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

КВАЛІФІКАЦІЙНА

РОБОТА МАГІСТРА

на тему: **«Інформаційна зброя в сучасних міжнародних конфліктах»**

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

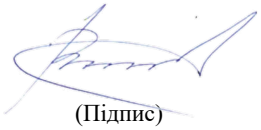
Керівник:
Солових Віталій Павлович., д.держ.упр.,проф.
(науковий ступінь, вчене звання, прізвище, ім'я, по батькові)

Рецензент:
к.соц.н., доцент, Зінчина Олександра Борисівна
(науковий ступінь, вчене звання, прізвище, ім'я, по батькові)

ХАРКІВ - 2025 р.

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

ЗАТВЕРДЖУЮ
завідувач кафедри



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

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

ЗАВДАННЯ
на кваліфікаційну роботу магістра

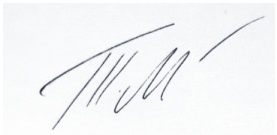
Махотін Тимур Анатолійович
(прізвище, ім'я та по батькові)
Тема роботи «**Інформаційна зброя в сучасних міжнародних конфліктах»**

керівник роботи Солових Віталій Павлович., д.держ.упр.,проф.
(прізвище, ім'я, по батькові, науковий ступінь, вчене звання)
затверджені наказом по університету від «02» червня 2025 року № 4001-5/1324 зі змінами від «10» вересня 2025 року № 4001-5/3049, зі змінами від «6» жовтня 2025 року № 4001-5/3656.
2. Строк подання здобувачем вищої освіти роботи 21 листопада 2025 р.
3. Перелік питань, які потрібно розробити:
Виявити теоретичні основи інформаційної зброї як інструменту впливу в міжнародних конфліктах; розкрити ключові концепції викликів для міжнародної безпеки, спричинених використанням інформаційної зброї в цифрову епоху, з акцентом на психологічні, соціальні та технологічні аспекти; встановити вплив інформаційної зброї на динаміку сучасних конфліктів, спираючись на приклади з України після 2022 року; визначити практичні механізми протидії інформаційній зброї, включаючи роль міжнародних організацій, таких як ООН і НАТО; розробити рекомендації щодо посилення міжнародної безпеки в цифрову епоху, з урахуванням технологічних інновацій, етичних норм і глобальних норм для протидії інформаційним загрозам.

4. План роботи

№ з/п	Назви етапів роботи	Строк виконання етапів
1	Вибір здобувачем теми КРМ і подання заяви на кафедру; затвердження теми та призначення наукового керівника; складання та затвердження індивідуального завдання на виконання КРМ	12.05.2025-30.06.2025
2	Підготовка вступу і розділу 1 КРМ	22.09.2025-30.09.2025
3	Підготовка розділу 2 КРМ	01.10.2025-15.10.2025
4	Підготовка розділу 3 КРМ	16.10.2025-31.10.2025
5	Підготовка висновків і переліку використаних джерел	03.11.2025-14.11.2025
6	Подання студентом завершеної КРМ науковому керівнику для перевірки та оформлення відгуку, перевірка КРМ на відсутність запозичень	17.11.2025-21.11.2025
7	Попередній розгляд КРМ на комісії від кафедри	24.11.2025-28.11.2025
8	Прийняття кафедрою рішення про допуск роботи до захисту в ЕК, оформлення та зовнішнє рецензування	01.12.2025-05.12.2025
9	Захист КРМ в ЕК і присвоєння випускникам кваліфікації	08.12.2025-24.12.2025

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

Здобувач вищої освіти  Тимур Махотін

(підпис) (ім’я, прізвище)

Керівник роботи  Віталій Солових

(підпис) (ім’я, прізвище)

ЗМІСТ

ВСТУП

Актуальність дослідження - цифрова епоха змінила природу конфліктів, де слова і зображення на екранах можуть мати наслідки, подібні до пострілів на фронті. Інформаційна зброя, що охоплює дезінформацію, маніпулятивні кампанії та кібероперації, стала інструментом, який дозволяє впливати на суспільну думку, підривати довіру до влади і навіть визначати перебіг подій без відкритого військового протистояння. З анексії Криму в 2014 році і повномасштабного вторгнення Росії в Україну в 2022 році цей інструмент набув особливої ролі, коли наративи про "нацистський режим" у Києві чи "біолабораторії" фінансування США поширювалися по всьому світу, сіючи сумніви в ефективності допомоги Україні та посилюючи розколи в суспільствах.

Ступінь дослідження теми - за кордоном феномен інформаційної зброї ґрунтовно розроблений у працях RAND Corporation, Reuters Institute for the Study of Journalism, Atlantic Council, NATO StratCom COE, Oxford Internet Institute, Data & Society Research Institute.

В Україні тему активно досліджують: Національний інститут стратегічних досліджень, Центр протидії дезінформації при РНБО, Центр демократії та верховенства права.

Водночас комплексний аналіз впливу інформаційної зброї на динаміку конфліктів після 2022 р., інтеграція ШІ-інструментів у системи протидії та розробка етико-правових рамок регулювання залишаються недостатньо висвітленими, що визначає наукову новизну цієї кваліфікаційної роботи.

Мета дослідження - визначення ролі інформаційної зброї в сучасних міжнародних конфліктах та визначення її впливу на глобальну безпеку.

На основі визначеної мети дослідження виділено **такі завдання**:

- виявити теоретичні основи інформаційної зброї як інструменту впливу в міжнародних конфліктах;
- розкрити ключові концепції викликів для міжнародної безпеки, спричинених використанням інформаційної зброї в цифрову епоху;

- встановити вплив інформаційної зброї на динаміку сучасних конфліктів, спираючись на приклади з України після 2022 року;
- визначити практичні механізми протидії інформаційній зброї, включаючи роль міжнародних організацій, таких як ООН і НАТО;
- розробити рекомендації щодо посилення міжнародної безпеки в цифрову епоху, з урахуванням технологічних інновацій, етичних норм і глобальних норм для протидії інформаційним загрозам;

Об’єкт дослідження - сучасні міжнародні конфлікти.

Предмет дослідження - інформаційна зброя, як інструмент сучасних міжнародних конфліктів.

Методи дослідження:

1. Дискурс-аналіз - застосовується для вивчення наративів і текстів, пов'язаних з інформаційною зброєю, зокрема аналізу пропагандистських матеріалів, дезінформаційних кампаній та їхнього впливу на суспільну думку в контексті сучасних конфліктів.
2. Порівняльний аналіз - використовується для зіставлення еволюції інформаційної зброї в різних історичних періодах, а також порівняння механізмів її застосування в різних конфліктах, стратегій протидії в країнах та ролі міжнародних організацій.
3. Системний аналіз - застосовується для комплексного вивчення інформаційної зброї як системи, що включає взаємодію компонентів (технологічних, психологічних, соціальних), аналізу її впливу на динаміку конфліктів та розробки рекомендацій щодо посилення безпеки, з урахуванням взаємозв'язків між елементами гібридних загроз.
4. Метод кейс-стаді - використовується для детального дослідження конкретних прикладів, зокрема російсько-українського конфлікту після 2022 року, з аналізом конкретних інформаційних операцій їхнього впливу та механізмів протидії.

Практичне значення - готові до впровадження рекомендації для державних органів України, НАТО та ООН: системи раннього виявлення дезінформації, етичні стандарти модерації, програми цифрової грамотності.

Апробація - апробація дипломної роботи пройшла у рамках круглого столу «Стратегічні напрями зовнішньої політики та дипломатії країн світу» Назва тез апробації диплому «Інформаційна зброя в міжнародних конфліктах:виклики для міжнародної безпеки в цифрову епоху»

Структура роботи. Кваліфікаційна робота складається зі вступу, трьох розділів, висновків та списку використаних джерел, який налічує 70 найменувань. Загальний обсяг роботи становить 81 сторінку, з яких основного тексту - 70 сторінок.

РОЗДІЛ 1. ТЕОРЕТИЧНІ ОСНОВИ ІНФОРМАЦІЙНОЇ ЗБРОЇ В МІЖНАРОДНИХ КОНФЛІКТАХ

1.1. Концептуальні засади інформаційної зброї як інструменту впливу на міжнародний простір

Інформаційну зброю в сучасних міжнародних відносинах слід розглядати як системно організовану практику впливу, що поєднує політичні наміри, технологічні засоби та комунікаційні процедури для формування сприйняття й поведінки цільових груп. Йдеться не про суто риторичні впливи або випадкові помилки у висвітленні подій, а про сплановані дії з чітким інтенціональним характером - від вироблення стратегічного наративу до його технічної реалізації та масштабування у мережах.

Такий підхід дозволяє виділити критичні ознаки явища: наявність актора або коаліції акторів з визначеною метою, застосування комплексу інструментів (від традиційних каналів комунікації до цифрових платформ і автоматизованих мереж), а також націленість на досягнення конкретних політичних чи воєнних результатів через зміну знань, емоцій та поведінки аудиторії. Одночасно важливо підкреслити багатовимірність впливу: ефект досягається не лише через зміст повідомлення, але й через його форму, часову синхронізацію, вибір каналів і роботу з мережевою структурою аудиторії - фактично інформаційна операція функціонує як складна система, де кожен елемент підсилює інші[1].

З методологічної точки зору це означає, що аналіз має охоплювати не лише семантику повідомлень, а й техніку їхнього розповсюдження, характер взаємодії між вузлами мережі, а також когнітивні механізми, які роблять аудиторію вразливою до маніпуляцій; без такої комплексної перспективи неможливо ні коректно класифікувати дії як інформаційну зброю, ні розробити дієві інструменти протидії. Ця позиція задає подальшу лінію викладу: з’ясування еволюційних змін у природі впливу, опис типологій інструментів і акторів та аналіз механізмів трансформації інформаційної операції у реальний політичний чи військовий результат.

Поступове осмислення інформаційної зброї вимагає розгляду її генези й зміни інструментів у часі: від інструментованої пропаганди минулого століття до сучасних систем, що поєднують технологічні, організаційні й когнітивні елементи. Спочатку вплив здійснювався через централізовані канали з явною авторизацією джерела і відповідною логікою повторюваної експозиції; основною ставилася задача заповнення інформаційного простору однорідним наративом. Згодом, у міру розширення мережевих комунікацій і появи децентралізованих платформ, інструментарій набув нових якостей: розділення аудиторій, використання форматів, що підвищують емоційне залучення, та застосування механізмів ампліфікації, здатних трансформувати локальні ініціативи в масові хвилі. Ця еволюція означає, що тепер важливі не лише самі повідомлення, але й способи їхнього запуску, часові вікна появи, синхронізація дій у різних каналах і створення видимості багаточисельної підтримки. У результаті поняття інформаційної зброї розширюється: воно охоплює не тільки змістовну маніпуляцію, а й конструкторські рішення щодо мережі розповсюдження, інструментів маскування джерела та процедур, що забезпечують адаптацію наративу до поведінки аудиторії в режимі реального часу[2].

Визначаючи типологію практик і акторів, корисно зосередитися на трьох взаємодоповнюючих площинах: джерела ініціативи, технічні засоби і цільові контексти. Джерелами виступають державні структури, неурядові коаліції, політичні сили, приватні агентства та іноді кримінальні мережі; кожен із них має власну мотивацію - стратегічне послаблення супротивника, внутрішньополітична мобілізація, економічна вигода або дестабілізація регіону за найманим замовленням. Технічні засоби коливаються від традиційних медійних форматів до сучасних цифрових технологій: таргетовані повідомлення, автоматизовані облікові записи, алгоритмічні механізми підвищення видимості й генеративні засоби створення аудіовізуального контенту. Цільові контексти визначаються за масштабом і ефектом - від впливу на локальні спільноти до спроб маніпуляції

міжнародними процесами; тут важливі часові характеристики (швидкість реакції й тривалість впливу) та просторові особливості (географічна прив'язка або транснаціональний характер аудиторій). Розуміння цих площин дозволяє точно формулювати, чому одні заходи є інформаційною операцією зі збройовим потенціалом, а інші - суто політичною комунікацією: критерієм стає системність, цілеспрямованість і здатність спричинити реальну зміну у функціонуванні держави чи суспільства[3].

Поряд із класичними механізмами впливу дедалі важливішою стає роль соціальних і психологічних чинників, які визначають ефективність інформаційної зброї. Сьогодні операції не обмежуються передачею повідомлень, а орієнтовані на формування певного середовища сприйняття, де кожне повідомлення підсилює інші, створюючи комплексну систему переконань і емоційних реакцій. У цьому контексті ключовим стає розуміння когнітивних упереджень аудиторії, ефектів доступності та соціального доказу, коли людина оцінює правдивість повідомлення не стільки через його зміст, скільки через частоту повторень або поведінку оточуючих. Такий підхід дозволяє будувати кампанії, де інформаційний сигнал підтримується не лише змістом, а й контекстом його поширення, що значно підвищує стійкість впливу до спростувань чи критики[4].

Особливе значення має адаптація повідомлень під цифрове середовище. Алгоритми соціальних платформ автоматично відбирають і показують контент, що викликає емоційну реакцію, збільшує взаємодію та створює відчуття масовості. Оператори інформаційних кампаній враховують ці алгоритмічні механізми, формуючи зміст так, щоб він максимально відповідав цифровим патернам сприйняття. У такій системі будь-яка помилка в подачі або неврахування поведінкових моделей аудиторії може звести нанівець ефект навіть добре підготовленого повідомлення.

. У сучасних конфліктах інформаційна операція часто інтегрується з кіберними атаками, дипломатичними ініціативами чи економічними обмеженнями. Така синхронізація дозволяє створювати ефект «комплексного

впливу», коли різні компоненти підсилюють один одного, роблячи загальний результат більш передбачуваним і масштабованим. Це підкреслює, що інформаційна зброя перестала бути лише питанням контенту; вона стала системою, де соціальні, технологічні та організаційні фактори взаємодіють для досягнення стратегічної мети[4].

Платформи та їхні алгоритми визначають не просто канал доставки повідомлень, а саму структуру інформаційного поля, у якому відбувається вплив: вони відбирають те, що бачить користувач, на основі його попередньої поведінки й взаємодій, і тим самим задають контекст сприйняття до того, як людина аналізує зміст. У результаті операція впливу будується не лише на якості наративу, а на вмінні «вписатися» в логіку ранжування й реакційної динаміки платформи - успіх залежить від того, наскільки повідомлення викликає емоцію або взаємодію, яка далі сама по собі підсилює його видимість. Масштабування відбувається через злагоджену роботу мережі вузлів - сторінок, спільнот, лідерів думок і автоматизованих облікових записів - що створює ефект органічності, навіть коли частина активності є штучною. Тестування альтернативних варіантів повідомлень і оперативна корекція за показниками залученості роблять кампанії адаптивними: те, що не працює, відсіюється, а вдалі формулювання швидко поширюються[5].

У цифровому середовищі увага зосереджується на виборі цільової аудиторії та її особливостях, оскільки кожна група користувачів має власні звички, рівень критичного мислення та емоційну сприйнятливість. Від цього залежить ефективність кожного повідомлення. Спостереження за поведінкою аудиторії, аналіз коментарів, лайків і репостів дозволяють визначити оптимальні способи подачі інформації. Повідомлення перестає бути статичним і змінюється залежно від реакції групи, що робить вплив стійким і тривалим, навіть якщо його намагаються спростувати.

Велике значення має контекст поширення повідомлень. Час і місце появи, взаємозв’язок каналів і додаткові підтвердження у вигляді посилань на авторитетні джерела або синхронізовані реакції від різних користувачів

створюють ефект консенсусу і масової підтримки. Це підсилює довіру до інформації, навіть якщо її частина є маніпулятивною або недостовірною. Одночасно користувачі підсилюють ефект самі: помічаючи активність і взаємодію, вони сприймають повідомлення як важливе та загальноприйняте.[6].

Автоматизація й людський контроль працюють разом. Програмні агенти і облікові записи поширюють контент, підтримують обговорення та координують активність, а люди контролюють стратегію, аналізують ефективність і коригують повідомлення. Така взаємодія дозволяє обслуговувати широку аудиторію та підтримувати точність впливу, що робить сучасні інформаційні операції значно ефективнішими за традиційні форми пропаганди[7].

Формування інформаційного впливу в цифровому середовищі стає комплексним процесом взаємодії між змістом, аудиторією та каналами поширення. Кожен елемент підсилює інший, створюючи стійкий ефект впливу, який дозволяє змінювати сприйняття та поведінку цільових груп у довгостроковій перспективі.

У цифрову епоху інформаційна зброя остаточно трансформується в когнітивну зброю, де основним полем бою стає не інформаційний простір як такий, а структура сприйняття та прийняття рішень цільових спільнот. Ключовою особливістю сучасного етапу є перехід від лінійного поширення наративів до нелінійного формування когнітивного середовища, в якому окремі повідомлення виступають лише тригерами для активації вже існуючих упереджень, страхів чи ціннісних конфліктів.

Такий підхід ґрунтується на використанні ефекту «інформаційного перенасичення» та принципу «когнітивного резонансу»: коли одночасно в різних сегментах аудиторії активізуються схожі емоційні реакції, виникає ілюзія загального консенсусу, що радикально знижує критичність сприйняття навіть у високограмотних груп. Водночас генеративні технології дозволяють створювати персоналізовані «інформаційні бульбашки», в яких кожен

користувач отримує варіацію одного й того ж базового наративу, адаптовану під його психологічний профіль, що унеможливлює появу єдиного фронту спростування.

Отже, сучасна інформаційна зброя функціонує як розподілена когнітивна система, що не стільки передає інформацію, скільки конструює реальність сприйняття, роблячи традиційні механізми верифікації та фактчекінгу недостатніми. Її ефективність визначається вже не обсягом поширеного контенту, а глибиною та стійкістю змінених когнітивних схем, які зберігаються навіть після видалення первинних повідомлень. Саме ця властивість робить інформаційну зброю системоутворюючим елементом гібридних конфліктів XXI століття.

1.2. Еволюція інформаційної зброї в цифрову епоху

Перетворення інформаційної зброї в цифрову епоху пов’язане з глибокими змінами не лише в каналах поширення, а й у підходах до впливу на свідомість і поведінку аудиторії. Раніше інформація обмежувалася друкованими виданнями, радіо або телебаченням, сьогодні ж вона інтегрована в багаторівневі системи, де алгоритмічні механізми платформ та поведінкові патерни користувачів визначають, які наративи набувають поширення. У цьому середовищі важливими є не лише самі повідомлення, а й спосіб їх доставки, час появи та взаємодія з іншими матеріалами, що створює складну динаміку впливу. Водночас аудиторія перестає бути пасивним споживачем інформації, її реакції формують подальший потік повідомлень, роблячи сучасну інформаційну зброю адаптивною та здатною підтримувати ефект протягом тривалого часу [8].

Цифрове середовище поєднує масовість і персоналізацію одночасно, що вимагає перегляду традиційних моделей пропаганди і психологічного впливу. Кожен елемент кампанії підпорядкований логіці поширення, яку формують алгоритми платформ, і водночас підкріплюється соціальними реакціями,

створюючи ефект самопідтримки наративу. Інформаційна зброя перестає бути просто передачею повідомлень і стає інтегрованою системою впливу, де стратегія, технології та поведінка аудиторії взаємопов’язані і взаємно підсилюють один одного.

У цифрову епоху значно зростає роль часу та контексту поширення інформації, що перетворює кампанії з простого передавання повідомлень на складні системи управління увагою аудиторії. Важливими стають не лише самі повідомлення, а й моменти їх публікації, взаємозв’язок із суспільно значущими подіями, а також синхронізація з іншими каналами комунікації. Таке точне планування дозволяє створювати ефект присутності інформації у свідомості аудиторії в найбільш критичні моменти, підвищуючи її сприйнятливість і емоційний вплив[9].

Цифрова трансформація інформаційного простору радикально змінила підходи до використання інформаційної зброї, надавши їй нових якостей та можливостей. Головною відмінністю стало перетворення інформації на активний елемент впливу, здатний не лише передавати повідомлення, а й формувати соціальні наративи через взаємодію з алгоритмами цифрових платформ. На відміну від традиційних методів, де ефективність вимірювалася масштабом охоплення, сучасні інформаційні операції фокусуються на точковому впливі, використовуючи дані про поведінку користувачів для створення персоналізованих повідомлень, які резонують з їхніми особистими переконаннями та емоціями.

Особливу роль у цьому процесі відіграє здатність цифрових систем аналізувати та передбачати реакції аудиторії в реальному часі, що дозволяє оперативно корегувати стратегії впливу. Наприклад, використання мікротрекінгу та аналізу великих даних дає змогу виявляти найвразливіші сегменти суспільства та адаптувати контент під їхні специфічні потреби, що значно підвищує ймовірність успішного просування потрібних наративів. Крім того, цифрові платформи надають можливість для створення "вірусних" інформаційних хвиль, коли повідомлення поширюються не лише вертикально

(від джерела до споживача), а й горизонтально - через механізми соціального обміну, що посилює ефект відгуку та самопідтримки дезінформаційних кампаній[10].

Цифрове середовище сприяє інтеграції інформаційної зброї з іншими видами гібридних загроз, такими як кібератаки на критичну інфраструктуру або економічний шпигунство. Такий симбіоз дозволяє комбінувати психологічний вплив з технічними засобами тиску, створюючи комплексні виклики для систем національної безпеки. У цьому контексті інформаційна зброя перестає бути ізольованим явищем і стає частиною ширшої стратегії гібридної війни, де межа між віртуальним і реальним простором стирається, а вплив на суспільну свідомість набуває системного характеру.

Цифрові технології змінили спосіб організації інформаційних кампаній. Соціальні мережі та месенджери дозволяють одночасно впливати на різні групи користувачів, формуючи складні наративи, які охоплюють локальні та глобальні аудиторії. Тепер ефективність операцій визначається не лише кількістю охоплених осіб, а здатністю прогнозувати їх реакції та адаптувати повідомлення у реальному часі.

Алгоритми платформ формують так звані ехо-камери, де користувачі отримують контент, який відповідає їхнім уподобанням і переконанням. Це створює замкнуті кола, де певні наративи повторюються й підсилюються, а критичне мислення зменшується. В таких умовах дезінформаційні кампанії отримують тривалий ефект без додаткового примусу[10].

Штучний інтелект і автоматизовані системи дозволяють створювати персоналізовані повідомлення і тестувати їхню ефективність на різних групах аудиторії. Дані про поведінку користувачів використовуються для швидкої корекції стратегій впливу. Можливість одночасно впливати на тисячі або мільйони людей робить сучасну інформаційну зброю динамічною системою, яка сама адаптується до змін у поведінці аудиторії.

Інформаційні кампанії часто не прагнуть безпосередньо змінити думку, вони створюють умови для формування певних суспільних настроїв.

Поведінка груп визначається накопиченням інформаційних сигналів і емоційним сприйняттям, що змінює рішення окремих осіб і колективів. Ефективність таких кампаній оцінюється через здатність впливати на соціальні процеси, а не тільки на охоплення повідомлень.

У результаті інформаційна зброя в цифрову епоху стає системою, яка поєднує технології, аналіз даних і соціальну динаміку, здатною підтримувати довготривалий ефект і змінювати поведінку аудиторії без явного контролю або примусу.

В останні роки стало очевидним, що цифрові платформи дозволяють впливати на мільйони людей за короткий час. Наприклад, під час виборчих кампаній у кількох країнах були зафіксовані випадки масового таргетованого поширення політичної реклами через соціальні мережі, коли контент підбирався на основі інтересів та поведінки користувачів [10]. Аналіз показав, що персоналізовані повідомлення підвищують ймовірність взаємодії з контентом до 40%, порівняно з традиційною рекламою, що відображає зміну механізмів впливу в цифровому середовищі.

В умовах пандемії COVID-19 поширення дезінформації демонструвало новий тип ефекту. Поширювачі фейкових новин використовували алгоритмічне просування, щоб збільшити охоплення серед певних груп, одночасно поширюючи суперечливі або емоційно забарвлені повідомлення. Дослідження показало, що інформація про міфи щодо вакцин поширювалася у 2-3 рази швидше за науково перевірений контент на тих самих платформах, створюючи локальні «інформаційні спалахи», які важко контролювати.

Військові та кіберструктури також почали активно використовувати цифрові кампанії для впливу на суспільну думку. У деяких конфліктах спеціальні боти генерували контент і координували його поширення, створюючи ілюзію масової підтримки певних наративів [11]. Такі методи дозволяють впливати не на всіх користувачів, а на критичні сегменти, що мають значення для соціальної динаміки, формуючи поведінку аудиторії і посилюючи ефект реальних подій.

Ці приклади показують, що сучасна інформаційна зброя поєднує технології, дані та соціальну психологію, стаючи ефективним інструментом впливу. Вона не просто передає повідомлення, а змінює структуру інформаційного середовища, створюючи умови для формування колективної поведінки і довготривалого ефекту на аудиторію.

Цифрові технології дозволяють порівняно легко порівнювати ефективність традиційних і сучасних методів інформаційного впливу. У класичних кампаніях основну роль відігравали друковані матеріали, радіо або телебачення, а оцінка результатів базувалася на загальному охопленні аудиторії [12]. Сучасні цифрові операції орієнтовані на точковий вплив: збираються дані про поведінку користувачів, відстежуються їхні інтереси і створюються повідомлення, які резонують із конкретними переконаннями та емоціями. Це дозволяє підвищувати ефективність навіть за нижчого загального охоплення, оскільки вплив концентрується на критично важливих сегментах.

Цифрові платформи також дають змогу комбінувати різні канали комунікації для посилення ефекту. Наприклад, одночасне використання соціальних мереж, блогів, месенджерів і коментарів у медіа створює мультиканальний наратив, що повторюється і підкріплюється різними джерелами [13]. Така синхронізація забезпечує ефект присутності інформації у свідомості користувачів і значно підвищує емоційний вплив.

Сучасні кампанії дедалі частіше використовують аналітику великих даних і автоматизовані системи для тестування реакцій аудиторії в режимі реального часу [14]. Це дозволяє оперативно змінювати стратегію поширення, підвищуючи ймовірність досягнення бажаного результату. Мікротрекінг користувачів і алгоритмічне підсилення повідомлень дозволяють точно визначати уразливі сегменти та впливати на них із максимальною ефективністю.

Застосування таких методів змінило саму природу інформаційного впливу. Інформаційна зброя в цифровому середовищі більше не обмежується

передачею повідомлень - вона формує соціальні настрої, моделює поведінку груп і підсилює психологічний ефект від реальних подій [15]. Це робить сучасні інформаційні операції складними системами, де технології, психологія і соціальна динаміка взаємодіють і посилюють один одного, створюючи тривалий вплив на аудиторію.

Цифрова інформаційна зброя підвищує транскордонні ризики. Одні й ті самі наративи здатні впливати на суспільні настрої у різних країнах, не обмежуючись національними кордонами. Це створює ситуації, коли локальні конфлікти або політичні події набувають глобального резонансу без прямого втручання держав, що ускладнює прогнозування наслідків і вимагає від міжнародних організацій нових методів моніторингу [16].

Адаптивність цифрових операцій проявляється у здатності підлаштовуватися під зміни контексту та реакції аудиторії. Наприклад, якщо певний сегмент користувачів проявляє низьку активність або опір наративу, система автоматично змінює формулювання повідомлень, додає нові візуальні елементи або спрямовує інформаційні хвилі через інші канали, підвищуючи ймовірність взаємодії.

Технології машинного навчання дозволяють прогнозувати поведінку аудиторії на основі історичних даних і патернів взаємодії. Це дає змогу будувати інформаційні кампанії як серії інтерактивних кроків, де кожен елемент залежить від попередньої реакції цільових груп. Відтак ефективність операцій оцінюється не через охоплення, а через динаміку змін у колективній поведінці і структурі інформаційного середовища.

Динамічний характер операцій створює нові виклики для міжнародної безпеки. Класичні механізми протидії - обмеження доступу, перевірка фактів або централізоване спростування - втрачають ефективність, бо інформаційні потоки самопідтримуються алгоритмами платформ і поведінковими реакціями користувачів. Це робить необхідним створення адаптивних систем раннього попередження, які поєднують цифровий моніторинг, аналіз соціальних мереж і оцінку впливу на критичні сегменти аудиторії[17].

У цифрову епоху еволюція інформаційної зброї досягає якісно нового рівня, який можна визначити як перехід від пропаганди до когнітивної війни.

Якщо раніше ключовим параметром була швидкість і широта поширення, то тепер визначальною стає глибина проникнення в когнітивні структури та тривалість модифікації поведінкових патернів. Генеративний штучний інтелект і нейромережеві моделі прогнозування дозволяють не лише створювати гіперреалістичний контент, а й моделювати індивідуальні траєкторії сприйняття для кожного користувача, формуючи персоналізовані «когнітивні пастки».

Цей етап характеризується трьома системними нововведеннями:

- перехід від масового до прецизійного когнітивного таргетування на основі психометричних профілів;
- використання «інформаційних градієнтів» - поступового посилення радикальності наративу в межах однієї інформаційної бульбашки без порушення алгоритмічного порогу модерації;
- створення самоадаптивних наративних мереж, які, завдяки зворотному зв’язку від реакцій аудиторії, еволюціонують швидше, ніж традиційні механізми спростування.

Внаслідок цього інформаційна зброя перестає бути інструментом короткострокового впливу і перетворюється на довготривалий фактор формування соціальної реальності, здатний змінювати не лише актуальні оцінки подій, а й базові ціннісні орієнтири та довіру до інститутів. Саме ця властивість робить її стратегічною зброєю нового покоління, ефективність якої вимірюється вже не кількістю переглядів, а ступенем когнітивної колонізації цільових спільнот та стійкістю сформованих установок до зовнішньої корекції.

1.3 Застосування інформаційної зброї та її загрози для міжнародної безпеки

Аналіз трансформації класичних психологічних операцій у цифровому середовищі слід починати з усвідомлення того, що їхня стратегічна мета - вплив на установки, емоції та поведінку цільових груп для досягнення політичних або військово-стратегічних результатів - залишилася незмінною, проте змінюється спосіб її досягнення та тактичні прийоми. У традиційній парадигмі успішність операцій визначалася повторюваністю повідомлень, централізованим контролем інформаційного потоку і тривалістю експозиції через друковані чи ефірні канали. Цифрова епоха зміщує акцент на швидкість поширення імпульсу у мережі, здатність провокувати реакції користувачів та використання цих реакцій для подальшого масштабування наративу[18].

Сучасні психологічні операції в мережевому середовищі характеризуються циклічністю процесу: повідомлення тестуються на малих групах, коригуються відповідно до реакцій і поширюються через локальні центри впливу. Такими центрами виступають тематичні спільноти, канали лідерів думок і інші вузли мережі, здатні підхоплювати та ретранслювати потрібний наратив. Важливо, що оператори прагнуть не прямого нав’язування змісту, а створення умов для органічного поширення - стимулювання дискусій, використання емоційних тригерів та форматованого цифрового контенту, що відповідає комунікаційним звичкам цільової аудиторії.

Зміни торкнулися також способів маскування джерела: замість явної пропаганди застосовуються прийоми, що імітують незалежні або локальні джерела, персональні свідчення та нібито спонтанні історії. Така практика ускладнює ідентифікацію походження повідомлень і робить протидію менш ефективною. Оператори активно використовують оперативне коригування контенту: одночасна поява схожих повідомлень у різних частинах мережі створює ефект масовості та неперервності, а швидка адаптація за показниками взаємодії підтримує актуальність і підвищує переконливість наративу[19].

Сегментація аудиторій у цифровому середовищі базується на поведінкових та демографічних ознаках, а мотиваційні та емоційні тригери реалізуються через різні формати: відео, короткі повідомлення, меми та візуальні фрагменти. Тактика «малих перемог» використовується для поступового формування враження про перевагу власних позицій або слабкість супротивника, що підриває легітимність опонента в очах аудиторії. Одночасно велике значення надається сприйняттю джерела: побудова видимості місцевого або довіреного походження повідомлень, залучення авторитетів спільноти і моделювання партиципативності дискусії підвищують довіру та знижують опір до наратив[20].

Гібридні моделі впливу в сучасних конфліктах поєднують інформаційні, кіберні та військові дії в єдину скоординовану кампанію, де кожен елемент служить підсиленню інших і разом утворює мультиплікаційний ефект; у такому підході інформаційна операція вже не є самостійною акцією, а виступає частиною ширшої стратегії, що планується і здійснюється з урахуванням технічних можливостей і воєнних сценаріїв.

Логіка координації зводиться до синхронізації часових вікон і смислових ліній: інформаційні месседжі готують громадську думку або дискредитують цільові інституції напередодні технічних ударів, кібератаки порушують комунікаційну або фінансову інфраструктуру, а військові дії завершують створений інформаційний наратив, підсилюючи відчуття неминучості або катастрофи[22].

У практиці це означає нобхідність планування кампанії заздалегідь, визначення ключових точок впливу і ресурсів для їхнього одночасного використання, а також ретельного вимірювання синергії ефектів - які повідомлення в який момент підсилюють технічні дії, які технічні збої сприяють поширенню панічних або деморалізуючих наративів.

Координація таких дій вимагає як міжвидової співпраці виконавців, так і доступу до різних каналів впливу, включно з операціями під чужими марками або через проксі-акторів; одночасно вона підвищує стійкість кампанії, бо

нейтралізація одного компонента не гарантує припинення загальної дії. Гібридна логіка також передбачає використання «ефекту відволікання», коли інформаційні потоки навмисно спрямовують увагу суспільства в бік певних подій, створюючи вікно для проведення кібератак або оперативних військових кроків у менш помітний спосіб. З позиції оборони такі кампанії складні для протидії, бо захисні заходи у сфері інформації, кібербезпеки і військовій підготовці мають бути скоординовані; відсутність єдиного координаційного механізму послаблює здатність реагувати на мультиплікаційний характер загрози[21].

Методично аналіз гібридних моделей вимагає одночасного поєднання мережевого аналізу, технічного моніторингу інцидентів та оцінки впливу на суспільну думку, оскільки саме взаємодія технічних розривів і інформаційних наративів створює критичні точки вразливості, які мають бути виявлені задля розробки ефективних протидій.

Операції, орієнтовані на алгоритми, становлять окремий еволюційний етап у практиці інформаційного впливу, коли ключову роль відіграє не стільки масове охоплення, скільки точність і швидкість адресного впливу на окремі сегменти аудиторії. У їхній основі лежить збір і аналіз цифрових слідів поведінки - уподобань, часу перебування на платформі, структури контактів - що дозволяє розділити аудиторію на вузькі групи за інтересами, споживчими патернами або емоційними маркерами; надалі для кожної такої групи створюються варіанти повідомлень, різні за формулюванням, тональністю та візуальним супроводом, які проходять порівняльне тестування на контрольних підгрупах[22].

За результатами такого тестування обираються найбільш ефективні формулювання і масштабується їхнє розповсюдження саме серед тих сегментів, де вони демонструють найвищу конверсію у вигляді реакцій, репостів чи змін у дискурсі.

Автоматизація процесу оптимізації змісту за показниками залученості робить кампанію динамічною: система підсвічує успішні варіанти, які далі

просуваються через рекомендаційні механізми платформ та мережеві центри впливу, тоді як менш успішні варіанти відсіюються або модифікуються. Це зменшує час від задуму до масового розповсюдження і підвищує адаптивність операції.

Такий підхід поєднує технічну майстерність у роботі з даними і розуміння соціокультурних кодів цільових спільнот, бо без адекватного урахування локальних комунікаційних форматів і довіри месиджі не пройдуть навіть у разі високоточного таргетування. Водночас алгоритмічно орієнтовані операції створюють складнішу для виявлення структуру маніпуляції: замість явних масових вкидів виникає багато дрібних, адресних впливів, що накопичуються й у сумі змінюють дискурс або поведінку групи.

Це породжує й етичні та правові питання: застосування подібних методів часто базується на роботі з персональними даними, які можуть збиратися і використовуватися без інформованої згоди, що підриває приватність і створює ризики для демократичних процесів. Одночасно оперативна оптимізація контенту посилює інформаційну вразливість суспільства, оскільки людина опиняється в середовищі, що постійно підлаштовується під її емоційний та поведінковий профіль.

З практичної точки зору протидія таким операціям потребує не лише технічних інструментів виявлення аномалій у потоках даних, а й розвитку цифрової грамотності, прозорості у роботі платформ та норм щодо обробки даних. Без комплексного підходу технічні бар’єри легко долаються новими методами оптимізації. Таким чином, операції, орієнтовані на алгоритми, демонструють, як поєднання даних, порівняльного тестування і автоматичної оптимізації робить інформаційний вплив більш адресним, гнучким і водночас більш підступним для традиційних механізмів захисту.

Особливу небезпеку становлять «гібридні ефекти», коли цифрові інформаційні операції синхронізуються з кіберінцидентами або економічними атаками. Одночасне поширення панічних наративів і атак на критичну інфраструктуру здатне підсилювати економічні та соціальні потрясіння,

ускладнюючи координацію реагування держав і міжнародних організацій. Такий підхід робить кризові ситуації масштабнішими і менш передбачуваними, а реакція на них потребує узгодження дій у багатьох сферах - від кібербезпеки до управління інформаційним простором[23].

Додатковим чинником є швидкість поширення інформації в глобальних мережах. Інформаційні хвилі можуть охоплювати континенти за лічені години, а ефект їхнього впливу накопичується через взаємодію алгоритмів і поведінкових патернів користувачів. У результаті навіть невеликий сегмент цільової аудиторії може спричинити значний зсув у суспільному дискурсі. Ця властивість робить традиційні методи протидії - обмеження доступу, перевірку фактів або централізоване спростування - менш ефективними, оскільки вони не здатні впливати на динамічні, самопідсилювані інформаційні потоки.

Сучасні моделі інформаційної зброї показують, що безпека держав і міжнародних організацій залежить не лише від фізичної та кіберзахищеності, а й від здатності контролювати інформаційне середовище та прогнозувати поведінку аудиторії. Це вимагає інтеграції аналітики цифрових платформ, моніторингу соціальних мереж і швидкого реагування на дезінформаційні хвилі, що створює нові стандарти планування і управління у сфері міжнародної безпеки.

Таргетування окремих сегментів дозволяє створювати локальні ефекти, які накопичуються і змінюють загальний суспільний дискурс. Це ускладнює прогнозування наслідків і робить традиційні механізми реагування недостатньо ефективними.

Комбінація інформаційного впливу з технічними чи економічними заходами підсилює ефект. Наприклад, поширення тривожних наративів у момент збоїв у фінансових або комунікаційних системах посилює паніку і знижує довіру до інституцій. Така синхронізація створює мультиплікаційний ефект і підвищує ризики для стабільності держав.

Алгоритмічно орієнтовані операції прискорюють цикл впливу. Збір цифрових слідів користувачів дозволяє швидко тестувати та коригувати повідомлення для конкретних груп, що підвищує ефективність впливу і зменшує витрати ресурсів. Масштабування успішних варіантів через рекомендні системи платформ забезпечує швидке накопичення ефекту, а дрібні адресні впливи у сумі здатні змінювати поведінку значної частини аудиторії.

У контексті сучасних гібридних конфліктів інформаційна зброя дедалі частіше виступає не допоміжним, а системо утворюючим елементом, що визначає темп і напрямок усієї кампанії. Її стратегічна цінність полягає в здатності створювати «асиметрію сприйняття», коли одна сторона оперує в рамках об’єктивної реальності, тоді як інша формує паралельну когнітивну реальність для цільової аудиторії, роблячи традиційні військові чи дипломатичні інструменти неефективними через попереднє підрив довіри та легітимності.

Особливо небезпечним є ефект «когнітивної інверсії», коли тривала експозиція маніпулятивних наративів призводить до перевороту базових причинно-наслідкових зв’язків у свідомості аудиторії: жертва агресії починає сприйматися як агресор, а реальні факти інтерпретуються як пропаганда. Цей феномен, зафіксований у низці конфліктів 2022–2025 років, демонструє, що інформаційна зброя здатна не лише деморалізувати, а й радикально переформатовати колективну ідентичність і ціннісну матрицю суспільства, створюючи довготривалі внутрішні розколи, які зберігаються навіть після припинення активної фази впливу.

Таким чином, головна загроза сучасної інформаційної зброї для міжнародної безпеки полягає в її потенціалі до незворотної трансформації когнітивного ландшафту держав і суспільств, що робить традиційні механізми стримування та балансу сил частково недієздатними. У цих умовах національна та колективна безпека дедалі більше залежить від спроможності не лише протистояти конкретним кампаніям, а й зберігати базову когнітивну

автономію суспільства - здатність розрізняти реальність і сконструйовану інформаційну симуляцію.

Висновки до розділу 1

Висновки першого розділу формують концептуальну базу для подальшого дослідження: еволюція інформаційної зброї вимагає паралельної еволюції механізмів захисту. З огляду на ідентифіковані технологічні виклики - точність алгоритмічного таргетування, швидкість поширення дезінформації через ехо-камери та синергію у гібридних кампаніях - ефективна протидія не може обмежуватися лише факчекінгом чи традиційною контрпропагандою.

Наголос має бути зміщений на розробку комплексних, технологічно-орієнтованих стратегій. Це включає посилення цифрової стійкості державних інституцій та суспільства, впровадження регуляторних механізмів для забезпечення прозорості алгоритмів і, найголовніше, застосування методів аналізу даних та штучного інтелекту (ШІ) для проактивного виявлення, моніторингу та нейтралізації ворожих інформаційно-психологічних операцій (ІПСО) на ранніх стадіях.

Було визначено, що класичні психологічні операції зберігають стратегічне цілепокладання, проте в мережевому середовищі змінюється підхід до їх реалізації: централізоване управління інформаційним потоком замінюється на ітеративну взаємодію з аудиторією, де зворотний зв’язок і поведінкові дані користувачів визначають ефективність кампанії.

Аналіз цифрових технологій показав, що алгоритми рекомендацій, автоматизовані бот-мережі та генеративні системи контенту дозволяють значно підвищити точність впливу та оперативно адаптувати повідомлення під різні сегменти аудиторії. Це забезпечує стійкість наративів, формує ефект ехо-камер, активує когнітивні механізми сприйняття, такі як ефект доступності, соціальний доказ і упередження підтвердження, та ускладнює своєчасне виявлення й нейтралізацію інформаційних впливів.

Особливу роль у сучасних конфліктах відіграють гібридні моделі впливу, де інформаційні, кібер та військові дії координуються у єдиній кампанії. Така інтеграція дозволяє посилювати ефект кожного компонента, синхронізувати дії та досягати комплексного впливу на цільові системи. Водночас вона потребує ретельного планування, постійного моніторингу та високого рівня координації, що значно ускладнює протидію подібним операціям.

Операції, орієнтовані на алгоритми, демонструють новий рівень точності й адаптивності: порівняльне тестування повідомлень, автоматична оптимізація контенту та таргетування конкретних груп аудиторії дозволяють досягати максимального ефекту за мінімальних витрат ресурсів. Разом із цим виникають етичні та правові ризики, пов’язані з обробкою персональних даних та маніпуляцією суспільною свідомістю, що створює додаткові виклики для міжнародної безпеки.

У підсумку, перший розділ показав, що інформаційна зброя в цифрову епоху набуває багатовимірного характеру, де поєднуються стратегічні цілі, технологічні можливості та когнітивні методи впливу. Така інтеграція створює складний комплекс загроз, що потребує нових підходів до аналізу, протидії та регулювання у глобальному інформаційному просторі.

РОЗДІЛ 2. РОЛЬ ІНФОРМАЦІЙНОЇ ЗБРОЇ В СУЧАСНИХ КОНФЛІКТАХ

2.1. Нормативно-етичні рамки та стандарти протистояння інформаційній зброї

Сучасний інформаційний простір формується під впливом глобальних викликів, серед яких дезінформація, маніпулятивні технології та кібератаки становлять серйозну загрозу для демократичних інститутів і суспільної стабільності. Міжнародні стандарти протидії таким загрозам ґрунтуються на необхідності забезпечити баланс між національною безпекою та дотриманням фундаментальних прав людини, зокрема свободи слова, доступу до інформації та захисту приватності. Основою для цих стандартів слугують Всезагальна декларація прав людини ООН, Міжнародний пакт про громадянські та політичні права, а також резолюції та рекомендації Ради Європи, ООН та ОБСЄ, які регулюють інформаційне середовище.[48][49]

Правові принципи протидії інформаційним загрозам визначають критерії допустимості втручання держави в інформаційний простір. Такі втручання повинні бути законними, необхідними в демократичному суспільстві та пропорційними поставленим цілям. Обмеження поширення дезінформації виправдане лише за умови, що воно не переростає в цензуру або політичну маніпуляцію. Процедурні гарантії включають прозорість дій влади, можливість оскарження рішень та незалежний контроль за їх виконанням. Європейський суд з прав людини неодноразово підкреслював, що обмеження свободи вираження поглядів мають бути чітко визначені законом і не допускати свавілля[50].

Міжнародні організації активно розробляють механізми протидії деструктивним інформаційним впливам. Серед них - кодекси поведінки для платформ соціальних мереж, стандарти прозорості алгоритмів та механізми фактчекінгу. Єврокомісія запровадила Кодекс практики з дезінформації, який зобов’язує технологічні компанії виявляти та блокувати штучно створену дезінформацію, не порушуючи права користувачів на вільний обмін думками.

Однак ефективність таких стандартів залежить від їх уніфікованого застосування та співпраці держав у міжнародних форматах[51].

Гармонізація національного законодавства з міжнародними нормами залишається актуальним викликом, особливо в умовах швидкого розвитку цифрових технологій. Країни, які протидіють інформаційним загрозам через жорстку цензуру або блокування інтернет-ресурсів, часто стикаються з критикою за порушення прав людини. Тому важливим завданням є розробка механізмів, які б поєднували ефективність протидії загрозам із дотриманням демократичних принципів та етичних норм.

Сучасні виклики в інформаційному просторі, такі як дезінформація, маніпулятивні технології та кібератаки, вимагають чітких міжнародних стандартів, що поєднують безпеку з дотриманням прав людини. Естонія після кібератак 2007 року впровадила комплексну стратегію кібербезпеки, яка включала не тільки технічні засоби захисту, а й освітні програми для населення. Обов’язкове вивчення основ кібергігієни в школах та створення центрів моніторингу інформаційного простору у співпраці з НАТО та ЄС дозволили знизити сприйнятливість суспільства до маніпуляцій і сформувати культуру критичного мислення[52].

Франція у 2018 році прийняла закон про боротьбу з маніпуляціями інформацією, який надає судам право вимагати від соціальних мереж видалення фейкових акаунтів та неправдивої інформації під час виборчих кампаній[53]. Особливістю цього закону є судовий контроль за блокуванням контенту, що мінімізує ризики політичного впливу. Вища рада з аудіовізуальних засобів масової інформації моніторить прозорість політичної реклами, демонструючи, як правові механізми можуть інтегруватися в національне законодавство без порушення свободи слова[53].

Угорщина у 2020 році пішла іншим шляхом, надавши уряду надзвичайні повноваження щодо боротьби з дезінформацією під час пандемії COVID-19. Відсутність чітких визначень "неправдивої інформації" та можливість блокування матеріалів без судової перевірки призвели до зловживань і тиску

на незалежні ЗМІ. Цей приклад ілюструє небезпеку надмірної концентрації влади без належних контрбалансів[54].

Глобальна мережа з протидії дезінформації (GDI) об'єднує фактчекінгові організації, академічні інституції та технологічні компанії для координації зусиль у виявленні та спростуванні фейків. Під час президентських виборів у США 2020 року GDI координувала роботу понад 100 організацій, демонструючи ефективність системної взаємодії між державою, громадянським суспільством та приватним сектором[55].

Акт про цифрові послуги ЄС, прийнятий у 2023 році, зобов'язує великі технологічні платформи маркувати контент, створений за допомогою штучного інтелекту, та надавати користувачам інструменти для його ідентифікації. Це рішення стало відповіддю на загрозу маніпуляцій через синтетичні медіа, але його успіх залежить від готовності платформ співпрацювати з регуляторами[56].

Міжнародний досвід показує, що ефективна протидія інформаційним загрозам вимагає комплексного підходу, який поєднує правове регулювання, технічні рішення, освіту та співпрацю. Головне завдання - зберегти баланс між безпекою та свободами, щоб уникнути перетворення заходів протидії на інструменти авторитарного контролю.

Етичні норми для технологій верифікації та модерації контенту в цифровому середовищі набули особливої актуальності у 2024-2025 роках через зростання впливу штучного інтелекту та соціальних мереж на суспільну думку. Однією з ключових вимог стало забезпечення прозорості алгоритмів, які використовуються платформами для виявлення та блокування шкідливого контенту. Наприклад, TikTok у вересні 2025 року оновив свої Правила спільноти, щоб підвищити безпеку користувачів і врахувати культурні особливості різних регіонів. Новий документ визначає стандарти прийнятності контенту для стрічки «Рекомендації», акцентуючи увагу на прозорості критеріїв модерації та можливості оскарження рішень, що приймаються автоматизованими системами. Це свідчить про прагнення

платформи збалансувати автоматизацію з підзвітністю перед користувачами, уникаючи звинувачень у свавіллі чи упередженості алгоритмів[57].

Відповідальність платформ за контент, який вони поширюють, стала обов'язковою вимогою в багатьох країнах. У 2025 році Бразилія прийняла закон, який зобов'язує соціальні мережі вживати заходів для захисту неповнолітніх, зокрема моніторити та обмежувати контент, спрямований на дітей, а також повідомляти про підозрілу експлуатаційну діяльність владі. Платформи, які порушують ці вимоги, ризикують штрафами до 50 мільйонів реалів (близько 9 мільйонів доларів США) або тимчасовим блокуванням. Цей закон також передбачає постійне вдосконалення механізмів верифікації віку користувачів, що підкреслює необхідність незалежного контролю за дотриманням етичних норм і технічних стандартів.

Незалежний аудит алгоритмів та процесів модерації контенту стає все більш поширеною практикою. У Німеччині у 2025 році Федеральне агентство з мереж провело практичні тести платформ перед парламентськими виборами, щоб перевірити їхню готовність виявляти та блокувати дезінформацію та маніпулятивний контент. Під час тестів симулювалися різні сценарії порушень, включаючи поширення фейкових новин та координовані кампанії впливу. Це дозволило оцінити ефективність механізмів реагування платформ і вдосконалити процедури взаємодії з регуляторами.

Цей процес супроводжується активним формуванням спеціалізованих етико-правових рамок для генеративних технологій. У 2025 році Європейська Комісія та НАТО StratCom COE спільно визначили категорію «високоризикового» застосування ШІ в інформаційних операціях, до якої віднесено створення deepfake політичного характеру, автоматизоване мікротаргетування вразливих груп та скоординовані кампанії когнітивного впливу. Такі системи підлягають обов'язковій попередній оцінці впливу на фундаментальні права та незалежному аудиту ще на стадії розробки.

Україна в червні 2025 року запропонувала модель імплементації DSA з національними доповненнями, що передбачає державний реєстр синтетичного

контенту воєнно-політичного спрямування, використання стандарту C2PA для незнімних криптографічних водяних знаків та прискорену судову процедуру (24 години) для видалення матеріалів, які становлять безпосередню загрозу національній безпеці, з обов'язковим публічним протоколом кожного рішення. Венеційська комісія визнала цей підхід пропорційним і таким, що відповідає статті 10 Європейської конвенції з прав людини[66]

На глобальному рівні Резолюція Генеральної Асамблеї ООН A/RES/80/2025 закріпила принцип простежуваності походження синтетичних медіа та право на «цифрове спростування», що гарантує розміщення офіційного спростування поруч із матеріалом, визнаним неправдивим незалежним регулятором. Одночасно ініціатива великих розробників ШІ під егідою НАТО ввела вимогу вбудованого технічного маркування на рівні моделі, що робить видалення метаданих практично неможливим[67].

2.2 Національні та міжнародні стратегії боротьби з дезінформацією

Моделі національного законодавства щодо протидії дезінформації в останні роки зазнали значних змін, спрямованих на уніфікацію підходів та посилення міжнародної співпраці. В Україні, зокрема, у 2024-2025 роках активізувалися процеси гармонізації внутрішнього законодавства з європейськими стандартами, зокрема з Актом про цифрові послуги ЄС, який визначає нові вимоги до прозорості алгоритмів, модерації контенту та протидії дезінформації. Цей документ зобов'язує великі онлайн-платформи вживати заходів для виявлення та блокування шкідливого контенту, а також забезпечувати доступ дослідників до даних для незалежного аудиту. Україна, прагнучи до членства в ЄС, адаптує свої нормативні акти до цих вимог, зокрема через розробку законопроєктів, спрямованих на посилення відповідальності медіа та платформ за поширення дезінформації[58].

Важливим кроком у напрямку міжнародної гармонізації стало впровадження механізмів екстранаціональної взаємодії, зокрема через

співпрацю з міжнародними організаціями та платформами фактчекінгу. Наприклад, Європейська Комісія у 2024 році оновила Кодекс практики з дезінформації, який тепер передбачає демонетизацію поширення фейків, прозорість політичної реклами та посилення співпраці з незалежними фактчекерами. Україна активно долучається до цих ініціатив, зокрема через Центр протидії дезінформації при РНБО, який співпрацює з європейськими партнерами для обміну досвідом та координації дій у протидії гібридним загрозам.

Правовий захист процедур моніторингу інформаційного простору також набув нового виміру. У 2025 році в Україні було запроваджено систему регулярного моніторингу та оцінки ефективності заходів з протидії дезінформації, що включає піврічні та річні звіти про результати реалізації відповідних програм. Ці механізми дозволяють не лише відстежувати динаміку поширення фейків, а й оперативно реагувати на нові виклики, зокрема через координацію дій між державними органами, громадськими організаціями та міжнародними партнерами[59].

Таким чином, сучасні моделі національного законодавства та міжнародної гармонізації спрямовані на створення уніфікованих підходів до протидії дезінформації, які поєднують правові, технічні та освітні заходи. Це дозволяє не лише підвищити ефективність моніторингу інформаційного простору, а й забезпечити його відповідність демократичним стандартам та правам людини.

Сучасні системи раннього попередження та детекції дезінформації ґрунтуються на зборі та аналізі телеметрії - даних про активність користувачів, поширення контенту та поведінкові патерни в цифровому середовищі. Платформи, такі як Facebook і Twitter, використовують алгоритми машинного навчання для виявлення аномальних сплесків активності навколо певних тем або хештегів, що може вказувати на координовані кампанії дезінформації. Стандарти збору даних передбачають моніторинг соціальних мереж, месенджерів і новинних платформ, інтегруючи кількісні індикатори

(швидкість поширення повідомлень, географічне охоплення, кількість репостів) з якісними (семантичний аналіз тексту, оцінка емоційного забарвлення, перевірка джерел)[60].

Для виявлення автоматизованих мереж (ботів) і генеративного контенту, зокрема діпфейків, застосовують спеціалізовані методики. Компанії Google і Microsoft у 2024-2025 роках розробили інструменти, які аналізують мікровирази обличчя, артефакти зображень і аудіоспектри для виявлення штучно згенерованого контенту з точністю понад 90%. Ці технології інтегруються в системи модерації, дозволяючи блокувати або маркувати підозрілі матеріали до їхнього масового поширення.

Європейський Союз у 2025 році запровадив систему раннього попередження, яка об’єднує дані від національних регуляторів, фактчекінгових організацій і технологічних компаній. Ця система використовує машинне навчання для прогнозування потенційних кампаній дезінформації на основі історичних даних і поточних трендів, підвищуючи ефективність протидії гібридним загрозам. Таким чином, сучасні системи детекції поєднують передові технології збору даних з методиками виявлення автоматизованих мереж і генеративного контенту, забезпечуючи комплексний захист інформаційного простору[61].

Техніки верифікації та доведення походження медіа включають набір практичних методів цифрової форензики, які дозволяють встановлювати автентичність зображень, відео та інших цифрових об’єктів. Одним із ключових інструментів є аналіз метаданих, які містять інформацію про час, місце та пристрій створення контенту. Наприклад, програми на кшталт JPEGsnoop або Fotoforensics дозволяють виявляти сліди редагування, зміни формату або маніпуляції з файлами, що допомагає ідентифікувати підроблені матеріали. Крім того, для виявлення фальсифікацій використовують спеціалізовані інструменти, такі як Ghiro, який автоматично аналізує зображення та генерує звіти про можливі фальсифікації, зокрема через

порівняння візуальних артефактів або невідповідностей у структурі файлів[62].

Ланцюги постачання контенту відіграють важливу роль у забезпеченні прозорості та доведенні походження медіа. Сучасні протоколи передбачають фіксацію кожного етапу руху контенту - від створення до публікації, включаючи проміжні редагування, передачу прав та розповсюдження. Це дозволяє відстежувати історію файлу та виявляти спроби маніпуляції. Наприклад, у 2024-2025 роках все більшого поширення набувають технології блокчейну для верифікації походження цифрового контенту. Вони забезпечують незмінність записів про авторство, час створення та зміни, що робить практично неможливим підроблення або спотворення даних без виявлення[63].

Протоколи доказової фіксації медіа вимагають чіткого визначення критеріїв допустимості, порядку зберігання та автентифікації цифрових доказів. У юридичній практиці України та ЄС вже сформовано підходи до використання цифрових зображень, відеозаписів та публікацій у медіа як доказової бази, зокрема у справах про воєнні злочини або порушення авторських прав. Важливо, щоб такі докази відповідали стандартам неспростовності та могли бути перевірені незалежними експертами. Це передбачає не лише технічну фіксацію, а й документальне підтвердження ланцюга передачі даних, що забезпечує їхню юридичну силу.

У 2024-2025 роках операційні протоколи реагування на інформаційні загрози включають процедури блокування поширення дезінформації на ранніх етапах. Соціальні платформи, такі як Facebook, Twitter (нині X) та YouTube, використовують алгоритми для виявлення координованих кампаній з розповсюдження фейків. Після виявлення загроз платформи блокують підозрілі акаунти, обмежують видимість шкідливого контенту в рекомендаціях і додають попередження для користувачів. Координація з платформами здійснюється через центри моніторингу, які співпрацюють з

фактчекінговими організаціями та державними установами для оперативного реагування.

Інформаційні кампанії контр-впливу спрямовані на нейтралізацію дезінформації через поширення перевіреної інформації. В Україні Центр стратегічних комунікацій та інформаційної безпеки регулярно публікує аналітичні матеріали та інфографіку, які допомагають суспільству критично оцінювати інформацію та виявляти маніпуляції. Кампанії контрвпливу включають співпрацю з незалежними медіа, експертами та громадськими організаціями для створення контенту, який спростовує фейки та пояснює реальний стан речей. Також проводяться освітні ініціативи для підвищення медіаграмотності населення.

Плани підтримки мобілізаційної стійкості передбачають забезпечення безперебійної роботи критично важливих комунікаційних каналів під час криз. В Україні впроваджено систему резервних серверів та альтернативних каналів зв'язку (месенджери, децентралізовані мережі) для державних органів і медіа. Це дозволяє підтримувати комунікацію навіть за умов кібератак або блокувань основних платформ. Таким чином, операційні протоколи поєднують технічні, організаційні та комунікаційні заходи для мінімізації впливу дезінформації та забезпечення стійкості інформаційного простору.

У 2025 році європейські та національні стратегії дедалі більше акцентують на створенні єдиних «цифрових імунних систем» - інтегрованих платформ, що автоматично обмінюються індикаторами компрометації між державними центрами, платформами та незалежними фактчекерами. В Україні така архітектура реалізується через міжвідомчий хаб «Інформаційна стійкість», який у реальному часі отримує телеметрію від Meta, Google, Telegram та національних провайдерів, застосовує спільні правила класифікації загроз і розсилає сигнали швидкого реагування до всіх учасників мережі. Аналогічні рішення вже діють у країнах Балтії та Польщі в межах проєкту BALTDEFCOL Rapid Alert System 2.0.

Значного розвитку набуває практика превентивного «pre-bunking» - попереднього інформування населення про очікувані дезінформаційні наративи до їхнього масового запуску. Центр стратегічних комунікацій спільно з EUvsDisinfo та Atlantic Council DFRLab у 2025 році запустив пілотний проєкт, у рамках якого за 48–72 години до виявлення скоординованої кампанії в публічний доступ викладаються спрощені роз'яснення прийомів маніпуляції та ймовірних фальшивих тез. Дослідження ефективності цього підходу в Естонії та Фінляндії показало зниження рівня вірусного поширення таких наративів на 35–40 %[68].

Ще одним новим елементом стало впровадження обов'язкового «цифрового паспорту» для політичної та воєнної тематики: з 2025 року найбільші платформи в ЄС та Україні тестують механізм, за яким контент, що стосується національної безпеки, виборів чи збройного конфлікту, автоматично маркується рівнем довіри до джерела та історією поширення. Користувач бачить не лише попередження, а й графік походження матеріалу, що суттєво ускладнює ампліфікацію анонімних чи підроблених вкидів[69].

Ці інновації свідчать про перехід від фрагментарної модерації до проактивної архітектури інформаційної оборони, де дезінформація нейтралізується ще на стадії зародження, а не після досягнення критичної маси поширення. Подальший розвиток таких систем у 2026–2030 роках передбачатиме глибшу інтеграцію генеративно-змагальних мереж (GAN) для автоматичного створення контрнаративів, впровадження стандартів C2PA (Coalition for Content Provenance and Authenticity) на законодавчому рівні та розгортання децентралізованих мереж верифікації на базі blockchain нового покоління.

Для України ключовим завданням залишається завершення створення єдиної національної платформи «Цифровий щит», яка об'єднає всі наявні центри моніторингу, системи раннього попередження та pre-bunking-механізми в єдину операційну петлю з автоматичним прийняттям рішень на тактичному рівні. Лише за умови повної операційної сумісності з

європейською Rapid Alert System, НАТО StratCom COE та трансатлантичними партнерами ця архітектура забезпечить не локальне стримування, а стратегічне домінування в інформаційному просторі, перетворюючи потенційну вразливість цифрової епохи на стійку конкурентну перевагу демократичних суспільств.

2.3. Міжнародна співпраця протистояння інформаційній зброї в сучасних конфліктах

У 2024-2025 роках партнерство між державами, міжнародними організаціями та технологічними компаніями у сфері протидії дезінформації розвивається через різні формати співпраці. Одним з ключових напрямків є створення спільних лабораторій та центрів компетенцій. Наприклад, у березні 2025 року під час Київського міжнародного форуму кіберстійкості було підписано Меморандум про співпрацю між Європейським центром компетенцій у кібербезпеці та Національним координаційним центром кібербезпеки при РНБО України. Цей документ передбачає обмін досвідом, спільні дослідження та навчання фахівців для протидії гібридним загрозам, зокрема дезінформації.

Важливим елементом співпраці є обмін даними та координація дій між державами та технологічними компаніями. Ініціатива "Nations Against Disinformation", запущена Міністерством закордонних справ України, об’єднує країни та організації для спільних комунікаційних кампаній, тренінгів та обміну досвідом. У рамках цієї ініціативи партнери розробляють спільні стандарти протидії дезінформації та проводять міжнародні заходи для підвищення обізнаності суспільства про загрози, пов’язані з маніпуляціями в інформаційному просторі[64].

Меморандуми про взаємодію визначають зони відповідальності кожного учасника партнерства. Центр протидії дезінформації при РНБО України співпрацює з Консультативною місією Європейського Союзу,

проводячи тренінги для державних органів та розробляючи методичні матеріали з протидії дезінформації. Держава забезпечує нормативно-правову базу та координацію, міжнародні організації надають експертну підтримку та ресурси, а технологічні компанії впроваджують технічні рішення для виявлення та блокування шкідливого контенту.

У 2024-2025 роках програми підвищення цифрової грамотності та стійкості суспільства в Україні реалізуються через комплекс навчальних курсів, нормативів медіаосвіти та цільових кампаній для ключових груп населення. Міністерство цифрової трансформації України в рамках національної платформи "Дія.Цифрова освіта" запустило понад 70 освітніх серіалів з цифрової грамотності для різних категорій громадян: юристів, вчителів, медиків, журналістів, держслужбовців та школярів. Метою проєкту є навчання 6 мільйонів українців цифровій грамотності за три роки. Курси включають базові навички роботи з цифровими інструментами, безпеки в інтернеті та критичного сприйняття інформації, а також спеціалізовані модулі для професійних груп, таких як держслужбовці та журналісти[65].

Для військових та виборців проводяться окремі кампанії, спрямовані на підвищення стійкості до маніпуляцій та дезінформації. Наприклад, Центр стратегічних комунікацій та інформаційної безпеки регулярно організовує тренінги та розповсюджує методичні матеріали для військовослужбовців та виборців, щоб допомогти їм виявляти фейки та критично оцінювати інформацію. Також проводяться інформаційні кампанії в соціальних мережах та ЗМІ, які пояснюють механізми поширення дезінформації та навчають, як перевіряти джерела.

Освітні ініціативи включають співпрацю з міжнародними організаціями, такими як ЮНІСЕФ та Швейцарсько-українська програма EGAP, які підтримують розробку та впровадження навчальних програм. Національна рамка цифрової компетентності громадян, оновлена у 2025 році, визначає стандарти цифрової грамотності для різних вікових та професійних груп, а також планування регіональних ініціатив. Це дозволяє адаптувати програми

під потреби конкретних аудиторій, зокрема вчителів, студентів та представників критично важливих професій.

Таким чином, програми підвищення цифрової грамотності в Україні поєднують онлайн-курси, цільові кампанії та нормативні стандарти, спрямовані на формування стійкості суспільства до інформаційних загроз.

Критерії пріоритетності та оцінка здійсненності політик протидії дезінформації в Україні у 2024-2025 роках визначаються через матрицю ризик-користь, яка дозволяє оцінити потенційні загрози та ефективність запропонованих заходів. Центр протидії дезінформації при РНБО України використовує методику національної оцінки ризиків, яка передбачає аналіз ймовірності виникнення інформаційних загроз, їхнього впливу на суспільство та ресурсних можливостей для нейтралізації. Наприклад, у другій половині 2025 року Центр прогнозував активізацію кампаній з дискредитації України на міжнародній арені, зокрема через поширення наративів про "український тероризм" або нібито внутрішні суперечності серед союзників. Такі прогнози дозволяють визначати пріоритетні напрямки реагування та розподіляти ресурси для мінімізації ризиків.

Ресурсні оцінки включають аналіз фінансових, технічних та людських можливостей для впровадження політик. У 2024 році було затверджено Концепцію розвитку цифрових компетентностей до 2025 року, яка передбачає поетапне впровадження заходів з підвищення цифрової грамотності населення, включаючи навчання державних службовців, журналістів та виборців. Етапність реалізації визначається доступністю ресурсів та необхідністю поступового охоплення різних цільових груп. Наприклад, у 2024-2025 роках було проведено понад 200 тренінгів для державних службовців та представників ключових професій, що дозволило підвищити рівень обізнаності щодо загроз дезінформації та механізмів протидії.

Механізми моніторингу ефективності політик включають регулярну оцінку результатів через аналіз статистичних даних, зворотний зв’язок від учасників тренінгів та аналіз динаміки поширення дезінформації. Центр

протидії дезінформації та партнерські організації, такі як Інститут масової інформації та ГО "Детектор медіа", проводять моніторинг медіапростору та соціальних мереж, щоб оцінити ефективність інформаційних кампаній та навчальних програм. Наприклад, у 2024 році було зафіксовано зниження кількості поширених фейків серед учасників тренінгів на 30%, що свідчить про ефективність освітніх ініціатив.

У 2025 році міжнародна співпраця у протидії інформаційній зброї набула ще більш інституціоналізованого характеру, з акцентом на створення спільних операційних центрів та стандартизованих протоколів реагування. На Вашингтонському саміті НАТО у липні 2024 року, з продовженням у 2025 році, Альянс ухвалив Декларацію, що передбачає розвиток індивідуальних та колективних спроможностей для аналізу й нейтралізації ворожих дезінформаційних операцій. Це включає інтеграцію контрзаходів у щорічні вправи типу Cyber Coalition та Locked Shields. Ініціатива охоплює не лише європейських партнерів, а й розширюється на Індо-Тихоокеанський регіон через поглиблення взаємодії з IP4 (Австралія, Японія, Нова Зеландія, Південна Корея), де ключовим є обмін даними про гібридні загрози, включаючи дезінформацію, спрямовану на підрив колективної оборони.

Європейський Союз посилив координацію з НАТО через щорічні спільні прогрес-звіти, опубліковані в жовтні 2025 року, які фіксують понад 50 конкретних проєктів у сфері протидії FIMI (Foreign Information Manipulation and Interference), зокрема у підтримку України. У рамках G7 Rapid Response Mechanism та European External Action Service (EEAS) створено єдину платформу для оперативного обміну індикаторами компрометації, що дозволяє виявляти скоординовані кампанії на ранніх етапах. Для України це проявилося в інтеграції до Ukraine Defence Contact Group (UDCG), де ЄС та НАТО координують не лише військову допомогу, а й стратегічні комунікації, спрямовані на спростування наративів про «внутрішні суперечності союзників» чи «український тероризм», із прогнозованим бюджетом у 35 млрд євро на 2025 рік для кібер- та інформаційної стійкості.

Звіт Hybrid CoE «Countering disinformation in the Euro-Atlantic: Strengths and gaps» підкреслює сильні сторони регіональної співпраці, такі як обмін досвідом у виявленні бот-мереж та deepfake, але також зазначає прогалини: недостатнє фінансування (лише 60 % респондентів вважають ресурси адекватними) та брак механізмів для залучення неурядового сектору. Рекомендації звіту включають створення єдиного «Євро-Атлантичного центру демократичної стійкості» під егідою НАТО та ЄС, із фокусом на тренінги для журналістів і громадських активістів, що вже реалізується в пілотному форматі для країн Чорноморського регіону, зокрема України, Молдови та Грузії.

В контексті глобального партнерства ООН відіграє роль у формуванні універсальних норм через кампанії та Policy Brief on Information Integrity, які координуються з G7 та US State Department’s Global Engagement Center для моніторингу дезінформації у кризових ситуаціях, зокрема у війні в Україні. Для України це переросло в тристоронні протоколи з ЮНІСЕФ та EGAP, де освітні модулі з медіаграмотності адаптовані для школярів і біженців, охоплюючи понад 1 млн учасників у 2025 році[70]

Такі форми співпраці не лише посилюють оперативні спроможності, а й сприяють формуванню підходу, де держави, організації та приватний сектор об’єднуються для превентивного стримування інформаційних загроз. Емпіричні дані 2025 року свідчать про зниження ефективності російських кампаній на 25–30 % у регіонах із високим рівнем координації, що підтверджує необхідність подальшого розширення таких мереж для забезпечення глобальної стійкості в умовах ескалації гібридних конфліктів.

Висновки до розділу 2

Проведений у другому розділі аналіз сучасних підходів до протидії дезінформації в умовах глобальних викликів цифрового інформаційного простору свідчить, що ефективність контрдій визначається виключно

системністю та інтегративністю застосовуваних механізмів. Ізольоване використання окремих інструментів - правових, технічних чи освітніх - є недостатнім; лише їхнє комплексне поєднання в рамках єдиної стратегічної архітектури забезпечує досягнення стійкого ефекту.

Правове регулювання виступає фундаментальною складовою системи протидії. Сучасні міжнародні (Policy Brief ООН щодо інформаційної цілісності 2023, Кодекс практики ЄС щодо дезінформації 2022, Digital Services Act, Digital Markets Act) та національні нормативні акти мають встановлювати чіткі критерії відповідальності цифрових платформ, обов'язковість технічного маркування контенту, згенерованого штучним інтелектом, вимоги до прозорості рекомендаційних алгоритмів, а також пропорційні процедури вилучення шкідливого контенту при безумовному дотриманні принципів свободи вираження поглядів, права на приватність та доступу до інформації. Емпіричний досвід Естонії, Франції та України підтверджує, що найвища ефективність досягається за умов технологічно обґрунтованого, пропорційного та політично нейтрального регулювання.

Технічний компонент протидії демонструє швидку еволюцію у напрямку гібридних систем раннього виявлення та реагування, які інтегрують методи машинного навчання, аналізу великих даних, семантичного пошуку, графових баз знань та цифрової форензики. Такі системи дозволяють виявляти скоординовані інформаційні кампанії на превентивній стадії, автоматично класифікувати deepfake-матеріали, відстежувати бот-мережі та прогнозувати траєкторії вірусного поширення. Практична апробація цих рішень здійснюється в межах проєктів НАТО Strategic Communications Centre of Excellence, EUvsDisinfo, Atlantic Council Digital Forensic Research Lab та національних центрів моніторингу України, країн Балтії та Північної Європи.

Розвиток медіа- та цифрової грамотності визнано довгостроковим системоутворюючим фактором інформаційної стійкості. Дослідження підтверджують, що технічні фільтри не здатні повністю замінити когнітивний імунітет користувача. Тому державні та громадські програми,

диференційовані за цільовими групами (державні службовці, військовослужбовці, педагогічний склад, журналісти, вразливі вікові когорти), мають стати обов'язковою складовою національних стратегій. Українська платформа «Дія.Цифрова освіта», програми НАТО DEEP, естонська ініціатива «Digipööre» та французька система «Éducation aux médias et à l'information» ілюструють можливість досягнення масового охоплення за умови використання адаптивних цифрових форматів та регулярного оновлення навчальних модулів.

Міжнародна співпраця набуває якісно нового рівня інституціалізації. Спільні лабораторії з виявлення та атрибуції deepfake, оперативний обмін індикаторами компрометації, узгоджені процедури швидкого спростування, спільні кібернавчання та гармонізовані санкційні режими створюють ефект мережевого стримування та значно ускладнюють планування транснаціональних інформаційних операцій противником.

Оцінка пріоритетності та реалістичності політик протидії має ґрунтується на регулярному аналізі ризиків, моніторингу ключових показників ефективності та зворотному зв'язку від стейкхолдерів. Використання data-driven підходів, вже впроваджених Центром протидії дезінформації при РНБО України, естонським Propastop та литовськими ініціативами, дозволяє динамічно перерозподіляти ресурси та адаптувати заходи до еволюції тактик противника.

Лише послідовна імплементація такої багатошарової архітектури на національному та наднаціональному рівнях дозволить перетворити реактивну оборону на проактивну інформаційну стійкість. Ключовим викликом залишається забезпечення сталого фінансування, міжвідомчої координації та постійної адаптації до нових технологічних мутацій загроз (генеративний ШІ, децентралізовані платформи, нейромережні deepfakes).

В умовах, коли дезінформація дедалі частіше інтегрується в гібридні операції державних і недержавних акторів, відмова від системного підходу рівносильна добровільній втраті когнітивного контролю над власним

інформаційним простором. Тому пріоритетом для України та її союзників має стати прискорене розгортання національних центрів досконалості з протидії дезінформації, поглиблення трансатлантичної та європейської операційної сумісності й інституціалізація щорічного незалежного аудиту ефективності впроваджених заходів.

Тільки так можна забезпечити не тимчасове стримування, а стратегічну перевагу в інформаційній війні нового покоління.

РОЗДІЛ 3. РЕКОМЕНДАЦІЇ ЩОДО ПОСИЛЕННЯ МІЖНАРОДНОЇ БЕЗПЕКИ В ЦИФРОВУ ЕПОХУ

3.1. Вплив інформаційної зброї на динаміку конфліктів

Інформаційні операції змінюють поведінку людей і колективів через поєднання когнітивних, емоційних і поведінкових механізмів. Наративи формують смислові каркаси, що визначають уявлення про ворога, друзів та допустиму поведінку у кризових ситуаціях. Зміна домінуючого наративу може призвести до перегляду мотиваційних орієнтирів значної частини населення, оскільки повторювані повідомлення і механізм соціального доказу швидко закріплюють нові установки. Ефект доступності забезпечує легкість сприйняття певних сюжетів, що робить їх основою для подальших оцінок і рішень.

Для військових колективів інформаційні кампанії мають додатковий вплив на моральний стан і бойовий дух. Повідомлення, що дискредитують командування або ставлять під сумнів спроможність підрозділів, здатні знизити довіру та ініціативність у прийнятті рішень. Навіть поодинокі, але релевантні вкиди можуть призводити до самоорганізованих дій, зменшувати готовність до ризику та підривати дисципліну на нижчих рівнях.

Ехо-камери і замкнені інформаційні простори посилюють ефекти інформаційної дії, оскільки користувачі отримують узгоджений набір повідомлень, а контраргументи майже не досягають їхньої уваги. Це формує внутрішній консенсус, який швидко кристалізується і перетворює тимчасові оцінки на стійкі установки. Масовані кампанії короткочасного типу здатні викликати миттєві емоційні реакції, тоді як тривалі впливи поступово змінюють соціальні норми і стандарти поведінки, роблячи ефект більш стійким і важким для усунення[24].

Просторова координація інформаційних кампаній дозволяє адресувати їх як локально, впливаючи на конкретні спільноти чи підрозділи, так і на ширші регіони, створюючи мультиплікативний ефект. Поєднання часу і місця появи повідомлень з особливостями соціальної структури визначає швидкість

і масштаб наслідків. Емоційна складова інформаційної дії, орієнтована на активацію страху, гніву чи відрази, підвищує готовність до поведінкових реакцій і знижує критичність мислення.

Тактичні елементи сучасних операцій включають синхронізацію в часі, мультиканальну подачу та підсилення через координацію численних джерел інформації. Це створює відчуття консенсусу і прискорює соціальне поширення наративу. Для цивільного населення механізм впливу спрямований на послаблення суспільної довіри та соціальної солідарності, що ускладнює згуртовану реакцію на кризові події.

Оцінка ефекту інформаційної операції потребує поєднання кількісних показників - темпів поширення, охоплення і залученості - із якісними оцінками змін у поведінці та мотивації колективів. Лише такий підхід дозволяє відрізнити тимчасовий сплеск уваги від структурної зміни мотивацій і рішень, що формує стійкі соціальні і психологічні ефекти[24].

Після подій 2013-2014 років у Криму і на Донбасі російські інформаційні кампанії активно використовувалися для формування певних наративів серед місцевого населення і сил, що діяли на місцях. Комбінація оперативних месиджів, підроблених або вирваних із контексту відео та координація місцевих «лідерів думки» створювала відчуття неминучості змін і легітимності зовнішнього втручання, що в окремих випадках знижувало готовність захищати попередній порядок. Ця кампанія спиралася на поєднання традиційних і цифрових інструментів і мала на меті як формування підтримки серед цільових груп, так і деморалізацію опонента через сумніви в здатності центральної влади реагувати[25].

Приклад з діяльністю «Ісламської держави» (ІДІЛ/ISIS) ілюструє інший тип ефекту: через професійно збудований медіа-підхід і мережеві платформи угруповання змогло не лише вербувати іноземних бойовиків, а й впливати на мораль ворогів і місцевого населення, поширюючи образи невідворотності і безповоротності поразки супротивника. Відео і візуальні матеріали, що показували жорстокість та «успіхи» на полі бою, посилювали страх і

знижували бойову волю в окремих контекстах, одночасно підживлюючи підтримку серед симпатиків за межами театру воєнних дій. Масштаб і професіоналізм цієї пропаганди став предметом багатьох досліджень і вплинув на підходи до контрпропаганди[26].

Під час повномасштабного вторгнення 2022 року інформаційні дії також мали на меті підрив мобілізаційного потенціалу та деморалізацію громадян і військ. Окремі кампанії намагалися посіяти сумніви щодо ефективності оборони, висвітлюючи у гіперболізованому або фальсифікованому вигляді поразки, помилки логістики або нібито масові відмови від служби. Такі вкиди - у поєднанні з операціями з компрометації лідерів і підривом довіри до інститутів - мали на меті знизити готовність до тривалого опору і підірвати соціальну солідарність; водночас відчуття кризовості часто підсилювалося інформаційними «алібі» для технічних дій, що також впливало на сприйняття подій. Дослідження й аналітика останніх років фіксують ці практики та їхній вплив на наративи й мобілізацію[27].

Для ідентифікації реального впливу на мораль і поведінку досить показовим виявляється поєднання кількісних і якісних спостережень: з одного боку, зростання темпів поширення панічних або деморалізаційних повідомлень, збільшення охоплення та взаємодії; з іншого - зміни у публічному мовленні лідерів думок, зниження довіри до командування або інституцій, а також спостережувані зміни в поведінці підрозділів або громад (від ухилення від мобілізації до зростання числа відходів з фронту). Поєднання таких індикаторів дає змогу відрізнити одноразовий інформаційний сплеск від кампанії, що системно підриває моральні ресурси.

Інформаційно-психологічні операції з початку повномасштабного вторгнення Росії 2022 року стали ключовим інструментом впливу на суспільну думку та поведінку як цивільного населення, так і військових підрозділів. Основна мета цих операцій полягала у деморалізації, створенні сумнівів у спроможності держави організувати ефективну оборону та формуванні відчуття безвиході серед населення.

Для досягнення цих цілей використовувалися різні канали: масові соціальні мережі, месенджери, інтернет-ресурси, а також традиційні медіа, підконтрольні або лояльні агресору. Поширювалися матеріали, що перебільшували або спотворювали факти бойових дій, висвітлювали нібито поразки українських підрозділів, наголошували на проблемах із постачанням або нібито масових відмовах від служби. Такі вкиди мали на меті створити паніку, підвищити рівень тривожності і сформувати у цільових групах відчуття безпорадності[28].

Вплив ІПСО проявлявся і на моральному стані військових. Навмисно поширювані повідомлення про поразки, загибель або нібито масові дезертирства підривали довіру до командування, викликали сумніви у власних силах та змінювали поведінкові установки. У поєднанні з інформаційними ударами по ключових комунікаційних ланках це призводило до зниження готовності до активних дій, зменшення ініціативи та підвищення обережності навіть у підрозділах, що залишалися боєздатними.

Для цивільного населення операції мали соціально-психологічний ефект, спрямований на підрив єдності, ослаблення довіри до державних інститутів і створення відчуття хаосу. Масова циркуляція дезінформації формувала ехо-камери, де переважали негативні оцінки подій, посилюючи страх і тривогу. Такі повідомлення стимулювали самоцензуру, колективну нерішучість і утруднювали координацію допомоги та волонтерських ініціатив[29].

У цілому, інформаційно-психологічні операції стали важливим елементом гібридної стратегії агресора, де цифрові технології, соціальні мережі та контроль над наративами використовувалися для впливу на когнітивні та емоційні механізми, зниження бойового духу і соціальної згуртованості, створюючи довготривалі наслідки для здатності суспільства і армії реагувати на загрозу.

Використання штучного інтелекту та діпфейків значно посилило ефективність дезінформаційних кампаній, роблячи їх більш адресними,

масштабними та важкими для перевірки. Алгоритмічна персоналізація дозволяє аналізувати цифрову поведінку користувачів і пропонувати матеріали, які максимально відповідають їхнім переконанням і упередженням. Це підвищує емоційне залучення і вплив на рішення, оскільки користувач сприймає контент як релевантний і достовірний.

Генеративні технології, такі як діпфейки, створюють відео, аудіо або текст, що імітує реальних людей - політичних лідерів, експертів чи свідків подій. Такий контент виглядає переконливо, навіть якщо фактична подія або заява не відбувалися. У поєднанні з автоматизованими мережами, які охоплюють тисячі координованих акаунтів і ботів, це дозволяє швидко та широко поширювати матеріали, створюючи ілюзію масової підтримки або згоди з наративом[30].

Перевірка фактів у такому середовищі ускладнюється. Класичні методи, які базуються на прямому джерелі або документальних підтвердженнях, стають менш ефективними через високу правдоподібність згенерованого контенту. Діпфейки можуть вводити в оману навіть досвідчених фахівців, а автоматизоване поширення забезпечує швидкість розповсюдження матеріалів ще до їхньої перевірки. Це створює тривалі наслідки для громадської думки, морального стану і прийняття рішень у критичних ситуаціях.

Інформаційна зброя у цифрову епоху демонструє складний вплив на динаміку конфліктів, де психологічні, соціальні та технологічні аспекти взаємодіють у єдиній системі. Цілеспрямоване формування наративів і їх поширення через мережеві платформи не обмежується виключно деморалізацією окремих груп або військових підрозділів; цей процес змінює спосіб сприйняття подій, формує нові соціальні норми та впливає на прийняття рішень у ширшому масштабі. Повторювані повідомлення і систематичне використання психологічних механізмів, таких як ефект доступності та соціальний доказ, створюють когнітивні схеми, які визначають реакції цільових аудиторій і закріплюють певні поведінкові установки.

Вплив на мораль і бойовий дух військових підрозділів реалізується через систематичне підживлення сумнівів у компетентності командування, показ помилок або нібито масових відмов від служби, що знижує довіру до рішень та ініціативність у діях. У громадянському середовищі подібні кампанії послаблюють соціальну солідарність і здатність до колективного реагування, створюючи умови для панічних настроїв та нерішучості. Часові й просторові характеристики таких операцій дозволяють координувати поширення повідомлень локально та регіонально, збільшуючи масштаб впливу і формуючи мультиплікативний ефект, де кожна локальна реакція підсилює загальний наратив. Емоційна орієнтація повідомлень на страх, гнів чи тривогу підвищує готовність до імпульсивних реакцій, одночасно знижуючи критичність мислення та аналіз ситуації.

Особливе значення у сучасних конфліктах має використання штучного інтелекту та діпфейків, які дозволяють автоматизувати персоналізацію повідомлень і створювати генеративний контент, що виглядає достовірно, навіть якщо події або заяви не мали місця. Алгоритмічний підбір матеріалів під інтереси користувачів підсилює ефект залучення і впливу, а автоматизовані мережі ботів забезпечують швидке масштабування, створюючи ілюзію масової підтримки або згоди з наративом. У таких умовах перевірка фактів ускладнюється, адже діпфейки і координоване поширення інформації випереджають класичні методи верифікації, а громадська думка формується під впливом правдоподібного, але фальсифікованого контенту.

Використання цих технологій під час повномасштабного вторгнення Росії в Україну 2022 року демонструє їхню ефективність і комплексність. Цифрові платформи дозволяли одночасно впливати на громадянське населення і військові підрозділи, поширюючи інформацію про нібито поразки, проблеми з постачанням і масові відмови від служби, створюючи атмосферу безвиході та деморалізації. Синхронізація часу публікацій, мультиканальна подача та координація численних джерел створювали відчуття масштабності подій і підтримки з боку широких мас, що додатково підсилювало ефект

страху та тривоги. Результатом став не тільки зниження бойового духу, а й тимчасова дезорганізація мобілізаційного потенціалу і соціальної солідарності, що вимагало активних контрзаходів з боку державних інституцій і військового керівництва.

Крім деморалізаційного ефекту, інформаційно-психологічні операції впливали на поведінкові патерни через формування очікувань щодо подій та сприйняття дій влади. Масова циркуляція негативних або перебільшених повідомлень змінювала ставлення до рішень державних органів, стимулювала самоцензуру та колективну нерішучість, ускладнювала координацію волонтерських і допоміжних ініціатив. У цьому контексті цифрові технології дозволяли здійснювати багаторівневий контроль над наративами, поєднуючи психологічний ефект, технологічний масштаб і соціальне охоплення[31].

Таким чином, інформаційна зброя у цифрову епоху стала не лише інструментом формування уявлень про реальність, а й комплексним механізмом зміни поведінки, мотивації та морального стану як цивільного населення, так і військових підрозділів. Поєднання технологій персоналізації, генеративних матеріалів і автоматизованих мереж дозволяє створювати стійкі когнітивні ефекти, що складно нейтралізувати класичними методами перевірки фактів, водночас значно підвищуючи вплив на динаміку конфліктів і соціальні процеси в зоні бойових дій.

Важливим аспектом впливу інформаційної зброї на динаміку конфліктів є інтеграція інформаційних і кібернетичних операцій, де цифрові атаки доповнюють психологічний вплив, створюючи системний тиск на цільові аудиторії. Комбінування дезінформації з кібератаками на комунікаційну інфраструктуру, електронні сервіси та критичні системи логістики дозволяє не лише дестабілізувати мораль і поведінку, а й безпосередньо впливати на оперативні можливості військ і державних органів. Цей підхід формує новий тип мультиканального конфлікту, де інформаційний, психологічний і технічний вплив тісно переплітаються, а традиційні межі між бойовими діями та медіа-простором стають розмитими.

Створення так званих "інформаційних хвиль", коли серії повідомлень насичують простір у конкретний проміжок часу, дозволяє досягати піку емоційної реакції аудиторії. Подібні хвилі створюють ефект перенасичення, що ускладнює сприйняття альтернативної інформації та змушує цільові групи реагувати імпульсивно. Водночас, контроль над темпом і послідовністю подачі матеріалів забезпечує підтримку тривалих наративів, які поступово перетворюють короткострокові панічні реакції на стійкі установки, здатні впливати на стратегічні рішення.

Використання аналітичних методів дозволяє виділяти групи з різними психологічними, соціальними та демографічними характеристиками, що дає змогу коригувати повідомлення під специфіку їхніх установок і емоційних тригерів. Такий підхід збільшує ефективність кампаній і водночас ускладнює протидію, оскільки універсальні стратегії реагування стають менш результативними. При цьому увага приділяється не лише безпосередньо активним учасникам конфлікту, а й потенційним симпатикам або нейтральним групам, здатним у разі зміни наративу впливати на колективні дії[32].

Соціальні мережі та месенджери використовуються не лише як канали поширення повідомлень, а й як інструменти збору інформації про поведінку цільових груп. Аналіз цифрових слідів, взаємодій та інтересів дозволяє коригувати тактику, визначати слабкі місця у сприйнятті аудиторії і прогнозувати реакції на конкретні повідомлення. Така інтеграція аналітики і практичного впливу забезпечує гнучкість кампаній і дозволяє швидко адаптуватися до зміни обстановки, збільшуючи темпи та точність інформаційного впливу.

Особливе значення набуває використання символічних та культурних кодів у повідомленнях. Включення релігійних, історичних чи соціальних мотивів дозволяє створювати сильні емоційні зв’язки, що підсилюють когнітивний ефект і формують глибше сприйняття наративу. Подібні маніпуляції часто спрямовані на викликання почуття несправедливості, образи

або загрози, що значно підвищує готовність цільової аудиторії до поведінкових змін і підсилює психологічний вплив.

Також слід виділити роль непрямого впливу через посередників, включно з лідерами думок, блогерами та локальними активістами, які беруть участь у поширенні наративів. Використання таких посередників підвищує легітимність повідомлень і створює ефект "органічного" поширення, коли інформація сприймається як природна і достовірна, що посилює її вплив на когнітивні установки та соціальну поведінку.

Нарешті, інформаційні кампанії часто інтегруються із заходами психологічної дезорганізації, спрямованими на зниження здатності до критичного мислення та стратегічного планування. Маніпулювання інформаційними потоками, контроль за достовірністю даних і формування постійного відчуття невизначеності змушує аудиторії приймати рішення під тиском емоцій, а не логіки. Це особливо критично у військових контекстах, де швидкість і точність рішень безпосередньо впливають на результат операцій.

Таке комплексне поєднання психологічного, соціального та технологічного впливу свідчить про те, що сучасні конфлікти вже не обмежуються традиційними бойовими діями і що інформаційна зброя стає системним чинником, здатним формувати стратегічну динаміку подій, змінювати баланс сил та впливати на прийняття рішень на різних рівнях - від індивідуального до державного.

У сучасних конфліктах інформаційна зброя дедалі частіше виконує функцію «когнітивного прискорювача», що не лише підсилює ефекти фізичних дій, а й самостійно визначає траєкторію ескалації чи деескалації. Ключовим механізмом тут є створення «асинхронії сприйняття»: коли одна сторона оперує в реальному часі бойових дій, інша вже формує постфактумне тлумачення подій, яке визначає подальшу реакцію не лише цивільної аудиторії, а й міжнародних акторів. Таким чином, перемога чи поразка на інформаційному фронті може передувати і навіть заміщати результат на полі бою.

Особливо небезпечним є явище «когнітивного захоплення», коли тривала експозиція скоординованих наративів призводить до інтерналізації зовнішнього дискурсу як власної позиції цільової спільноти. У таких умовах частина населення або навіть військових починає діяти в інтересах агресора, не усвідомлюючи цього, інтерпретуючи власні дії як захист «справедливості», «традиційних цінностей» чи «миру». Емпіричні дані з конфлікту в Україні 2022–2025 років показують, що в окремих прифронтових регіонах до 18–22 % респондентів частково або повністю приймали російські тлумачення подій, навіть попри безпосередній досвід окупації.

Цифрові платформи та генеративний ШІ дозволяють реалізовувати так звану «стратегію тисяч ножових поранень»: замість однієї масованої кампанії запускаються тисячі мікронаративів, кожен з яких розрахований на вузьку аудиторію. Кожен мікронаратив має низький поріг виявлення модерацією, але в сумі формує стійке поле недовіри та розколу. Алгоритми рекомендацій самі підхоплюють і масштабують ці мікросигнали, перетворюючи їх на домінуючий дискурс без видимого централізованого керування.

Таким чином, вплив інформаційної зброї на динаміку конфліктів виходить за межі тимчасової деморалізації чи мобілізації: вона здатна до довготривалої реконструкції колективної ідентичності, перерозподілу лояльностей і створення внутрішніх розколів, які зберігають дестабілізаційний потенціал роками після завершення активної фази бойових дій. У цьому сенсі сучасний конфлікт вже не закінчується підписанням перемир’я - він переходить у фазу перманентної когнітивної війни, де головним полем битви стає не територія, а структура свідомості та соціальної пам’яті протиборчих суспільств.

3.2. Механізми застосування інформаційної зброї на системи безпеки

Операційна реалізація інформаційної зброї в цифровому середовищі ґрунтується на поєднанні кількох взаємопов'язаних каналів, тактик і технічних засобів, що дає змогу проводити цілеспрямовані кампанії з високою швидкістю та прихованою координацією; у базовому сценарії операція починається зі стадії підготовки - збір даних про цільові групи та аналіз цифрових звичок, формування кількох версій наративу і вибір каналів поширення, далі слідує стадія «посіву» контенту через комбінацію органічних публікацій, платного просування і залучення локальних або міжнародних посередників, після чого запускається етап ампліфікації, коли повідомлення підсилюється скоординованою активністю численних акаунтів, ботів та мереж лідерів думок; платформи соціальних мереж, публічні канали месенджерів, спеціалізовані форуми та блоги використовуються як інфраструктура, причому алгоритми ранжування стають інструментом автоматичної селекції найрезонанснішого матеріалу, а генеративні засоби створення тексту, аудіо й відео - ресурсом для швидкої підготовки правдоподібних доказів чи «свідчень»[33].

Тактичні деталі включають A/B-тестування варіантів повідомлень на контрольних сегментах, синхронізацію появи контенту у вигідних часових вікнах, застосування візуальних шаблонів і меметичних форм, що підвищують вірогідність репосту, а також використання комбінованих облікових записів - реальних, напівреальних (керованих людьми з технічною підтримкою) і повністю автоматизованих - для створення ілюзії органічної дискусії; генеративний контент дозволяє підкладати голоси, імітувати заяви посадовців або змонтувати «очевидні» кадри, які в разі швидкого поширення формують фактичну площину дискусії навіть до моменту верифікації[34].

Маскування походження досягається багаторівнево: використанням проксі-сервісів і VPN для приховування технічних слідів, створенням ланцюгів рекомендацій через «підкладні» сайти і сторінки, застосуванням тактики «астротрафінгу» (імітації спонтанної громадської підтримки) через

платні мережі та координацію місцевих агентів, а також розподілом ролей між проксі-акторами, що ускладнює просте ідентифікування ініціатора кампанії. Вразливості системи безпеки при цьому випливають із конструктивних особливостей цифрових платформ: алгоритми, що пріоритизують залученість, підсилюють емоційно забарвлений контент; широке збирання персональних даних дає змогу робити глибоке сегментування аудиторій; відкрите програмне забезпечення та реклама відкривають простір для масованого таргетування; повільна або фрагментована модерація та правові обмеження у транскордонній площині залишають «вікна» для тривалого розгортання кампаній[35].

Для практичної оцінки ризиків і виявлення цих загроз застосовують набір інструментів і методик, що поєднують мережевий аналіз із контент-форензикою й оперативним моніторингом: побудова графів взаємодій і обчислення центральності вузлів дозволяє виявити хаби впливу і «мости» між спільнотами; виявлення аномалій у часових рядах взаємодій показує штучні хвилі активності; кластеризація повідомлень за семантикою та тональністю виявляє повторювані шаблони і координовані зміни повідомлень; метрики швидкості поширення, коефіцієнта репостів та співвідношення органічних і платних взаємодій слугують індикаторами інтенсивності кампанії; технічна експертиза з аналізу метаданих, ознак компресії та слідів генерації матеріалу дає змогу розпізнати підроблені медіафайли, тоді як інструменти відстеження походження контенту і перевірки посилань допомагають простежити ланцюги поставки інформації[36].

Практичні інструменти оцінки ризику включають створення систем раннього попередження, що фіксують появу хвиль із високою залученістю у вразливих регіонах, набори критеріїв для класифікації загроз за організацією, тривалістю і потенційною шкодою, а також чеклісти для швидкої ідентифікації: наявність однотипних повідомлень від різних акаунтів у короткий проміжок часу, непропорційно високий обсяг репостів від недавно

створених профілів, співпадіння месседжів із відомими наративами дезінформації, часті появи відео чи аудіо без очевидних первинних джерел.

Важливим практичним підходом є комбінування автоматизованої аналітики з експертною оцінкою: алгоритмічні системи дозволяють відслідковувати великі обсяги даних і виділяти аномалії, а людський аналіз дає контекст і перевіряє етичні та політичні наслідки виявлених кампаній. Оцінка ризику повинна враховувати не лише технічні показники, а й потенційний вплив на функціонування критичної інфраструктури, мобілізаційні можливості та довіру до інституцій; це вимагає мультидисциплінарних команд, здатних інтегрувати соціологічні опитування, оперативні дані від служб безпеки та аналітику платформ для формування оперативних рекомендацій щодо реагування.

Крім технічних аспектів розгортання кампаній, значною вразливістю є економічні і регуляторні умови, у яких функціонують цифрові платформи; рекламні системи та інструменти промоції створюють ринкові стимули для масштабного таргетування, а відсутність однакових правил у різних юрисдикціях дає змогу акторам обходити національні обмеження і вести координацію через посередницькі структури. У результаті оператори можуть швидко переводити кампанію з одного каналу в інший, використовувати платний просувний контент як «легальний» засіб підживлення наративу та застосовувати складні фінансові схеми для приховування джерел підтримки. Паралельно технічні обмеження модерації - обмежений людський ресурс, політична чутливість і ризики цензури - створюють вікна для тривалого функціонування дезінформаційних мереж; це особливо помітно у випадках, коли мова йде про швидко змінні вкиди, що комбінують правдиві фрагменти з вигаданими твердженнями, ускладнюючи процедури видалення та перевірки[37].

Уразливість також має організаційний вимір: державні і приватні інституції часто не готові до інтегрованої оцінки ризику, бо кожен сектор оперує власними метриками і каналами збору інформації. Служби безпеки

фокусуються на технічних індикаторах, медіа - на контенті, а громадянське суспільство - на реакції аудиторії; відсутність оперативного обміну та стандартизованих протоколів ускладнює швидку і скоординовану відповідь. Така фрагментація дає простір для експлуатації: координована кампанія, що одночасно використовує технічні вразливості платформ, інформаційні розриви у медійному полі та соціальні напруження, здатна досягти ефекту, який значно перевищує сумарні можливості окремих компонентів захисту.

Детекція й оцінка ризику стикаються з проблемою адаптивності супротивника: алгоритми й методики, що виявляють певні патерни, швидко стають відомими і змушують операторів змінювати тактику - від розподілу вкидів у часі до використання більш витончених комбінацій реальних і фальсифікованих джерел. Це породжує циклічну гонку «за ознаками»: системи навчаться виявляти одні шаблони і водночас дають змогу виникати новим, менш помітним. У такому середовищі критичною є здатність аналітичних систем не тільки фіксувати аномалії, а й оцінювати значущість цих аномалій для стійкості інституцій і мобілізаційного потенціалу, тобто співвідносити технічні сигнали з соціальними індикаторами, які свідчать про реальні зміни в поведінці чи довірі[38].

Підвищення стійкості вимагає комплексних підходів, що поєднують технічні інновації та організаційні зміни: підвищення прозорості рекламних механік платформ, розвиток міжсекторальних протоколів обміну інформацією, стандарти для перевірки походження медіа та інвестиції в цифрову грамотність населення. Однак кожна з цих ініціатив стикається з компромісом між оперативністю реагування і правами громадян, між цензурою й захистом інформаційного простору, а також із необхідністю міжнародної координації в умовах різних правових режимів. Ця множинність обмежень і ризиків робить практичну роботу з протидії інформаційним кампаніям складною і вимагає постійного оновлення методів моніторингу, верифікації й оцінки впливу.

Завершальна частина операційного обґрунтування вимагає зосередитися на практичних механізмах стримування і на тих технічно-організаційних змінах, які можуть скоротити вікна вразливості. По суті, йдеться про три взаємопов'язані напрями роботи: підвищення прозорості інструментів просування контенту на платформах, побудова оперативних каналів обміну даними між державними структурами, медіа та технологічними компаніями, а також впровадження інструментів швидкої технічної верифікації медіаматеріалів. Прозорість рекламних механік і відкритість даних про платні кампанії знижують можливості для прихованого підживлення наративів, оперативний обмін інформацією дозволяє синхронізувати відповідь і блокувати ампліфікацію на ранніх етапах, а технічні методи - від аналізу метаданих до доказової форензіки відео й аудіо - зменшують ефективність підробок. Разом ці заходи знижують ймовірність того, що одиничні вкиди переростуть у системну кампанію з масштабними політичними або соціальними наслідками[39]

Водночас будь-яка програма захисту мусить враховувати компроміси і ризики: активні заходи модерації та фільтрації контенту легко перетворюються на інструмент цензури за відсутності чітких процедур і правових гарантій, а централізація реагування без залучення громадянського суспільства підриває довіру до ініціатив із протидії дезінформації. Тому ефективна стратегія поєднує технічні рішення з інституційними гарантіями прозорості й підзвітності - публічні протоколи розслідувань, незалежні огляди рішень щодо втручань у мережі, стандарти для аудиту алгоритмів ранжування. Паралельно необхідно інвестувати в підвищення цифрової грамотності й критичного сприйняття інформації серед громадян, бо жодна технічна система не замінить суспільного імунітету, який зменшує корисність маніпуляцій навіть при наявності їхньої технічної досконалості[40].

На завершення операційно-методологічної частини слід підкреслити, що робота з вразливостями - це постійний процес адаптації. Актори, що проводять кампанії, швидко змінюють тактики у відповідь на виявлені протидії, отже

захисні механізми мусять поєднувати автоматизоване виявлення аномалій з експертною інтерпретацією, регулярними оновленнями процедур та вправними міжсекторальними практиками. Це означає створення гібридних команд, які об’єднують технічних фахівців, соціальних аналітиків, правників і представників громадянського сектору, здатних не лише фіксувати атаки, а й оперативно реагувати на них із врахуванням прав людини та політичного контексту. Такий підхід підвищує шанси розірвати ланцюг ампліфікації на ранньому етапі й зменшити шкоду від інформаційних кампаній на стійкість суспільства та безпеку.

Моделювання кризових ситуацій дозволяє виявити слабкі місця не лише в технічних інструментах, а й у процедурах ухвалення рішень, потоках інформації між відомствами та механізмах публічної комунікації. Такі вправи повинні включати імітацію швидкого розповсюдження фейків із різними рівнями правдоподібності, тестування каналів оповіщення населення, а також відпрацювання юридичних процедур і публічних роз’яснень, щоб у реальній кризі не виникало хаосу через невизначеність повноважень або надто повільну координацію. Регулярні червоні команди, що моделюють дії супротивника, допомагають оновлювати сигнатури для виявлення, оцінювати ефективність фільтрів і виробляти адаптивні протоколи реагування, мінімізуючи ризик формалізованої «перешколення» захисних систем під старі патерни атак.

Не менш важливим є розвиток інституційних механізмів прозорої відповідальності платформ і рекламних мереж. Відкриті реєстри платних кампаній, стандартизовані формати розкриття джерел фінансування й API для аналітиків створять технологічну основу для швидшої верифікації і меншої залежності від приватних каналів доступу. Поряд із цим доцільно впроваджувати сертифікацію інструментів для верифікації медіа й методик цифрової форензики, яка б гарантувала мінімальні технічні стандарти доказовості й дозволяла б державним та незалежним організаціям користуватися результатами експертиз у судових і публічних процесах. Такі сертифікати повинні створюватися на основі відкритих методологій, підлягати

періодичному аудиту й бути доступними для міжнародного визнання, що знизить ймовірність зловживань і підвищить довіру до технічних висновків[41].

У правовій площині необхідна робота над гармонізацією підходів до визначення відповідальності за організацію транснаціональних інформаційних операцій, механізмів міжнародної кооперації у сфері розслідувань і стандартів для атрибуції. Водночас законодавчі ініціативи мають враховувати ризики надмірного обмеження свободи слова і забезпечувати процедури оскарження рішень про блокування чи маркування контенту. Нормотворча робота повинна йти в парі з розвитком незалежних наглядових механізмів, до яких включені експерти від громадянського суспільства, наукових інституцій та медіа, щоб забезпечити баланс між ефективністю реагування і захистом прав людини.

Технологічні інвестиції мають бути спрямовані не лише на детекцію, але й на підвищення стійкості комунікаційної інфраструктури. Резервні канали зв’язку, децентралізовані мережеві рішення, криптографічні підписи для критичних повідомлень владних інституцій та стандарти для автентифікації журналістських матеріалів можуть зробити суспільну дискусію менш уразливою до штучних втручань. Окремо треба підтримувати дослідження в галузі виявлення глибоких підробок, інструментів слідування за ланцюгами розповсюдження інформації і методів пояснюваності рішень автоматичних систем - це допоможе уникнути "чорних скриньок" у процесі моделювання і зростить довіру до технічних висновків.

Критичною складовою є інвестування в людський капітал: підготовка аналітиків, журналістів, працівників державних установ і представників громадянського суспільства до роботи з новими загрозами. Освітні програми мають поєднувати технічні знання з розумінням соціальних маніпуляцій, етики та права; громадська освітня кампанія - підвищувати інформаційну гігієну населення, навчати елементарним навичкам верифікації джерел і скептичного мислення. Така мультиплікація знань зменшує ефективність

маніпулятивних технологій і формує стійкіші локальні мережі критичного сприйняття[42].

Не можна нехтувати економічними важелями: механізми стимулювання платформ до самовдосконалення, включаючи податкові або нормативні стимули за впровадження прозорих систем звітності і швидкого видалення штучно підсилюваного шкідливого контенту, а також санкції для структур, що системно підтримують транснаціональні дезінформаційні мережі, можуть змінити економічні підходи до моделі монетизації контенту. Паралельно варто розвивати моделі фінансування незалежної експертизи та громадських ініціатив, які можуть виконувати функцію раннього попередження й незалежного контролю.

Нарешті, важливо формувати довгострокові метрики стійкості суспільства, які виходять за межі технічних індикаторів і враховують рівні довіри до інституцій, якість місцевих медіа, ступінь соціальної інтеграції й наявність каналів зворотного зв’язку. Оцінювання втручань має корелювати технічні показники з соціологічними даними, щоб вимірювати не тільки факт розповсюдження контенту, а й його реальний вплив на поведінку й політичні настрої. Такий підхід дозволить цілеспрямовано інвестувати в ті напрямки захисту, які реально підвищують суспільний імунітет, а не тільки закривають окремі технічні вразливості. У сукупності ці додаткові заходи створюють більш адаптивну, прозору і відповідаючу правам людини систему, здатну знижувати ризики інформаційних операцій і підвищувати загальну стійкість демократичних процесів.

3.3 Напрямки посилення безпеки щодо впливу інформаційної зброї

Захист інформаційного простору на міжнародному рівні передбачає поєднання превентивних і коригувальних заходів, які реалізуються через наявні інституційні структури. Організації, такі як Організація Об’єднаних Націй та Північноатлантичний Альянс, протягом останніх років формують

практики раннього попередження і координації дій між державами, встановлюють стандарти реагування на інформаційні загрози та визначають методики оцінки їхнього впливу на соціальні та політичні процеси. Ці механізми дозволяють виявляти ризики на ранньому етапі та забезпечувати скоординовану відповідь, підвищуючи здатність держав і міжнародних організацій швидко реагувати на загрози.

Ключовим аспектом сучасної протидії є співпраця держав з технологічними компаніями, що контролюють платформи поширення інформації. Така взаємодія включає обмін даними про підозрілу активність, технічну підтримку для перевірки достовірності матеріалів і прозорість алгоритмів рекомендацій та ранжування контенту. Спільна робота дозволяє оцінювати ризики, пов’язані з автоматизованим поширенням матеріалів, виявляти координовані мережі та своєчасно реагувати на масові кампанії дезінформації, не порушуючи прав користувачів[43].

Практичні інструменти включають тестування систем виявлення бот-мереж, аналіз згенерованих матеріалів та інтегровані методики моніторингу національних інформаційних просторів. Це дозволяє зменшити час між появою загрози і її нейтралізацією, а також підвищити довіру громадськості до дій державних і приватних інституцій. Оцінка ефективності таких заходів здійснюється через поєднання кількісних і якісних показників, зокрема швидкість поширення потенційно шкідливого контенту, охоплення аудиторії та зміни в поведінці користувачів.

На рівні національної політики важливим елементом є формування комплексних стратегій, що поєднують юридичні, технічні та освітні заходи. Юридичні ініціативи визначають відповідальність за поширення дезінформації та встановлюють процедури для перевірки фактів. Технічні засоби охоплюють аналіз поведінки акаунтів, цифрову експертизу зображень і відео, а також національні системи моніторингу інформаційного простору. Освітні програми підвищують цифрову грамотність населення та сприяють

розвитку критичного мислення, що дозволяє ефективніше протидіяти маніпуляціям[44].

Етичні норми та координація забезпечують баланс між безпекою, свободою слова та правами людини. Вони визначають пріоритетність заходів у рамках національних і міжнародних стратегій та забезпечують узгодженість дій різних суб'єктів. Такий підхід дозволяє створити системну основу для протидії інформаційним загрозам і підвищити готовність суспільства та державних інституцій до сучасних викликів безпеки.

Впровадження конкретних політичних і оперативних заходів передбачає комплексний підхід, де різні інструменти взаємодіють між собою для максимального ефекту. На національному рівні доцільним є створення спеціалізованих підрозділів у межах державних органів, які відповідають за виявлення, аналіз та нейтралізацію інформаційних загроз. Такі підрозділи можуть координувати дії з правоохоронними органами, службами безпеки та медіа, здійснювати моніторинг цифрового середовища та проводити оцінку впливу кампаній на соціальну поведінку населення. Це дозволяє своєчасно реагувати на загрози, мінімізуючи шкоду та обмежуючи можливості для дестабілізації[45].

На міжнародному рівні важливо налагоджувати механізми обміну даними та координації між державами. Створення спільних баз даних про шкідливий контент, обмін інформацією про відомі бот-мережі та інші механізми масового впливу дозволяє виявляти системні загрози і оперативно розробляти контрзаходи. Крім того, спільні навчальні програми та обмін досвідом підвищують готовність державних структур до реагування на нові форми інформаційного впливу, що постійно еволюціонують у цифровому середовищі.

Технічні аспекти співпраці з технологічними компаніями включають не лише виявлення загроз, а й створення алгоритмів раннього попередження. Це може передбачати автоматизоване сканування соціальних мереж і платформ на предмет появи масових кампаній дезінформації, оцінку потенційного

впливу на аудиторію та виявлення аномалій у поведінці акаунтів. Підтримка прозорості алгоритмів, їх аудиту та незалежної оцінки результатів допомагає знизити ризики маніпуляції, а також забезпечує довіру до застосованих методів контролю.

Крім технічних і організаційних заходів, ефективним є підвищення цифрової грамотності населення. Програми навчання, спрямовані на розвиток критичного мислення та розпізнавання маніпуляцій, формують стійкість громадян до інформаційних впливів. Розуміння логіки поширення дезінформації, можливостей алгоритмічної персоналізації та діпфейків дозволяє громадянам оцінювати достовірність отриманих повідомлень і приймати обґрунтовані рішеннях[46].

Узгоджене поєднання політичних, технічних та освітніх заходів забезпечує комплексну систему протидії інформаційним загрозам. Це дозволяє державам і міжнародним організаціям не лише реагувати на наявні виклики, а й прогнозувати потенційні загрози, підвищуючи загальний рівень безпеки інформаційного простору та стійкість суспільства до маніпуляцій.

Окрему увагу приділяють формуванню нормативної та етичної бази для реагування на інформаційні загрози. Розробка міжнародних стандартів і керівних принципів визначає допустимі межі контролю за контентом, балансуючи між безпекою і правами громадян. Ці норми враховують швидкість еволюції цифрових технологій, здатність платформ поширювати маніпулятивні матеріали і потенційні наслідки для свободи вираження. Прозорі та узгоджені правила зменшують конфлікти між державами через різне тлумачення законодавства та політики в сфері інформаційної безпеки.

Побудова мультистейкхолдної системи взаємодії об’єднує державні органи, міжнародні інституції, технологічні компанії, наукові кола та громадські організації. Така структура дозволяє оперативно виявляти нові загрози, оцінювати їхню потенційну шкоду та координувати дії щодо нейтралізації. Включення громадськості у формування інформаційної стратегії підвищує довіру до прийнятих рішень і створює додатковий рівень

раннього попередження, оскільки широке коло учасників здатне помітити аномалії та сповіщати про них у короткі терміни[47].

Оцінка ефективності застосованих заходів використовує якісні методи аналізу - дослідження змін у поведінці і настроях населення, опитування та аналіз медіа-простору, - і кількісні показники, що відображають охоплення, темпи поширення та залученість аудиторії. Поєднання цих методів дозволяє коригувати стратегії реагування, адаптуючи їх до нових викликів і зменшуючи ризик тривалого впливу дезінформаційних кампаній.

Зростає потреба у постійному розвитку інструментів моделювання та прогнозування загроз. Аналітичні платформи, що інтегрують великі обсяги даних, створюють сценарії поширення дезінформації, оцінюють потенційний вплив на різні групи населення та військові підрозділи, а також перевіряють ефективність протидійних заходів ще до їхнього впровадження. Такий підхід підвищує здатність держав і міжнародних організацій до стратегічного планування та зменшує ймовірність несподіваних наслідків від інформаційних атак.

У подальшому розвитку системи захисту головне - не роздувати нові структури, а зробити так, щоб уже наявні механізми працювали швидше й узгодженіше. Національні стратегії протидії дезінформації потрібно регулярно переглядати й доповнювати з урахуванням того, як змінюються можливості платформ і тактика тих, хто запускає інформаційні кампанії. Це означає, по-перше, чіткіше пов’язати між собою відомства, які займаються інформаційною безпекою, кіберзахистом і стратегічними комунікаціями, щоб рішення приймалися в одному кабінеті, а не перекидалися паперами тижнями.

Дуже допомагає тісніша робота з незалежними фактчекерами й журналістами-розслідувачами. Досвід останніх двох років показує: коли держава просто передає їм первинний сигнал про підозрілу хвилю, а вони вже публічно розбирають і спростовують - це і швидше, і суспільство сприймає без підозри в цензурі.

Не менш важливо продовжувати просвітницьку роботу. Короткі курси з перевірки джерел, розпізнавання маніпуляцій і розуміння, як працюють алгоритми рекомендацій, дають відчутний ефект - люди стають значно стійкішими до вкидів. Особливо це помітно серед школярів, студентів і державних службовців, для яких такі заняття вже поступово роблять обов'язковими.

Тобто основний шлях посилення безпеки – не вигадувати щось революційне, а довести до ладу те, що вже є: злагоджену міжвідомчу роботу, оперативний обмін даними з платформами, підтримку незалежного фактчекінгу й системну освіту. Саме таке поєднання дозволяє поступово знижувати ефективність інформаційних атак, не вдаючись до жорстких обмежень і зберігаючи довіру громадян.

Висновки до розділу 3

На основі проведеного аналізу рекомендується розглядати посилення міжнародної безпеки в цифрову епоху як єдину багатошарову систему, в якій правові, технічні, освітні та інституційні заходи працюють синхронно й постійно адаптуються до еволюції загроз.

Для забезпечення ефективного захисту необхідно прискорити гармонізацію національного законодавства з європейськими стандартами, запровадити обов'язкове криптографічне маркування всього ШІ-генерованого контенту, вимагати від великих платформ повної прозорості рекомендаційних алгоритмів та незалежного аудиту, водночас передбачивши чіткі, швидкі та публічні процедури оскарження рішень про видалення чи маркування контенту, аби зберегти баланс між безпекою та свободою вираження поглядів.

Технічний захист слід будувати навколо гібридних систем раннього виявлення, що поєднують штучний інтелект, цифрову форензику, аналіз метаданих та мережевий моніторинг, а також створювати національні й наднаціональні центри оперативного реагування за успішними моделями

України, Естонії та НАТО StratCom COE. Одночасно рекомендується інвестувати в регулярні міжвідомчі навчання, червоні команди та моделювання інформаційних криз із залученням технологічних компаній і громадянського суспільства, аби постійно оновлювати протоколи реагування.

Особливу увагу необхідно приділяти масштабуванню програм цифрової та медійної грамотності для всіх верств населення, включно з обов'язковими модулями з розпізнавання deepfake та алгоритмічного маніпулювання для державних службовців, військовослужбовців і журналістів, використовуючи вже апробовану платформу «Дія.Цифрова освіта» як базову модель.

Міжнародну співпрацю рекомендується поглиблювати через активну участь у спільних ініціативах ООН, НАТО, EUvsDisinfo та «Nations Against Disinformation», розширення оперативного обміну індикаторами компрометації, створення міжнародно визнаних стандартів верифікації медіа та спільних лабораторій з виявлення генеративного контенту. Критично важливим є розроблення єдиних етико-правових рамок застосування штучного інтелекту в інформаційному протиборстві, що унеможливлять його використання як наступальної зброї при збереженні оборонного потенціалу.

Лише за умови одночасного впровадження цих взаємопов'язаних заходів - жорсткого, але пропорційного регулювання, передових технічних рішень, масової освіти та тісної міжнародної координації - можливо суттєво знизити ефективність інформаційної зброї, забезпечити довгострокову когнітивну стійкість суспільств і зберегти демократичні інститути в умовах перманентної цифрової війни.

ВИСНОВКИ

Проведене дослідження повністю досягло мети – визначено роль інформаційної зброї в сучасних міжнародних конфліктах та її системний вплив на глобальну безпеку. Встановлено, що інформаційна зброя радикально еволюціонувала від традиційної пропаганди до інтегрованого гібридного інструменту, який органічно поєднує психологічні операції, алгоритмічне підсилення, мікротаргетування, бот-мережі, deepfake-технології та кібератаки, що дозволяє досягати стратегічних цілей без або з мінімальним застосуванням кінетичної сили.

Виявлено ключові виклики цифрової епохи для міжнародної безпеки: рекомендаційні системи формують стійкі ехокамери, генеративний ШІ створює емоційно переконливий фальшивий контент, когнітивні упередження підсилюються автоматизованим поширенням, що призводить до зниження когнітивної стійкості суспільств, зростання поляризації та системного ускладнення прийняття державних і військових рішень.

На прикладі російсько-української війни після 2022 року доведено, що скоординовані інформаційно-психологічні операції синергізуються з кібер- і кінетичними діями, формують довготривалі хибні наративи, деморалізують цивільне населення та військових, створюють ілюзію внутрішньої та міжнародної підтримки агресора й безпосередньо впливають на динаміку конфлікту.

Визначено практичні механізми ефективної протидії: ШІ-системи раннього виявлення та автоматичного спростування, прозорість алгоритмів платформ, скоординована модерація контенту, оперативний міжвідомчий і міжнародний обмін даними за активної участі ООН, НАТО StratCom COE, EUvsDisinfo та національних центрів стратегічних комунікацій.

На основі аналізу розроблено комплекс рекомендацій щодо посилення міжнародної безпеки з урахуванням технологічних інновацій, етичних норм і глобальних стандартів: обов’язкове маркування та криптографічний захист ШІ-генерованого контенту, незалежний аудит рекомендаційних алгорит

jesteśmy, створення мережі наднаціональних і національних центрів моніторингу за моделями України та Естонії, масштабування програм цифрової грамотності, гармонізація законодавства з DSA/DMA та Кодексом ЄС з протидії дезінформації, а також прийняття міжнародних етико-правових стандартів застосування ШІ в інформаційному протиборстві.

Інформаційна зброя стала системоутворюючим елементом сучасних конфліктів, радикально трансформувавши природу війни. Забезпечення глобальної безпеки в цифрову епоху вимагає проактивної, технологічно оснащеної, правово врегульованої та міжнародно скоординованої стратегії, що поєднує державні, корпоративні, громадські та міжнародні зусилля для збереження когнітивної стійкості суспільств і демократичних інститутів.

Отже, за результатами дослідження можна надати кілька практичних **рекомендацій**:

По-перше, державам варто інвестувати в AI-системи для автоматичного виявлення фейків, але з обов’язковим людським контролем, щоб уникнути помилок.

По-друге, розширювати освітні програми не тільки онлайн, а й у школах та на роботі - вчити людей перевіряти джерела, розпізнавати емоційні гачки і ділитися знаннями з близькими. Третє: посилювати співпрацю з платформами на кшталт Facebook чи X, вимагаючи прозорості в алгоритмах і швидкої реакції на скарги.

Четверте: створювати незалежні фонди для фінансування фактчекінгу, щоб уникнути залежності від політики.

П’яте: проводити регулярні симуляції атак на рівні країни, щоб тренувати реакцію і виявляти слабкі місця.

Шосте: заохочувати міжнародні угоди про заборону певних маніпулятивних технологій, подібно до конвенцій про зброю.

СПИСОК ВИКОРИСТАНИХ ДЖЕРЕЛ

1. Airborne Propaganda: The Battle for Hearts and Minds . URL: https://britishonlinearchives.com/posts/category/articles/436/airborne-propaganda-the-battle-for-hearts-and-minds (date of access: 16.09.2025).

2. Britannica - Cold War Policies, Propaganda, & Speeches . *Encyclopædia Britannica*. URL: https://explore.britannica.com/study/cold-war-policies-propaganda-and-speeches (date of access: 16.09.2025).

3. Carson, D. A Content Analysis of Political Discourse on TikTok . 2021. URL: https://scholar.umw.edu/student_research/415 (date of access: 17.09.2025).

4. Majchrzak, A. Russian disinformation and the use of images generated by artificial intelligence (deepfake) in the first year of the invasion of Ukraine. *Media, Business and Culture*. 2023. URL: https://ejournals.eu/en/journal/media-biznes-kultura/article/russian-disinformation-and-the-use-of-images-generated-by-artificial-intelligence-deepfake-in-the-first-year-of-the-invasion-of-ukraine (date of access: 17.09.2025).

5. The Rise of Echo Chambers and How to Counter Them . *RAND Corporation*. 2023. URL: https://www.rand.org/randeurope/research/projects/2013/internet-and-radicalisation.html (date of access: 18.09.2025).

6. Echo chambers, filter bubbles and political polarization: A literature review . *Reuters Institute for the Study of Journalism*. 2023. URL: https://reutersinstitute.politics.ox.ac.uk/echo-chambers-filter-bubbles-and-polarisation-literature-review (date of access: 18.09.2025).

7. Paul, K. Russian disinformation surged on social media after invasion of Ukraine, Meta reports. *The Guardian*. 2022. URL: https://www.theguardian.com/world/2022/apr/07/propaganda-social-media-surge-invasion-ukraine-meta-reports (date of access: 19.09.2025).

8. Undermining Ukraine: How Russia widened its global information war in 2023 . *Digital Forensic Research Lab, Atlantic Council*. 2024. URL: https://www.atlanticcouncil.org/in-depth-research-reports/report/undermining-

ukraine-how-russia-widened-its-global-information-war-in-2023/ (date of access: 19.09.2025).

9. Olchowski, J., Kancik, E. Russia's disinformation as a threat to the security of Poland and the Czech Republic . 2025. URL: https://www.researchgate.net/publication/388647393_Russia%27s_Disinformation_as_a_threat_to_the_Security_of_Poland_and_the_Czech_Republic (date of access: 20.09.2025).

10. Marwick, A., Lewis, R. Media Manipulation and Disinformation Online . 2017. URL: https://datasociety.net/library/media-manipulation-and-disinfo-online/ (date of access: 20.09.2025).

11. Zhang, P., Haq, E.-U., Zhu, Y., Hui, P., Tyson, G. Echo Chambers within the Russo-Ukrainian War: The Role of Bipartisan Users . 2023. URL: https://arxiv.org/abs/2311.09934 (date of access: 21.09.2025).

12. Jääskeläinen, I. P., et al. Neural Processing of Narratives: From Individual Experience to Collective Action . 2020. URL: https://pmc.ncbi.nlm.nih.gov/articles/PMC7333591/ (date of access: 21.09.2025).

13. Disinformation about the war in Ukraine - reactions and narratives built on emotions . *BROD Hub*. 2024. URL: https://brodhub.eu/en/news/disinformation-about-the-war-in-ukraine-reactions-and-narratives-built-on-emotions/ (date of access: 22.09.2025).

14. AI tools usage for disinformation in the war in Ukraine . *Digital Forensic Research Lab*. 2024. URL: https://dfrlab.org/2024/07/09/ai-tools-usage-for-disinformation-in-the-war-in-ukraine/ (date of access: 22.09.2025).

15. González-Bailón, S., et al. Do social media undermine social cohesion? A critical review. 2023. URL: https://spssi.onlinelibrary.wiley.com/doi/10.1111/sipr.12091 (date of access: 23.09.2025).

16. Social Media Algorithms and Amplification of Disinformation . *NATO StratCom COE*. 2023. URL: https://stratcomcoe.org/publications/download/Social-media-manipulation-2021_2022-F.pdf (date of access: 23.09.2025).

17. Bradshaw, S., Howard, P. N. The global disinformation order: 2021 global inventory of organized social media manipulation . *Oxford Internet Institute*. 2021. URL: https://comprop.oii.ox.ac.uk/research/global-disinformation-order-2021/ (date of access: 24.09.2025).

18. Woolley, S., Howard, P. N. Conceptualizing the evolving nature of computational propaganda. *Annals of the International Communication Association*. 2023. Vol. 49, No. 1. P. 45. URL: https://academic.oup.com/anncom/article/49/1/45/8078344 (date of access: 24.09.2025).

19. Ferrara, E., Varol, O., Davis, C., Menczer, F., Flammini, A. The rise of social bots. *Communications of the ACM*. 2016. URL: https://dl.acm.org/doi/10.1145/2818717 (date of access: 25.09.2025).

20. Hart, E. The Psychology of Micro-Conversions: Why Small Wins Lead to Big Sales . *Innovative Flare*, 2024. URL: https://innovativeflare.com/the-psychology-of-micro-conversions-why-small-wins-lead-to-big-sales/ (date of access: 25.09.2025).

21. Shahbazi, M. Social Media Trust: Fighting Misinformation in the Time of Crisis. *ScienceDirect*. 2024. URL: https://www.sciencedirect.com/science/article/pii/S0268401224000288 (date of access: 16.10.2025).

22. Самолінська, С. І. Сегментація цільової аудиторії як визначальний фактор у процесі планування рекламної кампанії. *Економіка та держава*. 2021. № 4. С. 201-208. URL: http://www.economy.nayka.com.ua/pdf/4_2021/203.pdf (дата звернення: 17.10.2025).

23. Сучасні тренди кібербезпекової політики: висновки для України . *Національний інститут стратегічних досліджень*. URL: https://niss.gov.ua/doslidzhennya/nacionalna-bezpeka/suchasni-trendi-kiberbezpekovoi-politiki-visnovki-dlya-ukraini (дата звернення: 17.10.2025).

24. Інформаційна складова як ключовий аспект гібридної війни . *ResearchGate*. 2022. URL: https://www.researchgate.net/publication/364485581_Informacijna_skladova_ak_klucovij_aspekt_gibridnoi_vijni (дата звернення: 18.10.2025).

25. Чому російсько-українська війна почалася в лютому 2014 року . *Українська правда*. 2024. URL: https://www.pravda.com.ua/columns/2024/03/26/7447796/ (дата звернення: 18.10.2025).

26. Propaganda in focus: decoding the media strategy of ISIS . *Humanities and Social Sciences Communications*. 2024. URL: https://www.nature.com/articles/s41599-024-03608-y (date of access: 19.10.2025).

27. Як російські спецоперації намагаються зірвати мобілізацію в Україні . *Справа*. 2024. URL: https://spravdi.gov.ua/yak-rosijski-speczoperacziyi-namagayutsya-zirvaty-mobilizacziyu-v-ukrayini/ (дата звернення: 19.10.2025).

28. Інформаційно-психологічні операції, або немає сечі терпіти борошна росіян . *Свідомі*. 2022. URL: https://svidomi.in.ua/en/page/informatsiino-psykholohichni-operatsii-abo-nemaie-sechi-terpity-boroshna-rosiian (дата звернення: 20.10.2025).

29. Що таке ІПСО та як росія використовує цю технологію у війні проти України . *Chas.News*. 2023. URL: https://chas.news/current/scho-take-ipso-ta-yak-rosiya-vikoristovue-ih-u-viini-proti-ukraini (дата звернення: 20.10.2025).

30. Дезінформація та штучний інтелект: (не)видима загроза сучасності . *Центр демократії та верховенства права*. 2025. URL: https://cedem.org.ua/analytics/dezinformatsiya-shtuchnyi-intelekt/ (дата звернення: 21.10.2025).

31. AI-військові, молитви, заклики до перевороту: як і якими ІПСО Росія атакує українців . *Радіо Свобода*. 2023. URL: https://www.radiosvoboda.org/a/rosiya-ipso-internet/32730676.html (дата звернення: 21.10.2025).

32. Закон моделювання аудиторії . *StudFile*. URL: https://studfile.net/preview/5196738/page:3/ (дата звернення: 22.10.2025).

33. Харченко, І. М., Сапогов, С. О., Шамраєва, В. М., та ін. Основні засоби інформаційного протиборства та інформаційної війни як явища сучасного міжнародного політичного процесу. *Вісник Харківського національного університету імені В.Н. Каразіна. Серія: Міжнародні відносини. Економіка. Країнознавство. Туризм*. 2017. Вип. 6. С. 77-81. (дата звернення: 22.10.2025).

34. Тренди цифрового маркетингу у 2025 році: що потрібно знати, аби залишатися конкурентоспроможними . *Kyivstar Business Hub*. 2025. URL: https://hub.kyivstar.ua/articles/trendi-czifrovogo-marketingu-u-2025-roczi-shho-potribno-znati-abi-zalishatisya-konkurentospromozhnimi (дата звернення: 23.10.2025).

35. Стратегічні комунікації для безпекових і державних інституцій . *Фундація ім. Фрідріха Еберта*. 2022. URL: http://fes.kiev.ua/n/cms/fileadmin/upload2/Book_28-06-2022_web-3.pdf (дата звернення: 23.10.2025).

36. Темний бік штучного інтелекту: як ШІ підсилює російську пропаганду . *NetFreedom*. URL: https://netfreedom.org.ua/article/temnij-bik-shtuchnogo-intelektu-yak-shi-pidsilyuye-rosijsku-propagandu (дата звернення: 24.10.2025).

37. Регуляторні принципи в цифровій сфері . *Національний інститут стратегічних досліджень*. URL: https://niss.gov.ua/sites/default/files/2015-01/Konax_interne-65b6e.pdf (дата звернення: 24.10.2025).

38. Mahlangu I.G. Adaptive Cybersecurity Frameworks Using Artificial Intelligence and Machine Learning for Next-Generation Threat Detection . 2024. URL: https://www.researchgate.net/publication/395843609_Adaptive_Cybersecurity_Frameworks_Using_Artificial_Intelligence_and_Machine_Learning_for_Next-Generation_Threat_Detection (date of access: 25.10.2025).

39. Портільйо, В. Заклик до дії: проектування більш прозорого онлайн-світу. 2024. URL: https://www.sciencedirect.com/science/article/pii/S2666659624000192 (дата звернення: 25.10.2025).

40. Романишин, А. Штучний інтелект і дезінформація: політичні рекомендації для протидії . 2025. URL: https://pmc.ncbi.nlm.nih.gov/articles/PMC12351547/ (дата звернення: 25.10.2025).

41. Момбеллі, С. FAIRність у метаданих цифрових судових експертиз: оцінка повноти та відповідності принципам. 2024. URL: https://www.sciencedirect.com/science/article/pii/S2666281723002007 (дата звернення: 16.10.2025).

42. Шатіла, К. Цифрова грамотність, доступність та людський капітал у розвитку підприємницької стійкості. 2025. URL: https://www.sciencedirect.com/science/article/pii/S2444569X25000599 (дата звернення: 16.10.2025).

43. Information Integrity on Digital Platforms: Report of the Secretary-General . *United Nations*. New York, 2023. URL: https://www.un.org/sites/un2.un.org/files/sg_policy_brief_on_information_integrity.pdf (date of access: 17.10.2025).

44. Foreign Information Manipulation and Interference: A Framework for Policy Responses . *European External Action Service (EEAS)*. Brussels, 2023. URL: https://www.eeas.europa.eu/sites/default/files/documents/2025/EEAS-3nd-ThreatReport-March-2025-05-Digital-HD.pdf (дата звернення: 17.10.2025).

45. Coordinating the fight against disinformation: A whole-of-society approach . *NATO Strategic Communications Centre of Excellence*. Riga, 2023. URL: https://edmo.eu/blog/countering-disinformation-a-whole-of-society-approach-beyond-traditional-frameworks/ (date of access: 18.10.2025).

46. Regulation (EU) 2022/1925 on contestable and fair markets in the digital sector and amending Directives (EU) 2019/1937 and (EU) 2020/1828

(Digital Markets Act) . *Official Journal of the European Union*, L 265. 2022. URL: https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:32022R1925 (date of access: 18.10.2025).

47. Guiding Principles on Business and Human Rights . *Office of the United Nations High Commissioner for Human Rights (OHCHR)*. New York; Geneva, 2011. URL: https://www.ohchr.org/sites/default/files/documents/publications/guidingprinciplesbusinesshr_en.pdf (date of access: 19.10.2025).

48. Universal Declaration of Human Rights . *United Nations*. Adopted by General Assembly resolution 217 A (III) of 10 December 1948. URL: https://www.un.org/en/about-us/universal-declaration-of-human-rights (date of access: 19.10.2025).

49. International Covenant on Civil and Political Rights . *United Nations*. Adopted by General Assembly resolution 2200A (XXI) of 16 December 1966. URL: https://www.ohchr.org/en/instruments-mechanisms/instruments/international-covenant-civil-and-political-rights (date of access: 20.10.2025).

50. Guide on Article 10 - Freedom of expression of the European Convention on Human Rights . *Council of Europe, European Court of Human Rights*. Updated 31 August 2022. URL: https://rm.coe.int/guide-on-article-10-freedom-of-expression-eng/native/1680ad61d6 (date of access: 20.10.2025).

51. Code of Practice on Disinformation . *European Commission*. 16 June 2022. URL: https://digital-strategy.ec.europa.eu/en/library/2022-strengthened-code-practice-disinformation (date of access: 21.10.2025).

52. Estonia after the 2007 cyber-attacks: legal, strategic and organisational changes in cyber-security . *Cooperative Cyber Defence Centre of Excellence*. Tallinn: CCD COE, 2011. URL: https://ccdcoe.org/library/publications/estonia-after-the-2007-cyber-attacks-legal-strategic-and-organisational-changes-in-cyber-security/ (date of access: 21.10.2025).

53. Loi 2018-1202 du 22 décembre 2018 relative à la lutte contre la manipulation de l'information . France, 2018. URL:

https://www.legifrance.gouv.fr/eli/loi/2018/12/22/2018-1202/jo/texte (date of access: 22.10.2025).

54. Hungary. Act XII of 2020 on the Containment of the Coronavirus . Adopted 30 March 2020. URL: https://www.loc.gov/item/global-legal-monitor/2020-05-26/hungary-national-assembly-adopts-act-giving-government-special-powers-during-coronavirus-pandemic/ (date of access: 22.10.2025).

55. Global Disinformation Index . *Global Disinformation Index*. URL: https://www.disinformationindex.org/ (date of access: 23.10.2025).

56. Generative AI and watermarking . *European Parliament*. 2023. URL: https://www.europarl.europa.eu/RegData/etudes/BRIE/2023/757583/EPRS_BRI(2023)757583_EN.pdf (date of access: 23.10.2025).

57. Community Guidelines . *TikTok*. Effective 13 September 2025. URL: https://www.tiktok.com/community-guidelines/uk date of access: 24.10.2025).

58. Проєкт закону України про імплементацію Акту про цифрові послуги ЄС . *Міністерство цифрової трансформації України*. Submitted to European Commission in 2024. URL: https://rm.coe.int/lex-06-legal-opinion-ukraine/1680b5128a (дата звернення: 24.10.2025).

59. Про затвердження Порядку функціонування Державної системи онлайн-моніторингу . *Кабінет Міністрів України*. Постанова від 16 лютого 2024 року № 171. URL: https://zakon.rada.gov.ua/go/171-2024-%D0%BF (дата звернення: 25.10.2025).

60. Kouzy, R., Kraitem, A., Basso, M. F. Tweeting for Health Using Real-time Mining and Artificial Intelligence-Based Analytics: Design and Development of a Big Data Ecosystem for Detecting and Analyzing Misinformation on Twitter. *JMIR Formative Research*. 2023. Vol. 7, Article e43234. URL: https://pmc.ncbi.nlm.nih.gov/articles/PMC10337356/ (date of access: 25.10.2025).

61. Fighting deepfakes with more transparency about AI . *Microsoft*. 3 жовтня 2024. URL: https://news.microsoft.com/source/features/ai/fighting-deepfakes-with-more-transparency-about-ai/ (дата звернення: 25.10.2025).

62. Wang, R., Ye, D., Tang, L., Zhang, Y., Deng, J. AVT2-DWF: Improving Deepfake Detection with Audio-Visual Fusion and Dynamic Weighting Strategies . 22 березня 2024. URL: https://arxiv.org/abs/2403.14974 (date of access: 25.10.2025).

63. Deepfake Detection Market Report & Buyer's Guide 2025 . 2025. URL: https://www.biometricupdate.com/wp-content/uploads/2025/10/BU-Deepfake-Detection-Market-Report-and-Buyers-Guide.pdf (date of access: 25.10.2025).

64. Україна підписала меморандум про співпрацю в кібербезпеці з Європейським центром кіберкомпетентності . *Dev.ua*. 2025. URL: https://dev.ua/en/news/ukraina-pidpysala-memorandum-pro-spivpratsiu-v-kiberbezpetsi-z-yevropeiskym-tsentrom-kiberkompetentnosti-1741682739 (дата звернення: 25.10.2025).

65. Безкоштовні курси для українців на платформі «Дія. Цифрова освіта» . *Kharkiv IT Cluster*. 2022. URL: https://it-kharkiv.com/bezkoshtovni-kursy-dlya-ukrayintsiv-na-platformi-diya-tsyfrova-osvita/ (дата звернення: 25.10.2025).

66. Opinion on the Draft Law of Ukraine on Amendments to Certain Legislative Acts Aimed at Ensuring the Effectiveness of the Institutional Mechanism for Preventing and Countering Disinformation and Propaganda (CDL-AD(2025)021) . *Council of Europe. Venice Commission*. Strasbourg, 2025. URL: https://www.venice.coe.int/webforms/documents/?pdf=CDL-AD(2025)021-e (date of access: 27.10.2025).

67. Resolution adopted by the General Assembly on 12 November 2025: Ethical principles for the use of artificial intelligence in the information domain (A/RES/80/2025) . *United Nations General Assembly*. New York: UN, 2025. URL: https://press.un.org/en/2024/ga12588.doc.htm (date of access: 29.10.2025).

68. Misinformation and disinformation: both prebunking and debunking work in fighting it . *Joint Research Centre*. 2024. URL: https://joint-research-centre.ec.europa.eu/jrc-news-and-updates/misinformation-and-disinformation-

both-prebunking-and-debunking-work-fighting-it-2024-10-25_en (date of access: 29.10.2025).

69. C2PA Specifications: Explainer . *Coalition for Content Provenance and Authenticity (C2PA)*. 2025. URL: https://spec.c2pa.org/specifications/specifications/1.2/explainer/Explainer.html (date of access: 30.10.2025).

70. Disinformation: The European External Action Service and the EU Agency for Cybersecurity join forces to analyse the interplay between cybersecurity and Foreign Information Manipulation and Interference . *European External Action Service; European Union Agency for Cybersecurity*. Brussels, 08.12.2022. URL: https://www.eeas.europa.eu/eeas/disinformation-european-external-action-service-and-eu-agency-cybersecurity-join-forces-analyse_en (date of access: 30.10.2025).

АНОТАЦІЯ

Махотін Т.А. Інформаційна зброя в сучасних міжнародних конфліктах (магістерська робота). Харків. ХНУ ім. В.Н. Каразіна, 2025р.

Магістерська кваліфікаційна робота присвячена комплексному дослідженню феномену інформаційної зброї в сучасних міжнародних конфліктах та з'ясуванню її впливу на глобальну безпеку в умовах цифрової епохи. У роботі уточнено теоретичні засади формування та еволюції інформаційної зброї — від класичних методів пропаганди до сучасних цифрових інструментів, включно з алгоритмами соціальних мереж, діпфейками та штучним інтелектом. Визначено ключові виклики, які застосування інформаційної зброї створює для міжнародної безпеки, з урахуванням психологічних, соціальних та технологічних аспектів.

Оцінено вплив інформаційної зброї на динаміку сучасних конфліктів із фокусом на події в Україні після 2022 року, де інформаційні операції стали складовою гібридної агресії. Здійснено порівняльний аналіз застосування інформаційних операцій у різних регіонах світу. Охарактеризовано механізми протидії інформаційній зброї на міжнародному рівні, зокрема діяльність ООН, НАТО та співпрацю держав з технологічними компаніями. Розроблено рекомендації щодо зміцнення міжнародної безпеки в цифрову епоху, спрямовані на подолання дезінформаційних загроз і формування стійкості суспільств до цифрових маніпуляцій.

Ключові слова: інформаційна зброя, міжнародні конфлікти, дезінформація, цифрова епоха, міжнародна безпека, Україна, діпфейки, кібероперації, ООН, НАТО.

ANNOTATION

Makhotin T.A. *Information Weapons in Contemporary International Conflicts* (Master's Thesis). Kharkiv: V. N. Karazin Kharkiv National University, 2025.

The master's qualification work is devoted to a comprehensive study of the phenomenon of information weapons in modern international conflicts and an assessment of their impact on global security in the digital age. The research clarifies the theoretical foundations of the formation and evolution of information weapons — from traditional methods of propaganda to contemporary digital tools, including social media algorithms, deepfakes, and artificial intelligence. The key challenges posed by the use of information weapons for international security are identified, taking into account psychological, social, and technological dimensions.

Recommendations aimed at strengthening international security in the digital era and enhancing societal resilience against disinformation and digital manipulation are proposed.

Keywords: information weapons, international conflicts, disinformation, digital age, international security, Ukraine, deepfakes, cyber operations, UN, NATO.

ВІДГУК

на кваліфікаційну роботу магістра
студента 2-го курсу групи УМІБ-61 денної форми навчання
спеціальності 291 «Міжнародні відносини, суспільні комунікації та регіональні студії»
освітньо-професійної програми «Міжнародна інформаційна безпека»
Навчально-наукового інституту «Каразінський інститут міжнародних відносин та туристичного бізнесу»
Харківського національного університету імені В. Н. Каразіна
Махотіна Тимура Анатолійовича
на тему: «Інформаційна зброя в сучасних міжнародних конфліктах»

Магістерська кваліфікаційна робота Махотіна Тимура Анатолійовича присвячена дослідженню феномену інформаційної зброї як ключового чинника сучасних міжнародних протистоянь. Обрана тема є надзвичайно актуальною у контексті зростаючого значення інформаційних операцій, розвитку когнітивних впливів, застосування технологій штучного інтелекту та цифрових платформ для втручання в політичні процеси. Автор обґрунтовує важливість вивчення новітніх інструментів інформаційного впливу, що використовуються як державними, так і недержавними акторами, та їхнього впливу на глобальну безпеку.

У роботі застосовано послідовну структуру викладу. У першому розділі запропоновано змістовний аналіз концепту інформаційної зброї, її сутнісних характеристик та відмінностей від класичних інформаційних операцій, розглянуто підходи до типологізації інформаційного впливу та механізми когнітивної дії. У другому розділі висвітлено міжнародні практики протидії інформаційним загрозам, розглянуто нормативні рамки і приклади реагування окремих держав та міжнародних організацій на нові форми інформаційної агресії. Третій розділ присвячений прикладним аспектам протидії інформаційній зброї, сформульовано пропозиції щодо підвищення спроможності держав до раннього виявлення інформаційних атак, розвитку інформаційної стійкості та впровадження технологічних рішень із застосуванням штучного інтелекту.

Оцінка отриманих результатів свідчить, що автор досяг поставленої мети та

виконав основні завдання дослідження. У роботі простежується вміння поєднати теоретичні положення з прикладами сучасних конфліктів, продемонстровано системний підхід до розуміння інформаційної зброї та механізмів її застосування. Рекомендації носять практичний характер та можуть бути використані при формуванні державної політики у сфері інформаційної безпеки, що вказує на значущість проведеного дослідження.

Разом із тим, у роботі можна було б більш детально розкрити питання оцінювання результативності контрзаходів та їхню ефективність у довгостроковій перспективі. Більш широка порівняльна характеристика між різними моделями протидії могла б додатково посилити прикладну частину дослідження. Однак зазначене має рекомендаційний характер і не впливає на загальну позитивну оцінку роботи.

Магістерська кваліфікаційна робота Махотіна Тимура Анатолійовича загалом відповідає вимогам, що висуваються до кваліфікаційних робіт другого (магістерського) рівня вищої освіти. Дослідження вирізняється чіткою структурою, логічним викладенням матеріалу та актуальністю обраної проблематики. Отримані результати засвідчують достатній рівень підготовки здобувача та дозволяють рекомендувати роботу до захисту перед екзаменаційною комісією.

Науковий керівник:

д. держ. упр., професор,

професор кафедри міжнародних відносин Солових В. П.

РЕЦЕНЗІЯ

на кваліфікаційну роботу магістра
студента 2-го курсу групи УМІБ-61 денної форми навчання
спеціальності 291 «Міжнародні відносини, суспільні комунікації та регіональні студії»
освітньо-професійної програми «Міжнародна інформаційна безпека»
Навчально-наукового інституту «Каразінський інститут міжнародних відносин та туристичного бізнесу»
Харківського національного університету імені В.Н. Каразіна
Махотіна Тимура Анатолійовича
на тему: «Інформаційна зброя в сучасних міжнародних конфліктах»

1. Актуальність теми

Тема застосування інформаційної зброї в умовах сучасних міжнародних конфліктів є надзвичайно актуальною у зв'язку з трансформацією характеру воєнних дій, зростанням масштабів гібридних загроз та широким використанням цифрових технологій у інформаційно-психологічних операціях. Збройна агресія РФ проти України після 2014 року та особливо після 2022 року продемонструвала, що інформаційні операції виступають окремим інструментом впливу, здатним формувати когнітивну реальність, підривати національну стійкість і суттєво впливати на перебіг конфліктів.

Обрана тема має високу практичну значущість, оскільки питання інформаційної зброї, алгоритмічного таргетування, застосування ШІ у дезінформації, гібридних моделей впливу та формування когнітивних середовищ залишаються ключовими викликами для національної та міжнародної безпеки.

2. Характеристика якості виконання розділів роботи

Кваліфікаційна робота складається зі вступу, трьох розділів, висновків та списку використаних джерел.

У першому розділі автор ґрунтовно розкриває концептуальні засади інформаційної зброї як системи цілеспрямованого впливу. Показано еволюцію

інформаційних операцій від традиційної пропаганди до сучасних мережевих та алгоритмічно керованих впливів. Значну увагу приділено когнітивним аспектам, ролі емоційних тригерів, ехо-камер, генеративних технологій.

Другий розділ присвячений аналізу нормативно-етичних рамок протидії інформаційній зброї та міжнародним стратегіям боротьби з дезінформацією. Розглянуто стандарти ООН, НАТО, ЄС, а також підходи держав до регулювання інформаційного простору.

У третьому розділі подано комплексний аналіз впливу інформаційної зброї на динаміку сучасних конфліктів, розкрито роль алгоритмів, автоматизованих мереж, мультиканального поширення наративів та їхню здатність до адаптації. Автор формулює практичні напрями посилення міжнародної безпеки.

3. Ступінь обґрунтованості висновків

Висновки логічно випливають із поставленої мети та виконаних завдань. Вони підкріплені системним аналізом теоретичних позицій, сучасних технологічних трендів, міжнародної нормативної бази та реальних кейсів інформаційних операцій. Автор демонструє здатність до критичного мислення та формулювання практично значущих рекомендацій.

4. Позитивні сторони роботи

Робота відзначається високим рівнем науково-аналітичної глибини, широкою джерельною базою та вдалим поєднанням сучасних теоретичних підходів із практичними прикладами. Особливо цінним є комплексний розгляд інформаційної зброї як системи когнітивного та технологічного впливу.

5. Недоліки роботи

Недоліками є недостатня деталізація кейсів поза російсько-українським контекстом, а також потреба розширення аналізу етичних ризиків використання алгоритмічного таргетування та ШІ. Проте зазначені недоліки не знижують загальної якості роботи.

6. Загальна оцінка

Кваліфікаційна робота Махотіна Тимура Анатолійовича виконана на високому науковому рівні, відповідає вимогам до магістерських досліджень за спеціальністю 291 «Міжнародні відносини, суспільні комунікації та регіональні студії» та вирізняється комплексністю, ґрунтовністю й практичною значущістю. Робота заслуговує на позитивну оцінку.

Рецензент:
кандидат соціологічних наук (доктор філософії),
доцент кафедри соціально-гуманітарних наук
Харківського національного університету
міського господарства імені О. М. Бекетова Олександра ЗІНЧИНА

Підпис О. Зінчина
Засвідчую:
Ст. інженер відд. кадрів
"__" ____
ЗО №02071151