juli 2019 (englisch).

102. Social Media and Democracy The State of the Field, Prospects for Reform Edited by NATHANIEL PERSILY Stanford University JOSHUA A. TUCKER New York University © Cambridge University Press 2020 doi: 10.1017/9781108890960

103. Statement from National Economic Advisor Lael Brainard on Today's CHIPS & Science Act Announcement / The White House. JANUARY 04, 2024. URL: <http://surl.li/sajia> (дата звернення: 25.01.2024).

104. Strengthened Code of Practice on Disinformation
<https://digital->

[strategy.ec.europa.eu/en/library/2022-strengthened-code-practice-disinformatio](https://digital-strategy.ec.europa.eu/en/library/2022-strengthened-code-practice-disinformatio)

105. The New Yorker: Our Favorite Nonfiction Books of 2019. In: The New Yorker. 18. Dezember 2019, ISSN 0028-792X (englisch, [newyorker.com](https://www.newyorker.com) [abgerufen am 8. August 2024]).

106. The Weaponization of Social Media (2018) — аналіз використання платформ у гібридних конфліктах.

107. Woolley, Samuel and Philip N. Howard. Computational Propaganda: Political Parties, Politicians, and Political Manipulation on Social Media. Oxford University Press, 2018. ISBN 0190931418, 9780190931414