МІНІСТЕРСТВО ОСВІТИ ТА НАУКИ УКРАЇНИ
НАЦІОНАЛЬНИЙ АВІАЦІЙНИЙ УНІВЕРСИТЕТ
ФАКУЛЬТЕТ МІЖНАРОДНИХ ВІДНОСИН
КАФЕДРА МІЖНАРОДНИХ ВІДНОСИН, ІНФОРМАЦІЇ ТА
РЕГІОНАЛЬНИХ СТУДІЙ

ДОПУСТИТИ ДО ЗАХИСТУ
Завідувач випускової кафедри
_____ Ніна РЖЕВСЬКА
«15» 06 2023р.

КВАЛІФІКАЦІЙНА РОБОТА
ВИПУСКНИКА ОСВІТНЬОГО СТУПЕНЯ БАКАЛАВРА
ЗА СПЕЦІАЛЬНОСТІ 291 «МІЖНАРОДНІ ВІДНОСИНИ, СУСПІЛЬНІ КОМУНІКАЦІЇ ТА РЕГІОНАЛЬНІ СТУДІЇ»
ОСВІТНЬО-ПРОФЕСІЙНОЇ ПРОГРАМИ
«МІЖНАРОДНА ІНФОРМАЦІЯ»

Тема: «ПІДХОДИ ТА МЕТОДИ ІНФОРМАЦІЙНОГО ПРОТИБОРСТВА В РОСІЙСЬКО-УКРАЇНСЬКІЙ ВІЙНІ»

Виконавець: здобувач вищої освіти 4 курсу, 409 групи, Онопрійчук Алан Артурович
Керівник: к. політ.н., доцент кафедри міжнародних відносин, інформації та регіональних студій Сапсай Артем Петрович

Нормоконтролер: _____ Олексій МЕНДРІН
(підпис)

КИЇВ 2023

ЗМІСТ

ВСТУП

Актуальність теми дослідження обумовлена тим, що підходи та методи інформаційного протиборства в російсько-українській війні впливають на сучасне суспільство та міжнародні відносини. Ця форма війни, яка включає в себе розповсюдження дезінформації та маніпулювання інформацією, суттєво впливає на політичний, соціальний та культурний контекст Росії та України.

По-перше, інформаційна війна має велике значення для формування думок та уявлень громадськості. Широке застосування дезінформації та маніпулятивних методів призводить до спотворених уявлень про події, акторів конфлікту та світоглядні позиції. Це може негативно впливати на суспільну стабільність, міжнаціональні відносини та довіру до медіа.

По-друге, цифрова епоха надала інформаційній війні нові можливості. Інтернет та соціальні мережі стали ефективними засобами поширення інформації та впливу на громадську думку. Це створює нові виклики та загрози для національної та міжнародної безпеки, що вимагає розробки ефективних стратегій інформаційного протиборства.

По-третє, тривалість та непрямий характер російсько-української війни свідчать про необхідність детального дослідження підходів та методів, використовуваних сторонами конфлікту. Це дозволяє не тільки зрозуміти специфіку даного конфлікту, але й виявити загальні тенденції та принципи інформаційного протиборства, що можуть бути корисними в інших контекстах.

Медіаграмотність є ключовою умінням, яке допомагає аналізувати, оцінювати та критично мислити про інформацію. Вона включає здатність розпізнавати маніпулятивні методи, розуміти різні медійні формати та їх вплив, а також вміння перевіряти достовірність інформації та розпізнавати фейкові новини. Розвиток медіаграмотності допомагає людям стати більш самосвідомими та критичними споживачами інформації.

Тому, важливо вміти сприймати інформацію з різних джерел, аналізувати та обробляти її, розуміти контекст та можливі мотиви, що стоять за інформаційними повідомленнями. Сприйняття інформації вимагає здатності розрізняти об'єктивну інформацію від спотвореної, розуміти маніпулятивні техніки та методи, які використовуються для впливу на громадську думку.

Розвиток медіаграмотності та сприйняття інформації має першочергове значення для захисту інформаційного простору від негативного впливу. Це дозволяє громадянам розуміти можливі ризики маніпуляцій та дезінформації, запобігати поширенню небажаної інформації та сприяти побудові більш об'єктивного, раціонального інформаційного середовища. Розвиток медіаграмотності є процесом, що потребує спільних зусиль суспільства, освітніх інституцій та медіа організацій для забезпечення стійкості та розвитку інформаційної сфери.

Метою дослідження є обґрунтування якості трансформативності підходів та методів інформаційного протиборства в контексті російсько-української війни. Дослідження спрямоване на розкриття основних характеристик інформаційної війни, визначення її ролі та впливу на конфлікт між Росією та Україною.

Об'єктом є інформаційне протиборство в російсько-українській війні.

Предметом є підходи та методи, що використовуються в інформаційному протиборстві в рамках російсько-української війни, так і поза ними.

Головними **завданнями** є :

– проаналізувати поняття та теоретичні підходи до інформаційного протиборства: огляд основних теорій, концепцій та підходів, що використовуються в цій сфері;

– дослідити характеристики та особливості інформаційного протиборства в російсько-українській війні: виявити стратегії, тактики, методи та інструменти, що використовуються сторонами конфлікту;

– проаналізувати вплив інформаційного протиборства на суспільство та громадську думку: визначити його роль у формуванні думок, управлінні інформаційним простором та вплив на переконання людей;

– дослідити використання соціальних медіа та інтернету в інформаційному протиборстві;

– вивчити історичний контекст інформаційного протиборства в російсько-українській війні: розглянути зародження, розвиток та еволюцію інформаційного протиборства в рамках даного конфлікту, проаналізувати роль ЗМІ та інших комунікаційних каналів.

Характеристика джерельної бази роботи та стану дослідженості проблеми:

Проблема "підходів та методів інформаційного протиборства в російсько-українській війні" є актуальною та складною, і для її вивчення була використана різноманітна джерельна база, що допомогла освітлити різні аспекти цієї проблематики. Джерельна база включає наукові праці, експертні дослідження, аналітичні звіти та журналістські матеріали, що забезпечують різноманітні погляди та аналіз даної теми.

1. Законодавчі акти та нормативні документи, пов’язані з інформаційною війною та інформаційною безпекою.
2. Дослідження та публікації вітчизняних дослідників, що стосуються інформаційного протиборства в російсько-українській війні.
3. Роботи зарубіжних дослідників, які висвітлюють тему інформаційної війни, зокрема в контексті конфлікту між Росією та Україною.
4. Огляд історії розвитку проблеми інформаційної війни, включаючи роботи, що досліджують її етапи та основні характеристики.
5. Аналіз інформаційних технологій, методів та засобів, використовуваних у російсько-українській війні, зокрема їх взаємодію з військовими діями.
6. Вивчення ролі ЗМІ в контексті російсько-української інформаційної війни.
7. Аналіз стратегій, принципів, технологій та інструментів інформаційної безпеки як складової інформаційного протиборства.

Методи дослідження:

1. Аналіз: Цей метод дозволяє розкрити структуру, взаємозв'язки та особливості інформаційного протиборства в рамках російсько-української війни. Він включає розбір концепцій, теорій, стратегій, тактик та інструментів, що використовуються сторонами конфлікту, з метою з'ясування їх сутності та впливу.

2. Індукція: Цей метод полягає в виведенні загальних висновків на основі конкретних фактів, прикладів та спостережень про інформаційне протиборство в російсько-українській війні. Він дозволяє виявити тенденції, закономірності та особливості цього процесу.

3. Класифікація: Цей метод дозволяє групувати різноманітні аспекти інформаційного протиборства в російсько-українській війні на основі спільних ознак та характеристик. Наприклад, можна класифікувати методи дезінформації, використовувані сторонами конфлікту, за їхнім призначенням, масштабом чи способами реалізації.

4. Опис: Цей метод полягає у детальному описі конкретних подій, випадків та ситуацій, пов'язаних з інформаційним протиборством. Він дозволяє відтворити послідовність подій, розкрити взаємозв'язки та виявити ключові фактори, що впливають на його хід.

5. Пояснення: Цей метод передбачає роз'яснення причин, механізмів та наслідків інформаційного протиборства в російсько-українській війні. Він дозволяє розкрити фактори, які спонукають сторони конфлікту до використання певних підходів та методів, а також розуміння впливу цих дій на політичну, військову та інформаційну ситуацію.

Апробація результатів дослідження була представлена на XXIII Міжнародній науково-практичній конференції здобувачів вищої освіти і молодих учених «ПОЛІТ. Сучасні проблеми науки» (4-7 квітня 2023 року, м. Київ) [41].

Структура роботи складається зі вступу, 3 розділів, 9 підрозділів, висновків, списку використаних джерел (44 найменувань). Робота розглядає інформаційну війну та її основні характеристики. Він визначає поняття «інформаційна війна». Термін «інформаційна війна» має багато визначень. основні елементи та особливості

інформаційної війни Етапи становлення інформаційної війни Характеристики кожного етапу У контексті російсько-української війни інформаційна війна включає використання різних інформаційних технологій і методів, дезінформацію та пропаганду, кібератаки та кібершпигунство, використання соціальних мереж і медіа. Взаємодія інформаційної війни з військовими діями, реакцію України на інформаційне протиборство, контрінформаційні заходи та стратегії, Оцінка його ефективності. Аналіз результатів і впливу інформаційних кампаній. Виклики та перспективи інформаційного протиборства. Розробка нових технологій і захист від інформаційних загроз.

РОЗДІЛ 1
ІНФОРМАЦІЙНА ВІЙНА ТА ЇЇ ОСНОВНІ ХАРАКТЕРИСТИКИ

1.1. Визначення поняття «інформаційна війна»

Інформаційна війна – це форма ведення конфлікту, яка передбачає використання різних засобів і технологій для маніпулювання інформацією та впливу на думки, переконання та поведінку цільової аудиторії. Інформаційна війна може бути введена як міжнародними акторами, так і державними чи недержавними суб'єктами внутрішньої політики [1, с. 34].

Інформаційна війна - протиборство сторін за допомогою поширення спеціально підготовленої інформації та протидії аналогічному зовнішньому впливу на себе [2, с. 15].

Згідно з роботою Георгія Почепцова (2000)відмінності між звичайною війною та інформаційною війною можуть бути скомпоновані в сім блоків[10]:

1. інформаційна війна має гнучкий арсенал озброєнь та високу непередбачуваність;

2. в інформаційній війні можливе лише поетапне захоплення територій;

3. в інформаційній війні є можливість багаторазового захоплення тих самих людей (або окремих тематичних аспектів у їх свідомості), працює нечітка логіка;

4. в інформаційній війні воюючі сторони неможливо виділити за ознакою приналежності до будь-якої групи або виконання певної соціальної ролі;

5. в інформаційній війні вплив на супротивника невідчутний і може наділятися доброзичливою формою;

6. в інформаційній війні впливи вибіркові та охоплюють різні верстви населення по-різному;

7. в інформаційної війни основною небезпекою є відсутність видимих руйнувань. Внаслідок цього захисні механізми суспільства не активуються.

Інформаційна війна може включати в себе різноманітні засоби та методи впливу на інформаційне середовище, зокрема:

Дезінформацію та фейки - поширення неправдивої інформації з метою впливу на думки та переконання цільової аудиторії [4].

Дезінформація та фейки - це способи поширення неправдивої інформації з метою впливу на думки та переконання цільової аудиторії. Дезінформація - це навмисне поширення неправдивої або маніпулювальної інформації з метою впливу на думки та поведінку цільової аудиторії. Фейки - це фальшиві новини, що містять неправдиву інформацію або намагаються змінити загальний контекст події, щоб викликати певну реакцію.За допомогою дезінформації та фейків, зловмисники можуть змінювати громадську думку та впливати на громадські процеси. Таким чином, вони можуть змінювати результати виборів, створювати напруження між різними групами людей, підштовхувати до насильства та конфліктів, а також викликати хаос і незгоду в суспільстві.

Дезінформація та фейки можуть походити від різних джерел, таких як державні органи, приватні особи, політичні організації, соціальні мережі та інші. Одним з основних засобів поширення дезінформації та фейків є соціальні мережі та інтернет-ресурси, оскільки вони забезпечують швидкий та легкий доступ до інформації. Одним з наслідків дезінформації та фейків є загроза національній безпеці та стабільності. Якщо дезінформація та фейки були розповсюджені широко, вони можуть викликати хвилю незгоди в суспільстві та призвести до конфлікту, повстань або навіть війни. того, дезінформація та фейки можуть створювати загрозу здоров'ю та безпеці людей, наприклад, коли неправдива інформація про ліки або вакцини змушує людей відмовлятися від лікування або профілактики [5].

Одним зі способів боротьби з дезінформацією та фейками є збір та аналіз інформації, перевірка її достовірності та поширення правдивої інформації серед громадськості. того, важливо сприяти розвитку медіа-грамотності та критичного мислення серед громадян, щоб вони могли розпізнати правдиву інформацію від дезінформації та фейків.Захистом від дезінформації та фейків є освічені та свідомі

люди, які здатні дійсно оцінювати інформацію, що до них доходить, та робити розумні висновки.

Тому важливо зробити все можливе, щоб забезпечити доступність правдивої та достовірної інформації для всіх громадян та сприяти їхньому розвитку як свідомих та відповідальних членів суспільства.

Кібератаки - спроби зламати та пошкодити інформаційні системи та мережі противника [6].

Кібератака - це спроба зламати та пошкодити інформаційні системи та мережі противника, що може створити різноманітні дослідження, включаючи внутрішні дані, виток конфіденційної інформації, порушення функціонування критичної інфраструктури та інше.

Кібератаки можуть мати різні форми та мету, включаючи наступні:

Віруси та інші зловмисні програми: це можуть бути програми, що працюють на комп'ютері або в мережі, які можуть пошкодити або видалити дані, перехопити конфіденційну інформацію або заражати інші комп'ютери.

Фішинг та інші соціально-інженерні атаки: це можуть бути спроби отримати конфіденційну інформацію, так як паролі та інші особисті дані, за допомогою соціально-інженерних методів, таких як розсилка фішингових електронних листів або створення фальшивих веб-сайтів.

Denial-of-service (DoS) і denial-of-service-атаки з використанням зомбі-комп'ютерів (DDoS): це можуть бути атаки, спрямовані на сервери перевантаження та мережу шляхом надсилання великої кількості запитів з використанням зомбі-комп'ютерів [5].

Хакерські атаки: це можуть бути спроби здійснити несанкціонований доступ до комп'ютерної системи або мережі з використанням викрадення конфіденційної інформації або завдання іншої шкоди.

Кібершпіонаж: це можуть бути спроби отримати конфіденційну інформацію шляхом нелегального доступу до систем та мереж, що належать іншим країнам або

організаціям. Це може бути здійснено за допомогою зламування паролів, використання шкідливих програм або соціально-інженерних методів.

Кібератаки можуть бути здійснені з різних мотивів, таких як політичні, економічні, кримінальні або терористичні. В результаті таких атак можуть бути завдані значні збитки, включаючи фінансові, репутаційні та безпекові. Одним з найбільш відомих прикладів кібератак є атака на компанію Equifax у 2017 році, в результаті якої було вкрадено особисті дані понад 145 мільйонів користувачів [7].

Інформаційну блокаду - обмеження доступу до інформації, яка може бути корисною для противника [8].

Інформаційна блокада є одним з методів військової та політичної стратегії, що має на меті обмеження доступу до інформації, яка може бути корисною для противника. Цей метод полягає у тому, щоб використовувати різні інструменти та техніки для приховування та обмеження доступу до інформації, яка може бути використана противником для своїх потреб.

Інформаційна блокада може бути здійснена різними способами, зокрема:

Блокування доступу до інформації: це може бути здійснено шляхом заборони на доступ до певних джерел інформації, наприклад, блокування сайтів, заборони на використання деяких мереж, блокування доступу до певних публікацій та інших методів.

Розповсюдження дезінформації: цей метод полягає у тому, щоб розповсюджувати неправдиву інформацію про події, що може змінити уявлення противника про ситуацію та перекрутити його реакцію.

Контроль за засобами масової інформації: держава може забороняти певні джерела масової інформації, або навпаки, створювати свої власні засоби масової інформації, щоб контролювати потік інформації.

Шпигунство та кібератаки: противник може використовувати різні методи, такі як хакінг, шпигунство та інші, щоб зламати системи обміну інформацією та отримати доступ до захищеної інформації.

Контроль за джерелами інформації: можна використовувати різні методи, щоб контролювати джерела інформації, що надходять до противника, наприклад, перехоплювання, перевірка та заборона на використання певних джерел інформації.

Інформаційна блокада може мати різні наслідки. З одного боку, вона може сприяти захисту національних інтересів та забезпечити безпеку держави. З іншого боку, вона може порушувати право на свободу інформації, спричиняти дезінформацію та маніпулювання громадською думкою.

Важливо збалансувати необхідність захисту від потенційних загроз та забезпечення свободи інформації та доступу до неї. Для цього держави повинні розвивати механізми контролю та регулювання інформаційного простору, які дозволяють забезпечити безпеку держави, не порушуючи прав громадян.

Розповсюдження пропаганди - використання інформаційних каналів для підтримки своїх позицій та ідеології.

«Слова, звуки, картинки, відео — з них складається калейдоскоп нашої реальності. Яку саме мозаїку ми зафіксуємо перед очима, залежить від нас самих» [9, с. 57].

Розповсюдження пропаганди - це маніпулювання інформацією, яке використовується для підтримки своїх позицій та ідеології за допомогою різних інформаційних каналів. Це може бути здійснено різними способами, включаючи використання соціальних медіа, телебачення, радіо, газет, журналів та інтернет-сайтів.

Одним з методів розповсюдження пропаганди є використання емоційно заряджених термінів та фраз, які можуть викликати відчуття страху, гніву, ненависті або інших негативних емоцій. Це дозволяє певній стороні залучити увагу громадськості та вплинути на її поведінку.

Інший спосіб розповсюдження пропаганди - це використання дезінформації та фейкових новин. Такі новини можуть бути створені з метою дискредитувати певну людину, групу або ідеологію, або ж викликати суспільний розкол та нестабільність.

Пропаганда може використовуватися для зміни поглядів та переконань громадськості. Це може бути здійснено за допомогою повільної, поступової зміни у сприйнятті певних ідей та понять, які можуть відображатися у зміні мовлення, мислення та поведінки людей. Розповсюдження пропаганди може мати серйозні наслідки, такі як розкол у суспільстві, збільшення конфліктів та загострення міжнародних відносин. Щоб захиститися від пропаганди, важливо бути критичним до отримуваної інформаці і перевіряти її джерела. Важливо слідкувати за різними точками зору та перевіряти факти, щоб уникнути сприйняття неправильної або недостовірної інформації.

Також корисно звертати увагу на мову та тон повідомлень, щоб виявляти спроби маніпулювання емоціями чи поглядами людей.

Існує багато організацій, які працюють над протидією пропаганді та фейковим новинам, таких як фактчекерські проекти та інтернет-ресурси, які спеціалізуються на детальному аналізі та перевірці інформації. того, важливо взяти на себе відповідальність та розповісти іншим про важливість критичного мислення та перевірки джерел інформації.

5. Використання соціальних мереж та інтернет-платформ - маніпулювання думками та переконаннями цільової аудиторії за допомогою соціальних мереж та інтернет-платформ.

Інформаційна війна може мати значний вплив на політичну ситуацію та рівень соціальної стабільності в країні чи регіоні. Вона може знижувати рівень довіри до державних інституцій та ослаблювати державу, створюючи настрої недовіри та хаосу. Тому відстоювання інформаційної безпеки стає важливим завданням для держав та інших організацій, що мають доступ до значних обсягів інформації.

Інформаційна війна може мати різний масштаб та тривалість. Вона може бути обмежена до окремих подій або тривати протягом довгого часу, охоплюючи багато різних аспектів життя країни. Для успішної реалізації інформаційної війни необхідно мати значні ресурси, в тому числі людські, технічні та фінансові.

Інформаційна війна може мати різні мети. Найчастіше ці мети пов’язані з політикою, економікою та безпекою. Наприклад, інформаційна війна може бути спрямована на дискредитацію політичних опонентів, підірвання авторитету держави, створення соціальної напруги, зміну внутрішньої та зовнішньої політики країни, забезпечення власної безпеки або зниження безпеки противника а однією з найбільш небезпечних форм є хактивізм, який передбачає використання кіберзлочинів з метою досягнення політичних цілей. Це може бути викрадення та розповсюдження конфіденційної інформації, блокування роботи важливих інформаційних систем, а також вплив на дії громадських та політичних організацій. Інформаційна війна є складною проблемою, яка вимагає комплексного підходу та використання різних засобів та технологій для захисту від її негативного впливу. Для боротьби з інформаційною війною необхідно забезпечити ефективний захист інформаційних систем, вдосконалювати антивірусне програмне забезпечення та інші технічні засоби захисту.

Також необхідно підвищувати інформаційну грамотність населення, щоб люди могли розпізнати правдиву інформацію від фейкової, та збільшувати рівень кібербезпеки в організаціях [10].

Держави та організації повинні вести про активну політику щодо протидії інформаційній війні, включаючи створення відповідних відділів та служб для моніторингу та аналізу інформації, яка поширюється в мережі. Важливо також розробляти стратегії відповіді на інформаційні атаки та використання сучасних методів аналізу даних, щоб вчасно виявляти та протидіяти загрозам. Міжнародне співробітництво також відіграє важливу роль в боротьбі з інформаційною війною. Держави повинні співпрацювати в області кібербезпеки та обмінюватися досвідом та інформацією про нові загрози та методи їх протидії.

Інформаційна війна є серйозною загрозою для держав та інших організацій, і вимагає комплексних заходів та зусиль для її протидії. Важливо забезпечити ефективний захист інформаційних систем, підвищувати рівень кібербезпеки в організаціях та інформаційну грамотність населення, а також проводити про активну

політику та міжнародне співробітництво для моніторингу та аналізу інформації та виявлення загроз. Та для ефективної боротьби з інформаційною війною необхідно використовувати сучасні методи аналізу даних та розробляти стратегії відповіді на інформаційні атаки. Загалом, це питання потребує уваги та зусиль від усіх сторін, щоб забезпечити безпеку та стабільність в мережі та в суспільстві в цілому.

1.2. Етапи розвитку інформаційної війни

Інформаційна війна – це процес протистояння двох або більше сторін, які використовують засоби та технології інформаційної та комунікаційної сфери для досягнення політичних, економічних або військових цілей. Засоби та цілі постійно змінюються та доповнюються [1]. Цифровізація та нові технології тільки сприяють цьому. Розвиток інформаційної війни можна розглядати в різних контекстах та етапах [1], включаючи:

- Перший етап: використання технологій радіо та телевізійного мовлення в розповсюдженні пропаганди та впливу на громадську думку. У цей період активно використовувалися засоби масової інформації для маніпулювання думкою людей та формування їх поглядів.
- Другий етап: виникнення Інтернету та поширення соціальних мереж, що дозволяють широкому колу людей впливати на інформаційне середовище. У цей період багато держав та груп використовують Інтернет та соціальні мережі для здійснення пропаганди та інформаційної війни.
- Третій етап: зростання кількості та різноманітності інформаційних технологій, які можуть бути використані в інформаційній війні. Цей етап включає в себе розвиток інтернет-технологій, технологій шифрування, кібератак та використання штучного інтелекту в процесах аналізу та обробки інформації.
- Четвертий етап: поява нових типів загроз та викликів, які пов’язані зі збільшенням ролі та значенням кіберпростору. Цей етап характеризується зростанням кількості кібератаків, розповсюдженням штучного інтелекту в процесах

інформаційної війни та використанням соціальних мереж як інструменту впливу на громадську думку.

- П’ятий етап: ускладнення інформаційної війни через використання технологій, які можуть створювати фальшиву або неповну інформацію. Наприклад, технології глибокого навчання можуть використовуватися для створення фальшивих зображень та відео, що може призвести до маніпулювання інформацією та зміни громадської думки.
- Шостий етап: зростання ролі державних структур та міжнародних організацій в боротьбі з інформаційною війною. У цьому етапі відбувається створення нових правових і політичних механізмів для запобігання та реагування на інформаційні загрози, а також збільшення відповідальності за поширення дезінформації та пропаганди.
- Сьомий етап: розвиток технологій штучного інтелекту, які можуть бути використані для розпізнавання та боротьби з дезінформацією та пропагандою. У цьому етапі активно використовуються алгоритми машинного навчання та аналізу даних для виявлення неправдивої інформації та маніпулятивних технік в інформаційному просторі.

Інформаційна війна є надзвичайно складним і мінливим процесом, який постійно змінюється. Для створення та реалізації ефективних стратегій протидії дезінформації та пропаганди в інформаційному просторі важливо розуміти та усвідомлювати етапи розвитку інформаційної війни.

Для цього необхідно забезпечити доступ до правдивої та об’єктивної інформації, підвищити обізнаність громадян про медіа та критичне мислення, а також сприяти розвитку алгоритмів і технологій, які допомагають виявити та боротися з пропагандою та дезінформацією.

Наприклад, використання штучного інтелекту може бути корисним для боротьби з дезінформацією та пропагандою, але воно також може бути небезпечним для прав людини та свободи слова. Таким чином, важливо створити ефективний

механізм контролю за використанням штучного інтелекту в інформаційній війні, а також гарантувати, щоб у цьому процесі дотримувалися прав людини та демократії.

1.3. Основні характеристики інформаційної війни

Інформаційна війна - це форма війни, що використовується для здобуття переваги у політичній або військовій боротьбі за допомогою масової комунікації, зокрема за допомогою інформаційних технологій [11].

Використання інформаційних технологій: інформаційна війна використовує інформаційні технології, такі як Інтернет, соціальні мережі, блоги, електронна пошта та інші засоби масової комунікації, для поширення інформації та впливу на громадську думку.

Основні характеристики інформаційної війни включають наступні елементи [6]:

● Маніпуляція громадською думкою: інформаційна війна може включати маніпулювання громадською думкою, включаючи використання психологічних технік, щоб впливати на емоції та переконання людей.

● Спроби впливати на дії противника: інформаційна війна може бути використана для впливу на дії противника, такі як зниження бойової готовності, зміну позицій або зменшення підтримки.

● Використання соціальних мереж: соціальні мережі є потужним інструментом для поширення інформації та впливу на громадську думку, тому вони є важливим компонентом інформаційної війни.

● Широкомасштабність: інформаційна війна може бути проведена на широкому масштабі, охоплюючи значну кількість людей та територій. Вона може включати багато різних елементів, включаючи політичну пропаганду, маніпулювання соціальними медіа, кібератаки та інші методи впливу на громадську думку.

● Неформальний характер: інформаційна війна може мати неформальний характер, що робить її важко визначити та відслідковувати. Вона може бути

проведена без наявності відкритої військової агресії, що робить її складнішою для реагування.

● Суперечливість: інформаційна війна може включати суперечливу інформацію, яка намагається змішати людей та спричинити хаос. Це може створити певну незрозумілість та змішаність серед громадськості, що робить важчим розуміння та оцінку того, що відбувається.

● Психологічна бойова дія: інформаційна війна може включати психологічну бойову дію, що включає в себе застосування психологічного тиску та психологічного насильства для досягнення цілей.

● Відкритість: інформаційна війна може бути відкритою, коли сторони відкрито взаємодіють та співпрацюють одна з одною, або вона може бути проведена приховано, коли сторони роблять це таємно, без розголошення своїх дій.

● Висока швидкість: інформаційна війна може включати високу швидкість поширення інформації та впливу на громадську думку. Вона може бути проведена в реальному часі, що дозволяє швидко реагувати на події та впливати на них.

● Залежність від технологій: інформаційна війна є дуже залежною від технологій, таких як соціальні медіа, інтернет, кіберпростір та інші. Вона може використовувати різноманітні техніки та інструменти для досягнення своїх цілей.

● Неспроможність розпізнати правду та брехню: у сучасному світі інформаційна війна може бути дуже складною, оскільки дуже важко розрізнити правду та брехню. Інформаційна війна може включати в себе дезінформацію, фейки, пропаганду та інші методи, що можуть приховувати справжню картину подій.

● Загроза національній безпеці: інформаційна війна може становити серйозну загрозу національній безпеці та стабільності держави. Вона може спричинити розкол у суспільстві, збільшення конфліктів та загострення міжнародних відносин.

У підсумку, інформаційна війна є серйозною загрозою для сучасного світу, оскільки вона може мати широкий спектр наслідків, включаючи загрозу національній безпеці та стабільності, суперечливу інформацію, психологічний тиск та інші негативні наслідки. Щоб захиститися від інформаційної війни, необхідно бути

обережним та критичним до отриманої інформації, розвивати критичне мислення та критичний погляд на світ, та зберігати національну єдність та стабільність.

Інформаційна війна є досить складним і багатогранним явищем, що має багато визначень та інтерпретацій. Її можна розглядати як процес використання інформації з метою досягнення визначених цілей, зокрема, впливу на свідомість та поведінку інших осіб, груп або держав.

Етапи розвитку інформаційної війни зазвичай поділяються на підготовчий, активний та завершальний. Підготовчий етап включає підготовку та збір інформації, а також створення необхідної інфраструктури.

Активний етап передбачає активне використання інформації для досягнення визначених цілей, у тому числі, розповсюдження пропаганди та дезінформації. Завершальний етап полягає в оцінці результатів та аналізі досвіду.

Основні характеристики інформаційної війни включають в себе засоби та методи впливу, мету та об’єкт впливу, а також акторів, що беруть участь у процесі. Засоби та методи впливу можуть включати в себе масову медіа, соціальні мережі, бот-аккаунти та інші інструменти. Мета та об’єкт впливу можуть бути різними - від підірвання стабільності держави до впливу на поведінку окремих осіб. Акторами, що беруть участь у процесі інформаційної війни, можуть бути різні держави, терористичні організації, корпорації та інші суб’єкти.

Отже, розуміння основних характеристик інформаційної війни дозволяє розробляти ефективні стратегії протидії таким діям. Важливо виявляти та аналізувати різноманітні форми дезінформації та пропаганди, розвивати медіаграмотність та критичне мислення у населення, а також вдосконалювати технології захисту інформації та контрдії противників.

Також важливо співпрацювати з іншими країнами та міжнародними організаціями з метою координації заходів протидії інформаційним загрозам та зловживанням інформацією.

Інформаційна війна стала невід’ємною складовою сучасного світу, де інформація є одним з найцінніших ресурсів. У світі, де люди користуються

інтернетом, соціальними мережами та медіа платформами, інформаційна війна може мати серйозні наслідки для політики, соціальної сфери, економіки та культури. Основними характеристиками інформаційної війни є використання різних каналів для передачі інформації, зміна світогляду та переконань громадськості, маніпулювання емоціями та дезінформація, що може мати серйозні наслідки, такі як загострення міжнародних відносин, збільшення конфліктів та розкол у суспільстві.

Щоб захиститися від інформаційної війни, важливо бути критичним до отриманої інформації та перевіряти її достовірність, потрібно розвивати критичне мислення та критичний підхід до інформації, яку ми отримуємо, а також виховувати громадян, які мають здатність аналізувати та оцінювати інформацію. Важливо розробляти та впроваджувати ефективні механізми захисту від дезінформації та інших форм інформаційної агресії.

Сьогодні інформаційна війна є важливою частиною сучасного світу, де інформація є одним із найцінніших ресурсів. Інформаційна війна може мати серйозні наслідки для політики, соціальної сфери, економіки та культури в світі, де люди користуються Інтернетом, соціальними мережами та медіа платформами.

Інформаційна війна включає використання різних каналів для передачі інформації, маніпулювання емоціями, зміну світогляду та переконань громадськості та дезінформацію. Наслідки інформаційної війни включають загострення міжнародних відносин, збільшення конфліктів і розкол у суспільстві. Щоб уникнути інформаційної війни, важливо бути критичним до інформації, яку ви отримуєте, і перевіряти, чи вона справжня. Необхідно навчити людей критичному мисленню та ставлення до інформації, виховати здатність до аналізу та оцінки інформацію та створити та запровадити ефективні методи захисту від дезінформації та інших видів інформаційної агресії.

РОЗДІЛ 2
ІНФОРМАЦІЙНА ВІЙНА В КОНТЕКСТІ РОСІЙСЬКО-УКРАЇНСЬКОЇ ВІЙНИ

2.1. Інформаційні технології та методи, використовувані в російсько-українській війні

У російсько-українській війні Росія використовує різноманітні інформаційні технології та методи для досягнення своїх цілей [12]. Ось декілька основних з них:

Дезінформація та пропаганда: Росія активно поширює дезінформацію та пропаганду, щоб впливати на громадську думку. Це включає поширення фейкових новин, спотворення фактів, створення негативного образу України та підміну реальності. Російські медіа ресурси, такі як телеканали, радіостанції, веб-сайти та соц мережі, використовуються саме для цього.

Кібератаки: Росія використовує кібератаки для отримання контролю над інформацією та системами в Україні. Це може включати злам веб-сайтів, розповсюдження шкідливих програм, кібершпигунство та кібер саботаж. Кібератаки можуть спричиняти перебої в роботі критичних інфраструктурних об’єктів, таких як енергетичні системи або транспортні мережі, та перешкоджання роботі служб та агентств.

Соціальні мережі та інтернет-форуми: Росія активно використовує соціальні мережі та інтернет-форуми для поширення своїх пропагандистських наративів та маніпулювання громадською думкою. Це може включати створення фейкових акаунтів, ботів та роботизованих систем, які поширюють дезінформацію та створюють штучний образ підтримки своїх позицій.

Використання науково-дослідницьких центрів та пропагандистських агентств: Росія використовує науково-дослідницькі центри та пропагандистські агентства для розробки та поширення спеціально підготовленої інформації. Ці організації

створюють пропагандистські матеріали, проводять аналіз інформаційної ситуації та розробляють стратегії впливу на громадськість.

Використання «тролів» та псевдо журналістів: Росія використовує спеціально найманих осіб, відомих як «тролі», які активно коментують, поширюють дезінформацію та атакують противників у соціальних мережах та інтернет-форумах. того, псевдожурналісти можуть створювати фейкові новини та матеріали, що виглядають як відомості з відповідальних джерел, але насправді є частиною пропагандистської кампанії.

Ці інформаційні технології та методи дозволяють Росії контролювати інформаційний простір, маніпулювати громадською думкою, створювати негативний образ України та досягати своїх політичних та військових цілей.

Під час 1 та 2 світових воєн поширеним методом нагнітання паніки серед цивільного населення було розповсюдження пропагандистських листівок, які мали на меті завербувати або посіяти страх. Німецькі нацисти скидали з літаків схожі папірці на території країн антигітлерівської коаліції [13]. Під час війни на сході україни ще 2014 року використовували сучасніший, але схожий метод смс-спаму повідомлення слали і продовжують надсилати як мирному населенню так і солдатам у прифронтових зонах, аби зменшити бойовий дух або збільшити недовіру до української влади [14].

Методів впливу існує безліч. Це полегшує введення, будь якої війни, перш за все, не потрібно бути наївним і думати, що пропаганда існує лише на росії. Вона ведеться абсолютно в кожній країні. Але як ми знаємо росія лідер з найбіль налаштованих на пропропаганду держав, що ведуть інформаційну війну [9].

Пропаганда потрібна, аби змінити загальні переконання і погляди у великої кількості людей. Вона може бути напів правдивою, містити вибіркові історичні факти і упередженість. Але це, якщо говорити узагальнено, іноді виникає думка, що чим більш ірраціональною і абсурдною є та чи інша історія, тим більше росіян в неї повірить. Наприклад, що українську владу захопили нацисти або про біолабораторії,

існування яких чомусь ніхто не поспішав доводити ну всіж знають, якщо повторювати брехню багато багато разів, то вона раптом стане правдою.

Звичайно, пропаганда краще працює, коли велика кількість вірить і підтримує її, тому росіяни так полюбили виставляти школярів у формі нацистської символіки. Ну аби весь світ позаздрив народній згуртованості, це потрібно для того, аби люди, які ще не піддалися пропаганді до цього часу врешті зробили свій вибір. Ну якщо всі підтримують війну та «путінський режим» то це напевне правильно. Людина починає міркувати, що, якби щось було поганим, то велика кількість людей не підтримувала б таке. Правда, найпримітивніша пропаганда намагається маніпулювати почуттями і емоціями. Це низькосортний вид інформаційного бруду, який не має підтверджень, де максимум це слова «очевидців», але її основні споживачі і не мають наміру перевіряти інформацію. Вони споживають найпримітивніше з найпримітивнішого.

Діло не менш популярними в росії ток шоу, де створюють ілюзію дискусії, у який, звісно ж, провладна позиція виглядає більш переконливою і правильною. Звичайний формат новини не такий цікавий та емоційний, а от Соловйов, який з піною з рота розповідає, «яка Україна невдячна нащадниця ссср, вічно їй треба в той Євросоюз» значно краще.

Такі політичні шоу не мають на меті інформувати про стан справ чи змусити побачити істину в дискусії, а лише емоційно переконати, хто насправді правий повилазили тепер і борці з українськими фейками, що намагаються переконати людей з доступом до інтернету.

Крім попереднього варіанту, росіяни створюють інший тип пропаганди. Тут уже беруть певний тип інформації і викривляють її, у вигідній для себе позиції. Можливо, ви пам’ятаєте, що основним доказом існування біолабораторії в Україні критично-мислячі росіяни вважали слова заступниці державного секретаря Сша, Вікторії Нуланд, котрі насправді були просто неправильно проінтерпретовані [16]. Є ще один тип впливу, цільова аудиторія якого люди, що вивчають історію, скептично ставляться до теленовин та мають критичне мислення.

Саме для таких і переписують історію, аби виправдати анексію Криму чи окупацію частини України. До речі, для них же знімають величезну кількість фільмів і пишуть книги якраз прообраз меншовартості українця у російських фільмах. Такий тип пропаганди працює, аби переконати інтелігенції у тому нібито території України це споконвічно московитській території,тут проживають корінні росіяни.

Вміло маніпулюють і приписують українцям іншу релігію, якусь не таку та культурні цінності притаманні чужому заходу. Чим більше українцям присвоюють відмінного чужого, роблять їх якимись не такими людьми, тим менше до них жалю, а цим працювали багато багато років. Загалом же пропаганда зобов'язана демонізувати українців, аби виправдовувати свої злочинні дії, якщо не придумати казку про те, що Україну потрібно звільняти від нацистів, американців чи ще як.

Широкомасштабне використання дезінформації та пропаганди, вказує на важливу роль інформаційної війни в контексті конфлікту між Росією та Україною. Ці методи мають на меті маніпулювання громадською думкою, створення негативного образу та дезорієнтацію серед населення. Давайте розглянемо деякі основні характеристики використання пропаганди та дезінформації Росією [14; 17]:

1. Створення фейкових новин: Росія активно створює фейкові новини, що схожі на правдиві, але містять спотворені або вигадані факти. Це дозволяє їм розповсюджувати неправдиву інформацію через контрольовані медіа-ресурси та соціальні мережі, що впливає на переконання громадськості.

2. Маніпулювання фактами та контекстом: Росія використовує вибіркову інформацію та спотворені факти, щоб перекрутити події відповідно до своїх інтересів. Це створює спотворене уявлення про ситуацію та може призвести до неправильних висновків серед аудиторії.

3. Використання контрольованих медіа-ресурсів: Росія контролює певні медіа-ресурси, які використовуються для поширення пропагандистської інформації та дезінформації. Ці ресурси намагаються створити негативний образ України та підірвати довіру до українських владних структур.

4. Зловживання соціальними мережами та інтернетом: Росія використовує соціальні мережі та інтернет-платформи для поширення дезінформації. Вони можуть використовувати ботів, фейкові акаунти та роботизовані системи, щоб швидко поширювати неправдиву інформацію та створювати штучний образ підтримки своїх пропагандистських наративів.

5. Емоційне впливання на аудиторію: Росія активно використовує емоційні методи для впливу на аудиторію. Це включає використання гострих заголовків, емоційних зображень та історій, які стимулюють негативні емоції серед громадськості. Це сприяє поширенню дезінформації та підсилює реакцію аудиторії.

6. Важливо розуміти, що використання пропаганди та дезінформації є складними і стратегічними засобами впливу на громадськість. Ці методи мають на меті формування певних уявлень та переконань серед аудиторії з метою досягнення політичних або геополітичних цілей.

Тепер розглянемо декілька прикладів російської пропаганди на більш практиній основі та спробуємо зрозуміти «звідки в неї ростуть ноги та руки».

«Українських школярів вчать вбивати російських снігурів.Хлопчика розіп'яли у Слов'янську. Американські біо-лабораторії працюють в Україні.» Цей список відвертої брехні, в яку тяжко повірити свідомій людині, від російської пропаганди безкінечний. В це мало віриться, але, якщо це тільки один з елементів системи, яку побудували ще в часи КДБ для зміни мислення та поведінки людей. Сьогодні поговоримо про основу-основ російської пропаганди - її 7 заповідей .

У 2018 New York Times створив цикл документальних фільмів – про методи створення і поширення дезінформації. Саме ті, які Росія застосовує ще з часів Холодної війни і по нині. КГБісти чверть свого робочого часу витрачали на придумування брехні.Прийоми, які застосовує Росія – це класичні «активні заходи» з підручника КДБ.

Про те, як працюють ці методи, New York Times розповіли експерти:

Едвард Лукас – вивчав Росію десятиліттями. Спочатку як журналіст, а потім як аналітик методів дезінформації.

Доктор Клейр Уоделл – фахівець Гарвардського університету з верифікації даних в Інтернеті. Вона відстежує приклади брехні з 2008 року.

Клінт Уоттс – колишній співробітник ФБР та військовослужбовець. Він роками попереджав про ризики, які несе дезінформація.

Ларрі Мартін – колишній агент КДБ під прикриттям, який застосовував у країнах Заходу прийоми з дезінформації (так звані «активні заходи»).

За допомогою цих експертів, а також співробітників розвідувальних та детективних служб, New York Times реконструювала 7 заповідей російської дезінформації: перевірений часом покроковий рецепт створення ідеальної кампанії з дезінформації [18].

Заповідь перша. Розколоти!

Росіяни знаходять точку суспільного болю. Ту тріщину, яку можна поглибити та добряче розколоти. Вони шукають економічні, соціальні, демографічні, лінгвістичні, етнічні – будь-які джерела соціальних розбіжностей і роздувають їх, щоб люди втратили довіру один до одного.

Заповідь друга. Створити зухвалу брехню!

Вона має бути настільки приголомшливою, щоб ніхто й повірити не міг, що таке взагалі можна вигадати. Її транслюють звідусіль. Про неї говорять експерти, політики, астрологи, журналісти, військові. Кожен для своєї аудиторії та з своїми аргументами. Врешті решт люди вірять і наслідки цього згубні. Як тут не згадати цитату, яку приписують Гебельсу - «Повторюйте брехню досить часто, і вона стане правдою». У сучасній психології такий ефект отримав назву «ілюзія істини».

Заповідь третя. Додати дрібку правди!

А щоб у брехню швидше повірили її потрібно обгорнути навколо правдивої серцевини. Найбільш успішні інформаційні кампанії містять у собі елементи правди, і завдяки цьому дезінформація сприймається разом із ними. І так, Геббельс теж активно використовував такий прийом.

Заповідь четверта. Ховати руки!

Так, щоб джерелом повідомлення здавався хтось інший. І як тут не згадати, що 42% українців ніколи не перевіряють інформацію. А у 2020 лише 3% могли відрізнити правду від брехні в інформаційному просторі.

Заповідь п’ята. Знайти корисного ідіота!

Так Росія називає тих, хто бездумно сприймає кремлівські меседжі й просуває їх серед своєї аудиторії. На жаль, таких багато і кожна нова тріщина за яку береться російська пропаганда підсвічує нових.

Заповідь шоста. Заперечувати все що відбувається!

Коли набридливі правдошукачі намагаються спростувати фальшивку? Саме для цього потрібна шоста заповідь - заперечувати все. Навіть якщо правда є очевидною, все одно заперечувати. Агресивно наполягати на своєму.

Заповідь сьома. Грати в довгу!

Росія прагне вести тривалу гру і вкладає величезні ресурси у речі, які можуть не давати плодів роками. Зрештою нагромадження цих операцій протягом тривалого часу досягне потрібного результату. Це схоже на краплю, яка точить камінь. Відразу вона не дає ніяких помітних наслідків. Але якщо ці краплі падають роками, вона проб’ють у камені дірку. І росіяни про це знають.

Ці сім простих заповідей були потужною зброєю радянського КДБ, і Росія застосовує їх знову і знову, адаптуючи до цифрового світу.

«Гірший ворог будь-якої пропаганди - інтелектуалізм.»

Кібератаки є ефективним та улюбленим інструментом інформаційної війни, який використовується в російсько-українській війні. Вони полягають у зламі, руйнуванні або знищенні інформаційних систем та комп’ютерних мереж з метою завдання шкоди, зламу конфіденційної інформації, крадіжки даних або спотворення образу цілі. Після початку війни Росії проти України сталося кілька випадків кібератак [19, с.2], включаючи:

Атака на системи зв’язку газети «Kyiv Post» та супутникову мережу «KA-SAT» за годину до вторгнення (24 лютого).

Атака IssacWiper на урядові вебсайти (25 лютого).

Кібератака на пункт прикордонного контролю з метою перешкоджання виїзду біженців до Румунії (25 лютого).

Атаки на цифрову інфраструктуру України, що призвело до блокування доступу до фінансових послуг та енергетичних ресурсів (28 лютого).

У травні, верховний представник ЄС засудив атаку проти супутникової мережі «KA-SAT», яка призвела до перебоїв зі зв'язком для приватних осіб та державних і комерційних структур України. Він назвав цю атаку «ще одним прикладом безвідповідальної поведінки Росії в кіберпросторі» і попередив, що кібератаки на Україну можуть мати системні наслідки для безпеки громадян Європи.

З березня продовжилися кібератаки на українські урядові, фінансові, неурядові та гуманітарні організації. Ці атаки включали в себе використання шкідливого програмного забезпечення, фішингові атаки та атаки на постачальників телекомунікаційних послуг, що призводило до порушення функціонування українських мереж.

З кінця березня тривали кібератаки, які включали фішингові електронні листи, використання бекдору для стеження та кібернапади на сайти телекомунікаційних компаній та платформи WordPress. Ці атаки призводили до перебоїв у зв'язку та обмеження доступу до фінансових та урядових сайтів.

В квітні, хакери отримали конфіденційну інформацію та облікові дані користувачів урядових установ та медіаструктур. Вони також заволоділи банківськими та платіжними даними громадян за допомогою троянської програми та шахрайського опитування через сторінки в соціальних мережах.

І це тільки мала частина того, що нам відомо. Для спрощення поняття небезпеки та жорстокості кібератак Росії, можна розглянути саме види кібератак [4;20]. Ось деякі види кібератак, які використовуються за час російсько-української війни:

1. ДДоС-атаки (Distributed Denial of Service): Це атаки, під час яких велика кількість запитів надсилається до цільової системи, що перевантажує її та призводить до відмови в обслуговуванні.Росія використовує ДДоС-атаки для збою роботи

урядових веб-сайтів, банківських систем, медіа-ресурсів та критично важливих інфраструктурних об’єктів.

2. Фішинг та соціальний інжиніринг: Росія використовує фішингові атаки, що полягають у відправці підроблених електронних листів або повідомлень з метою обману отримувачів та отримання їх конфіденційної інформації, такої як паролі, особисті дані або фінансова інформація. Соціальний інжиніринг включає маніпулювання людьми з метою отримання доступу до їх систем або інформації.

3. Кібершпигунство: Росія здійснює кібершпигунство шляхом злому комп’ютерних систем та мереж для отримання конфіденційної інформації. Це може включати доступ до важливих військових, політичних або економічних даних, розробку шпигунського програмного забезпечення або перехоплення комунікацій.

4. Розповсюдження шкідливого програмного забезпечення: Росія використовує різні види шкідливого програмного забезпечення, такі як віруси, троянські програми, черв’яки та шпигунські програми, для злому систем, крадіжки інформації або здійснення кібершантажу.

Ці кібератаки дозволяють Росії отримати контроль над інформацією, завдати шкоди важливим інфраструктурним об’єктам та створити хаос та незручності в Україні. Важливо зазначити, що кібератаки можуть мати серйозні наслідки для безпеки, економіки та стабільності країни, тому захист інформаційної інфраструктури є надзвичайно важливим завданням.

Соціальні мережі та інтернет-форуми є потужними інструментами комунікації та обміну інформацією, але в контексті інформаційної війни їх також використовують для поширення пропаганди, дезінформації та маніпулювання громадською думкою. Росія активно використовує соціальні мережі та інтернет-форуми для досягнення своїх політичних та військових цілей в російсько-українській війні.

Ось деякі основні аспекти використання соціальних мереж та інтернет-форумів у контексті інформаційної війни:

Розповсюдження пропаганди та дезінформації: Росія створює та розповсюджує пропагандистські матеріали через соціальні мережі, такі як Facebook, Twitter,

VKontakte, інтернет-форуми та інші платформи. Ці матеріали можуть містити спотворені факти, фейкові новини або маніпулятивні повідомлення з метою вплинути на громадську думку та створити негативний образ України.

Створення фейкових акаунтів та ботів: Росія використовує фейкові акаунти в соціальних мережах, які прикидаються звичайними користувачами, але насправді є керованими російськими операторами. Ці акаунти використовуються для поширення пропаганди, ретвітів, лайків та коментарів, щоб збільшити вплив та розповсюдження певних повідомлень. Боти також використовуються для автоматичного поширення пропаганди та маніпулювання громадською думкою. Маніпулювання трендами та алгоритмами: Росія намагається маніпулювати алгоритмами соціальних мереж та інтернет-форумів, щоб контролювати видимість та розповсюдження певних повідомлень. Вони можуть активно коментувати та лайкати певні повідомлення, що допомагає їм з’являтись у трендах та отримувати більше уваги. Дискредитація опонентів та поширення конспірологічних теорій: Росія використовує соціальні мережі та інтернет-форуми для дискредитації опонентів та поширення конспірологічних теорій. Вони можуть створювати фейкові облікові записи, які критикують українську владу, активістів чи журналістів, та сприяють поширенню дезінформації.

Використання науково-дослідницьких центрів та пропагандистських агентств теж є одним із ключових елементів інформаційної війни Росії проти України. Ці структури використовуються для підтримки пропагандистських дій, розповсюдження дезінформації та маніпулювання громадською думкою.

Росія активно використовує свої науково-дослідницькі центри для підготовки пропагандистських матеріалів, які потім розповсюджуються через різні канали, включаючи соціальні мережі, медіа та інтернет-форуми. Ці центри можуть залучати вчених, експертів та аналітиків, які пишуть наукові статті, дослідження та коментарі, що підкріплюють позицію Росії та створюють образ ворога. Вони можуть надавати «наукові» обгрунтування для агресивної політики Росії та її втручання в Україну.

Використання «тролів» та псевдо журналістів є одним із ефективних методів інформаційної війни, які використовуються Росією в контексті російсько-української війни. Ці методи спрямовані на поширення дезінформації, маніпулювання громадською думкою та створення образу ворога. Давайте розглянемо деталізованіше кожен з цих аспектів:

«Тролі»: «Тролі» - це люди або групи людей, які спеціально наймаються або підконтрольні російським владним структурам, щоб активно поширювати дезінформацію та пропаганду в інтернеті. Вони часто діють під прикриттям або використовують фейкові профілі в соціальних мережах, форумах та інтернет-платформах. «Тролі» активно коментують, лайкають, діляться та поширюють пропагандистські повідомлення, створюючи враження, що підтримка таких ідей є широко поширеною. Вони також можуть вести агресивну антиукраїнську кампанію, атакувати критиків російської політики та поширювати конспірологічні теорії.

Псевдожурналісти: Росія використовує псевдо журналістів або контрольовані медіа ресурси для поширення дезінформації та пропаганди. Ці псевдожурналісти працюють під прикриттям незалежних журналістів, але насправді їх матеріали підпадають під контроль російських владних структур. Вони створюють фейкові новини, спотворювати факти та пропагувати позицію, яка вигідна Росії. Ці матеріали потім широко поширюються через соціальні мережі, медіа та інтернет-платформи, що сприяє їх впливу на громадську думку. Використання «тролів» та псевдо журналістів дозволяє Росії контролювати інформаційне середовище, створювати вигляд широкої підтримки своїх позицій, а також спотворювати образ України та її дій у міжнародному співтоваристві. Дуже важливо бути критичним до отриманої інформації, перевіряти її джерела та робити власний дослідницький аналіз, щоб уникнути попадання під вплив пропаганди та дезінформації.

2.2 Взаємодія інформаційної війни з військовими діями

Протягом конфлікту між Росією та Україною з 2014 по 2023 роки було безліч прикладів взаємодії інформаційної війни з військовими діями. Ось кілька прикладів:

Використання дезінформації під час окупації Криму [17;21]: У 2014 році, під час анексії Криму, Росія використала широкомасштабну дезінформаційну кампанію. Засоби масової інформації, контрольовані Росією, поширювали фейкові новини про загрозу етнічним росіянам та українцям у Криму, що виправдовувало військову інтервенцію. Ця дезінформація створила вигляд підтримки висування Росією своїх військових сил на територію України.

Коли російські війська окупували Крим у 2014 році, дезінформація стала важливим інструментом для досягнення своїх цілей і маніпулювання суспільною думкою. В цьому розділі розглядаються подробиці використання дезінформації під час окупації Криму, зокрема способи, наслідки та вплив на українське суспільство.

Під час окупації Криму одним із основних методів дезінформації було поширення неправдивої інформації про обставини на півострові. Російські ЗМІ та пропагандистські канали активно поширювали вигадані розповіді про загрозу російськомовному населенню, напад українських націоналістів і бажання кримчан приєднатися до Росії. Цей спосіб маніпулювання спотворив реальність, створивши враження, що окупація Росії є «захистом» національних інтересів.

Дезінформація також використовувалася для створення уявлення про Україну як про країну, яка підтримує тероризм, націоналізм і фашизм. Російська пропаганда активно розповсюджувала неправдиві новини про «злочинні дії» українських силових структур з метою тероризму та репресій проти російськомовних громадян. Це призвело до негативного ставлення до України та підтримки окупації Росією.

Крім того, російська пропаганда використовувала тактику «діли і володарюй». Вони намагалися створити неприязнь між різними групами населення та зменшити підтримку опозиційних сил, підкреслюючи національні та етнічні конфлікти.

Це призвело до загострення міжетнічних стосунків і поставило під загрозу стабільність на півострові.

Під час окупації Криму дезінформація мала значний вплив. Вона спричинила розкол і конфлікти між різними групами населення, зниження довіри до української влади та засобів масової інформації, а також створення «нової реальності», яка базувалася на брехні та фальсифікаціях.

Дезінформація підірвала національну безпеку та стабільність країни. Ці дії не обмежувалися Кримом, вони поширилися на інші частини України, підкреслюючи, наскільки важливо навчити людей розуміти медіа та критично мислити [9].

Таким чином, використання дезінформації під час окупації Криму було важливою частиною інформаційної стратегії Росії. Воно вплинуло на суспільну думку, створило перекручені точки зору на ситуацію та змінило конфліктний дискурс. Усвідомлення способів і наслідків використання дезінформації дозволяє зрозуміти, наскільки важливо навчити громадян критично мислити та розуміти медіа, щоб вони могли ефективно протидіяти таким маніпуляціям у майбутньому.

Інформаційні атаки на східні регіони України: Під час військових дій на сході України, Росія активно використовувала інформаційні атаки для дестабілізації ситуації та формування негативного образу українських силовиків. Це включало розповсюдження фейкових новин про вбивства, жорстокість та примусове виселення мирних мешканців, що мали на меті підірвати довіру до українських військових та правительства.

Інформаційні атаки на східні регіони України є складною проблемою, яка має значний вплив на життя та стабільність людей у цих регіонах. Ці атаки – це систематична інформаційна кампанія, спрямована на створення недовіри, конфлікту та розбрату серед місцевого населення з метою підриву суверенітету та територіальної цілісності України. Інформаційні атаки включають дезінформацію, маніпуляцію фактами, пропаганду та створення фейкових новин.

Атаки здійснюються через соціальні медіа, радіо, телебачення та інтернет-платформи. Їх мета полягає в тому, щоб підштовхнути людей до певних політичних

або геополітичних . Інформаційні атаки викликають розкол у суспільстві та конфлікт. Розповсюдження спотворених або неповних повідомлень, агресивна пропаганда та збудження ненависті створюють ворожнечу між людьми.

Це може спричинити соціальні розколів, напружені стосунки та навіть збройні конфлікти. Поряд із соціальними наслідками, інформаційні атаки також впливають на економіку.

Поширення неправдивих повідомлень і образливе представлення східних регіонів України може призвести до зниження інвестиційних можливостей, втрати робочих місць і посилення економічної нерівності. Такі атаки можуть вплинути на повсякденну життєдіяльність місцевостей, зокрема шляхом впливу на енергетичні системи, транспортну інфраструктуру та інші області. Захист від інформаційних атак вимагає спільних зусиль різних сторін, таких як уряди, громадські організації, медіа та звичайні люди.

Держава повинна приділяти достатню увагу забезпеченню кібербезпеки, захисту інформаційного простору та ефективному контролю за поширенням дезінформації. Також важливо навчати людей критичному мисленню, надавати доступ до правдивої інформації та сприяти розумінню принципів маніпуляції інформацією. Оскільки інформаційні атаки мають глобальний характер і можуть порушити безпеку та стабільність багатьох країн, співпраця з міжнародними партнерами також є важливою частиною боротьби з інформаційними атаками.

Підвищення усвідомленості населення [9], вдосконалення законодавства щодо кібербезпеки, зміцнення медійної грамотності та сприяння розвитку незалежних медіа – це основні стратегії захисту східних регіонів України від інформаційних атак. Щоб забезпечити безпеку та стабільність у східних регіонах України, необхідно співпрацювати та ефективно протистояти інформаційним атакам.

Кібератаки на українську інфраструктуру: Росія здійснювала кібератаки на критичну інфраструктуру України, таку як енергосистеми, транспортні мережі та комунікаційні системи. Ці атаки призводили до зниження ефективності оборонних

зусиль України, а також до перешкоджання командуванню та зв’язку між військовими одиницями.

Кібератаки на українську інфраструктуру є серйозною загрозою, тому потрібно проводити постійний моніторинг і заходи забезпечення кібербезпеки. Зважаючи на те, що Росія веде війну з Україною, російські хакери та кіберзлочинці постійно нападають на неї в Інтернеті.

Кібератаки можуть бути спрямовані на різні частини інфраструктури України, такі як енергетика, транспорт, фінанси, медіа, урядові установи та інші важливі системи. Ці атаки мають на меті завдати шкоди, порушити систему та викликати паніку серед населення.

DDoS-атаки є одним із найпоширеніших типів кібератак, коли хакери надсилають велику кількість штучного трафіку на цільові сервери, що призводить до зупинки систем і веб-ресурсів. Зловмисники також можуть використовувати фішингові атаки, шкідливі програми, віруси та троянські програми, щоб отримати несанкціонований доступ до інформації або пошкодити системи.

Українські уряди, організації та громадяни повинні постійно бути насторожі та вживати заходів кібербезпеки. Це включає використання надійних паролів, регулярне оновлення програмного забезпечення, використання ефективних антивірусних програм і захист мережі від несанкціонованого доступу до комп’ютерів.

Особливу увагу слід приділяти навчанню кібербезпеці. Користувачі повинні бути обізнаними про потенційні загрози та знати, як розпізнати підозрілі повідомлення та посилання. Вони також повинні уникати передачі своєї особистої інформації ненадійним джерелам. Важливим є наявність ефективних механізмів реагування на кібератаки та співпраця зі спеціалістами з кібербезпеки. Випадки повинні бути швидко виявлені та відповідно реагувати. Важливо постійно спостерігати, вивчати інциденти та вдосконалювати заходи кібербезпеки на основі того, що ми знаємо [22].

У сучасному світі, де інформація є важливим ресурсом, знання про загрози кібератак і вжиття заходів для забезпечення кібербезпеки є важливими

компонентами. Захист національної безпеки, економічного зростання та стабільності України залежить від захисту її інфраструктури від кібератак. Для забезпечення надійного функціонування цифрового середовища та боротьби з кіберзагрозами необхідні постійні зусилля та співпраця всіх зацікавлених сторін [9].

Використання соціальних мереж та інтернет-платформ: Росія активно використовувала соціальні мережі, такі як Facebook, Twitter та YouTube, для поширення своїх пропагандистських повідомлень та впливу на громадську думку. Наприклад, були створені багато фейкових акаунтів та ботів, які поширювали дезінформацію та маніпулювали думкою користувачів. Це сприяло поширенню негативного ставлення до української влади та підтримки російської агресії.

Ці приклади свідчать про те, як інформаційна війна взаємодіє з військовими діями, створюючи сприятливі умови для агресії та дестабілізації ситуації в Україні. Ця взаємодія є складною та динамічною, впливаючи на сприйняття конфлікту як на внутрішньому рівні, так і на міжнародній арені.

2.3. Роль ЗМІ у російсько-українській інформаційній війні

Роль ЗМІ (Засобів масової інформації) у російсько-українській інформаційній війні є значною. Росія активно використовувала свої медіа ресурси для поширення пропаганди, маніпулювання громадською думкою та впливу на сприйняття конфлікту як в Україні, так і за її межами. Основні аспекти ролі ЗМІ в цьому контексті включають:

Поширення дезінформації: Російські ЗМІ активно використовувалися для поширення фейкових новин та дезінформації про події в Україні. Це включало вигадані історії, маніпуляції фактами та спотворення подій, що створювало спотворений образ конфлікту та підтримувало російську пропаганду [23].

Створення пропагандистських наративів: Російські ЗМІ активно формували пропагандистські наративи, щоб створити певний образ подій та акторів конфлікту.

Це включало демонізацію української влади та силових структур, підтримку російської агресії та створення ілюзії широкої підтримки російським діям.

Залучення «експертів» та коментаторів: Російські ЗМІ активно залучали «експертів» та коментаторів, які підтримували російську версію подій та давали коментарі, що відповідали їхній пропаганді. Це надавало вигляд об'єктивності та додавало ваги російським позиціям.

Використання медіа для психологічного впливу: Російські ЗМІ використовувалися для психологічного впливу на населення України. Це включало створення загрозливого образу ворога, розповсюдження страху та невпевненості, а також підтримку розділу та конфлікту між українцями [9].

Заперечення правдивої інформації: Російські ЗМІ активно заперечували правдиву інформацію, що суперечила їхнім наративам. Вони намагалися відхилити критику та обвинувачення, змінювати факти та встановлювати власну версію подій.

Роль ЗМІ у російсько-українській інформаційній війні полягала у формуванні негативного образу України, української влади та українських силових структур, а також впливу на громадську думку в Україні та за її межами. Використання ЗМІ стало ефективним інструментом для маніпулювання інформацією та формування сприятливої обстановки для російської агресії.

Україна також використовувала ЗМІ у контексті інформаційної війни проти Росії. Однак, в порівнянні з Росією, ресурси та можливості України були обмежені. Незважаючи на це, українська влада та українські ЗМІ вживали кілька заходів для протистояння російській пропаганді та дезінформації:

Розповсюдження правдивої інформації: Українська влада та ЗМІ намагалися широко розповсюджувати правдиву інформацію щодо подій, що відбувалися в Україні. Це включало надання достовірних фактів, статистики та свідчень, щоб спростувати фейкові новини, що поширювалися російськими ЗМІ.

Активна комунікація з міжнародними ЗМІ: Україна зверталася до міжнародних ЗМІ та журналістів, щоб передати правдиву картину конфлікту та залучити увагу світової спільноти до російської агресії. Були організовані прес-конференції, інтерв'ю

та інші заходи, що допомагали заявити про свою позицію та протистояти російській пропаганді.

Розвиток власних медіа ресурсів: Україна поступово розвивала власні медіа ресурси, включаючи телебачення, радіо та онлайн-платформи, які ставили перед собою мету передати правдиву інформацію та боротися з російською пропагандою. Наприклад, було створено телеканал «Україна» та онлайн-платформу «Hromadske.tv».

Сприяння громадському журналістиці: Україна підтримувала громадські журналістські ініціативи, що допомагали висвітлювати реальну ситуацію в країні та опротестовувати дезінформацію. Були організовані тренінги та підтримка незалежних журналістських організацій [9].

Контрпропаганда та демаскування: Україна активно використовувала контрпропаганду та демаскування російської пропаганди. Через аналіз та розкриття фейкових новин, маніпуляцій та спотворень, Україна намагалася показати справжній образ російської інформаційної війни та невідповідність її тверджень реальності.

Дослідження показало, що сторони конфлікту активно використовують такі інформаційні технології та методи, як кібератаки, дезінформація, пропаганда та соціальні мережі. Ці інструменти розпалюють конфлікти в людських стосунках, змінюють уявлення громадськості та знижують довіру до ЗМІ.

Оскільки кожна сторона використовує інформаційні засоби для досягнення своїх військових цілей, взаємодія між інформаційною війною та військовими діями була тісно пов’язана. Інформаційна війна змінила внутрішню та зовнішню політику країн, громадську думку та міжнародну підтримку.

Це свідчить про те, що інформаційне протиборство впливає на громадську думку та стратегію війни. Дезінформація та маніпуляції можуть зіпсувати воєнні операції, надаючи перевагу одній стороні конфлікту. ЗМІ відіграють важливу роль у російсько-українській інформаційній війні через їхню важливість як засобу впливу та маніпуляції громадською думкою. ЗМІ використовуються для стратегічних цілей,

включаючи поширення дезінформації, створення образів ворога та створення сприятливої атмосфери [23].

Інформаційна війна в російсько-українській війні впливає на суспільство, воєнні операції та міжнародні відносини. Використання різноманітних інформаційних технологій і методів маніпулювання громадською думкою та створення образів ворога вимагає відповідної уваги та дій, щоб протидіяти цим загрозам. Розуміння ролі ЗМІ, взаємодії з військовими діями та використання інформаційних технологій є важливими для розробки ефективних планів і заходів забезпечення інформаційної безпеки в умовах конфлікту.

РОЗДІЛ 3
ІНФОРМАЦІЙНА БЕЗПЕКА ЯК СКЛАДОВА ІНФОРМАЦІЙНОГО ПРОТИБОРСТВА

3.1. Стратегії та принципи інформаційної безпеки

Стратегії та принципи інформаційної безпеки є важливими складовими інформаційного протиборства в контексті російсько-української війни. Основна мета інформаційної безпеки полягає у захисті інформаційного простору від небажаного доступу, маніпуляцій та дезінформації [24]. Ось декілька стратегій та принципів, що використовуються в інформаційній безпеці:

Концепція повного циклу інформаційної безпеки: Ця стратегія передбачає застосування комплексного підходу до інформаційної безпеки, що охоплює всі етапи циклу інформації – збір, обробка, передача та збереження. Вона забезпечує захист інформації на кожному етапі, починаючи від її джерел та закінчуючи кінцевими отримувачами.

Принцип обмеження доступу: Відповідно до принципу обмеження доступу конфіденційна та важлива інформація повинна бути доступна лише авторизованим особам. Це досягається за допомогою контролю користувачів, обмеження прав доступу, використання шифрування та інших технологічних заходів, які запобігають несанкціонованому доступу до інформації. Крім того, основний принцип включає в себе впровадження систем аутентифікації та авторизації, використання різних рівнів доступу та ролей користувачів, управління розподілом прав доступу, регулярне оновлення паролів і відстеження дій користувачів для виявлення потенційних порушень.

Моніторинг і реагування: цей принцип включає систематичний моніторинг інформаційного простору з метою виявлення потенційних загроз і атак на інформаційну безпеку. Для досягнення цієї мети використовуються системи моніторингу мережі, системи виявлення вторгнень і спеціалізовані програми.

Вживаються швидкі та ефективні заходи для ліквідації цієї загрози та відновлення інформаційної безпеки, якщо виявляється потенційна загроза або інцидент. Блокування атак, відновлення інформаційних систем та інші заходи, спрямовані на мінімізацію збитків від інциденту, є прикладами таких заходів.

Освіта та свідомість є важливими для захисту інформації від загроз, маніпуляцій і дезінформації. Це досягається шляхом надання людям правильної інформації та навичок безпечного користування нею. Основна мета полягає в тому, щоб підвищити обізнаність користувачів, щоб вони могли розуміти та ефективно реагувати на потенційні загрози. Уроки безпеки комп'ютера, включаючи використання надійних паролів, уникнення підозрілих посилань і небезпечних файлів, є життєво важливими для навчання та свідомості користувачів. Забезпечення освіти та свідомості є важливим кроком у захисті інформації та запобіганні багатьом інцидентам [1].

Основними принципами інформаційної безпеки є співпраця та партнерство. Це може включати співпрацю з приватним сектором, громадським суспільством, іншими країнами та міжнародними організаціями. Ефективний захист інформаційної безпеки можна досягти шляхом передачі інформації про загрози та кращих практик, спільної боротьби з дезінформацією та координації заходів. Розглядаючи загрози, обмінюючись досвідом і розробляючи плани для покращення інформаційного середовища, урядові органи, приватний сектор, громадські організації та активісти співпрацюють. Це сприяє розвитку інформаційного простору, стійкості та впровадженню нових політик і технологій, а також виявленню нових загроз.

Ці стратегії та принципи допомагають забезпечити ефективний захист інформації в контексті інформаційної війни. Використання комплексного підходу, обмеження доступу, моніторинг та реагування, освіта та свідомість, а також співпраця та партнерство створюють основу для забезпечення інформаційної безпеки та ефективного протистояння дезінформації та маніпуляціям у російсько-українській війні.

3.2. Технології та інструменти інформаційної безпеки

Технології та інструменти інформаційної безпеки відіграють важливу роль у протистоянні загрозам інформаційної безпеки та захисті від дезінформації. Ось деякі з них:

Криптографія: Криптографія забезпечує конфіденційність, цілісність і доступність інформації, що є важливим компонентом інформаційної війни. Це область знань, яка досліджує способи захисту інформації від несанкціонованого доступу та маніпуляцій. Дані, які зашифровані за допомогою криптографії, можуть прочитати або зрозуміти лише особи, які мають дозвіл [5].

Шифрування є важливою частиною криптографії в інформаційній війні. Процес шифрування, який називається шифротекстом, використовує ключі та математичні алгоритми, щоб зробити звичайний текст незрозумілим. Це дозволяє зберігати дані в зашифрованому вигляді, який не може бути відкритий для людей, які не мають відповідного ключа. Завдяки використанню шифрування важливі дані можна захистити від перехоплення та несанкціонованого доступу.

Крім шифрування, криптографія також включає аналіз і розшифрування повідомлень, які були зашифровані, що називається криптоаналізом. У цьому процесі потрібні навички розгадування шифру та виявлення слабких місць у системі шифрування. Криптоаналітики розкривають шифри та отримують доступ до зашифрованої інформації за допомогою різних методів і алгоритмів. Криптоаналіз використовується під час інформаційної війни для проникнення в захищені системи та отримання конфіденційної інформації [12].

Крім того, криптографія включає створення нових алгоритмів і шифрів, які мають високу стійкість і надійність. Оскільки з розвитком технологій з’являються нові небезпеки та методи зламу шифрів, це постійний процес. Криптографи розробляють нові алгоритми шифрування, які важко розкрити навіть за допомогою сучасних обчислювальних можливостей. Це допомагає захистити особисту інформацію від несанкціонованого доступу.

В інформаційній війні криптографія є життєво важливою для захисту та контролю над інформацією. Вона допомагає захистити конфіденційність спілкування, запобігти маніпуляції даними та зберегти цілісність даних. Споживачі можуть взаємодіяти без ризику витоку конфіденційної інформації або перехоплення її третіми особами завдяки протоколам і методам, які шифруються.

Застосування криптографії в інформаційній війні вимагає не лише технічних навичок, але й аналітичних навичок і стратегічного мислення. Криптографічні методи повинні постійно оновлюватися та вдосконалюватися, щоб захистити інформацію від зовнішніх загроз. Крім того, важливо розуміти, що криптографія не є універсальним способом захисту інформації під час інформаційної війни [20].

Антивірусні програми: В інформаційній війні антивірусні програми відіграють важливу роль у захисті від шкідливих впливів та кібератак. Вони служать своєрідним «захистом» комп'ютерних систем і мереж, оскільки вони здатні виявити, блокувати та видалити шкідливі програми, віруси, троянських коней та інші загрози, які можуть пошкодити, викрасти чи знищити цінну інформацію.

Антивіруси працюють, скануючи файли та системи, щоб знайти відомі шаблони зловмисних програм. Вони знаходять підозрілі дії, аналізують поведінку програм і вживають заходів для їх припинення та видалення. Деякі антивірусні програми також використовують покращені технології штучного інтелекту та машинного навчання, щоб виявити нові, раніше невідомі загрози.

Антивірусні програми спрямовані на забезпечення безпеки даних і запобігання поширенню шкідливих програм. Вони перевіряють файли, електронні листи, завантаження з Інтернету та інші джерела на наявність вірусів та інших небезпек. Антивірусна програма реагує на загрозу, блокуючи доступ до шкідливого контенту, видаляючи заражені файли або карантинуючи їх.

Антивірусні програми постійно оновлюються, щоб протистояти зростаючим загрозам інформаційної війни. Розробники регулярно випускають оновлення, які включають нові алгоритми виявлення та сигнатури вірусів. Це дозволяє антивірусним

програмам ефективно реагувати на нові загрози та створювати надійний захист інформаційних систем [10].

Важливо пам’ятати, що антивірусна програма є лише одним із компонентів складної стратегії інформаційної безпеки. Крім встановлення та оновлення антивірусного програмного забезпечення, також необхідно дотримуватися інших заходів безпеки, таких як використання надійних паролів, регулярне оновлення операційної системи та інших програм, використання надійних паролів і ретельне перевіряння вкладених файлів і посилань перед їх відкриттям.

Узагалі, наявність актуального антивірусного програмного забезпечення надзвичайно важлива для боротьби зі шкідливими програмами та захисту від кібератак. Воно підвищує надійність комп’ютерних систем, запобігає пошкодженню даних і втраті конфіденційної інформації. Для захисту від загроз в інформаційній війні важливою частиною стратегії кібербезпеки є правильний вибір, встановлення та регулярне оновлення антивірусного програмного забезпечення.

Фаєрволи: Фаєрволи відіграють важливу роль у захисті та контролі інформаційного простору. Фаєрвол - це програмно-апаратний комплекс, який контролює передачу даних і перешкоджає незаконному доступу до мережі. Фаєрволи використовуються під час інформаційної війни для фільтрації, спостереження та захисту інформації від небажаних впливів, зокрема від атак, дезінформації та кібершпигунства.

Вони дозволяють створювати правила та політики щодо доступу до інформаційних ресурсів, перехоплювати та аналізувати трафік у мережі, знаходити та блокувати небажані джерела або шкідливий контент. Фаєрволи забезпечують цілісність мережі та захищають важливі дані від несанкціонованого доступу. Крім того, вони можуть бути інструментом для виявлення та реагування на атаки, спрямовані на порушення інформаційної безпеки.

Також можуть бути використані під час інформаційної війни для виявлення та блокування таких методів протиборства, як розповсюдження дезінформації, хакерські атаки та кібершпигунство. Вони дають можливість створювати правила

фільтрації, які враховують різні елементи, такі як джерела інформації, ключові слова, мережеві протоколи тощо. Це забезпечує більшу безпеку інформаційного простору та знижує ризик поширення шкідливих ефектів.

Ще вони є життєво важливими для захисту від деструктивних атак, таких як DDoS-атаки, які спрямовані на заволодіння контролем над системою та перевантаження мережевих ресурсів. Вони здатні ідентифікувати та блокувати надмірний трафік, що допомагає підтримувати доступність інформаційних ресурсів і забезпечити безперебійну роботу мережі.

Здатність фаєрволів залишатися оновленими та адаптивними є важливою характеристикою. Зважаючи на швидкий розвиток технологій і зростання небезпек для інформаційної безпеки, фаєрволи повинні постійно оновлювати свої правила та політики фільтрації, а також використовувати найновіші методи виявлення загроз. Це забезпечує високий рівень безпеки інформаційного простору та ефективно захищає мережу від нових типів атак.

Підводячи підсумок, фаєрволи в інформаційній війні є важливою частиною захисту інформаційного простору. Вони захищають передачу даних від небажаних впливів і атак, а також допомагають виявляти та реагувати на загрози інформаційної безпеки. Для забезпечення безпеки та стабільності інформаційного середовища важливим є створення та постійне оновлення фаєрволів [17].

Системи виявлення вторгнень (Intrusion Detection Systems, IDS): Ідентифікація проникнення (IDS) — це апаратні або програмні засоби, призначені для виявлення незаконних або шкідливих дій у комп’ютерних системах та мережах. Ці системи можуть аналізувати трафік мережі, знаходити вторгнення та сповіщати про потенційні атаки та порушення безпеки.

Ідентифікація проникнення (IDS) є важливою частиною виявлення та реагування на загрози інформаційної війни. Вони допомагають виявити несанкціонований доступ до комп’ютерних систем, а також виявити атаки, спрямовані на викрадення, пошкодження або знищення цінної інформації.

Ідентифікація проникнення (IDS) може виявити розповсюдження шкідливих програм, зловживання привілегіями та незвичайну або підозрілу активність у мережі.

Аналіз мережевого трафіку є важливою частиною роботи ідентифікації проникнення. Вони шукають аномальні активності, певні сигнатури атак або зміни в поведінці мережі за допомогою різних методів і алгоритмів. Такий аналіз може включати перехоплення, аналіз і інтерпретацію пакетів даних, що пересилаються по мережі. Крім того, ідентифікація вторгнень може використовувати статистичні моделі, експертні правила та бази знань [4].

Реакція на виявлені вторгнення є одним із основних завдань систем виявлення вторгнень. Вони можуть виконувати інші стандартні процедури безпеки, блокувати атаки та сповіщати адміністраторів про події. Дані про вторгнення зазвичай збираються системами виявлення вторгнення, які можна використовувати для подальшого аналізу, покращення системи безпеки та виявлення нових загроз.

IDS стала важливим інструментом у сучасному контексті інформаційної війни, щоб захистити інформаційний простір від шкідливих атак і вторгнень. Вони сприяють забезпеченню конфіденційності, цілісності та доступності інформації, що є важливими компонентами інформаційної війни. IDS ідентифікує вторгнення, сповіщає про загрози та допомагає вживати заходів для нейтралізації атак. Вони є важливим компонентом складних стратегій інформаційної безпеки та протиборства в сучасному цифровому світі.

Оскільки загрози безпеці постійно зростають і розвиваються, системи виявлення та виявлення є постійним процесом. Компанії, урядові структури та організації постійно вдосконалюють свої системи виявлення вторгнень, щоб вони могли адаптуватися до нових типів атак і загроз. Важливо постійно оновлювати бази знань і сигнатури, щоб системи виявлення вторгнень могли ефективно виявляти нові атаки та шкідливі програми.

Загалом, системи виявлення вторгнень є життєво важливим інструментом, який необхідний для захисту від загроз, які виникають в інформаційній війні. Вони сприяють забезпеченню безпеки інформаційного простору та допомагають зберегти

цілісність, конфіденційність та доступність важливих даних, а також забезпечують виявлення та реагування на атаки.

Системи управління ідентифікацією та доступом (Identity and Access Management Systems, IAM): Ці системи контролюють доступ користувачів до різних ресурсів і інформації на основі їх ідентифікації та прав доступу. Вони дозволяють забезпечити обмеження доступу та захистити інформацію від несанкціонованого використання.

Моніторинг та аналітика: У сучасній війні моніторинг і аналітика є важливими компонентами стратегії протиборства. Систематичне спостереження, збору, аналізу та інтерпретації інформації з різних джерел і медіа є метою цих процесів [25].

Постійне відстеження різноманітних джерел інформації, таких як ЗМІ, соціальні мережі, веб-сайти, блоги та інші медіа-канали, відоме як моніторинг. Збір, систематизація та організація даних для подальшого аналізу є частиною цього процесу. Визначення ключових тем, акторів і трендів, що домінують у інформаційному просторі, є важливим етапом моніторингу.

Аналітика в інформаційній війні передбачає ретельне вивчення зібраних даних, їхнє розуміння та встановлення зв’язків між різними частинами інформації. Аналітики визначають патерни, тренди, стратегії та тактики, які сторони конфлікту використовуються для досягнення своїх інформаційних цілей. Вони відстежують зміни в поведінці акторів, поширення дезінформації, вплив медіа та інші елементи, які можуть вплинути на тривалість конфлікту.

Використання різноманітних методів і інструментів, таких як статистичний аналіз, мовний аналіз, візуалізація даних, соціальна мережева аналітика та інші, є необхідним для ефективної аналітики інформаційної війни. Аналітичні групи ретельно вивчають інформацію, яку вони зібрали, роблять припущення, створюють гіпотези та розробляють стратегії протиборства.

Забезпечити швидкість і точність збору та аналізу інформації є важливим компонентом моніторингу та аналітики в інформаційній війні. Застосування

автоматизованих систем і інструментів штучного інтелекту дозволяє забезпечити високу якість аналізу та виявлення важливих відмінностей, прискорюючи ці процеси.

Усе сказане свідчить про те, наскільки важливо моніторити та аналізувати в інформаційній війні. Цей тип процедур допомагає розкрити стратегії протиборства сторін конфлікту, допомогти зрозуміти їхні мотиви та цілі, а також допомогти приймати розумні рішення щодо взаємодії з інформаційним простором. Зміцнення інформаційної безпеки та ефективне протидія дезінформації залежать від постійного розвитку моніторингу та аналітики.

Експертні системи та штучний інтелект: Штучний інтелект (ШІ) і експертні системи відіграють важливу роль у сучасній інформаційній війні, оскільки вони допомагають сторонам конфлікту в аналізі, обробці та поширенні інформації з метою досягнення своїх цілей. Інформаційні агентства та військові організації отримали нові можливості завдяки цим технологіям, які дозволяють їм маніпулювати інформаційним простором і впливати на громадську думку [25].

Експертні системи є комп'ютерними програмами, які використовують логічні алгоритми та експертні знання для прийняття рішень у певній галузі. Експертні системи можуть використовуватись під час інформаційної війни для аналізу даних, виявлення тенденцій і шаблонів, а також ідентифікації дезінформації та маніпуляцій. Вони здатні автоматизувати процеси обробки інформації та швидко визначати впливові особи або організації.

Хоча, штучний інтелект охоплює широкий спектр технологій, які дозволяють комп'ютерам виконувати завдання, які зазвичай потребують людського інтелекту, а також «навчатись». Штучний інтелект може бути використаний в інформаційній війні для автоматизації процесів збору та аналізу інформації, виявлення шаблонів дезінформації, розпізнавання маніпулятивних технік і прогнозування розвитку подій.

Створення алгоритмів і програм, які здатні розпізнавати фейкові новини та дезінформацію, є одним із прикладів застосування експертних систем і штучного інтелекту в інформаційній війні. Ці системи використовують моделі навчання, де комп'ютери «навчаються» розрізняти правду від брехні. Вони оцінюють

достовірність інформації за допомогою різних критеріїв, включаючи джерело, стиль написання та історію публікацій.

Штучний інтелект і експертні системи можуть бути використані для аналізу соціальних мереж і медіа-платформ, щоб виявити та відстежувати маніпулятивні кампанії. Вони здатні аналізувати великі кількості даних, знаходити зв'язки та впливові групи, визначати тенденції та прогнозувати реакцію громадськості на конкретні події або повідомлення. Необхідно пам'ятати, що ШІ та експертні системи не є панацеєю від усіх проблем, пов'язаних з інформаційною війною. Вони недосконалі та можуть помилитися. Приватність даних і ймовірність зловживання владою є моральними проблемами, пов'язаними з використанням цих технологій.

І взагалі експертні системи та ШІ відіграють важливу роль в інформаційній війні, оскільки вони допомагають сторонам конфлікту аналізувати, розпізнавати та реагувати на маніпуляції, які відбуваються в інформаційному просторі. Хоча вони пропонують нові можливості для ефективного контролю та впливу на громадську думку, їх слід використовувати відповідно до моралі та закону.

Ці технології та інструменти є лише деякими засобами, які використовуються в інформаційній безпеці. Вони сприяють виявленню, захисту та реагуванню на загрози інформаційної безпеки, але вимагають постійного вдосконалення та адаптації до змінюючогося інформаційного середовища.

3.3. Розвиток медіаграмотності та сприйняття інформації

Розвиток медіаграмотності та сприйняття інформації є важливими аспектами інформаційної безпеки. Особи з високим рівнем медіаграмотності мають навички критичного мислення, вміння аналізувати та оцінювати інформацію, розрізняти факти від дезінформації та маніпуляцій. Ось деякі аспекти розвитку медіаграмотності та сприйняття інформації:

Критичне мислення: Важливо навчити людей аналізувати та оцінювати інформацію з різних джерел. Це включає перевірку достовірності джерел, перехресну

перевірку інформації, розпізнавання маніпуляційних та психологічних технік. Розвиток критичного мислення є життєво важливим для здатності розрізняти правдиву, перекручену чи неправдиву інформацію в сучасному інформаційному просторі, де маніпуляція та дезінформація стають все поширенішими.

Критичне мислення означає здатність аналізувати інформацію з різних джерел, перевіряти її достовірність і визначати потенційні причини, що сприяють цьому. Це означає, що важливо розглядати інформацію критично та запитувати себе: «звідки вона взята? Чи відомі вони? Чи є інші джерела, які підтверджують цю інформацію? Чи відповідає вона здоровому глузду та логіці?» [9].

Здатність ідентифікувати маніпулятивні стратегії та підходи, що використовуються для впливу на громадську думку, є важливим компонентом критичного мислення. Це означає, що ми повинні бути свідомими того факту, що певні джерела інформації можуть намагатися маніпулювати або впливати на наші думки та переконання. Аналіз засобів виразності, використання емоційного впливу, вигідне підкреслення певних фактів або нехтування іншими, а також застосування стереотипів або спрощень є частиною здатності ідентифікувати такі методи [9].

Крім того, критичне мислення вимагає розуміння різних медійних форматів і їх впливу. Зокрема, розуміння засобів виразності, які використовуються для підкреслення певних точок зору або зміни нашого сприйняття, є важливим, щоб відрізнити факти від оцінок або коментарів. Наприклад, зображення, відеоматеріали чи заголовки можуть містити методи, які впливають на нашу емоційну реакцію та сприйняття інформації. Таким чином, підвищення обізнаності про такі методи та здатність їх розпізнавати є життєво важливими. Крім того, це передбачає здатність аналізувати контекст інформаційних повідомлень і розуміти потенційні причини їх створення. Інформація може бути використана для досягнення певних цілей або впливу на громадську думку, тому важливо визначити, чи передає вона об’єктивну інформацію, чи має приховану політичну спрямованість або агенду. Це означає, що ми повинні розуміти контекст, у якому поширюється інформація, і знати, які можуть бути мотивації для конкретного повідомлення.

Зважаючи на це, критичне мислення є важливою здатністю, яка допомагає нам оцінювати та розуміти інформацію, яка надходить до нас у сучасному світі, який переповнений різноманітною інформацією та неправдивими фактами. Воно вимагає таких якостей, як уважність, обережність і здатність аналізувати; ці якості є життєво важливими для того, щоб стати більш обізнаними та критичними громадянами.

Розуміння медійних жанрів: Інформаційна війна залежить від розуміння жанрів медіа. Жанри медіа визначають спосіб розповсюдження та представлення інформації громадськості. У інформаційній війні різноманітні види медіа стають ефективним інструментом маніпуляції, впливу на громадську думку та формування фальшивих уявлень про учасників конфлікту та події.

Новини, коментарі, аналітика, репортажі, інтерв'ю, документальні фільми, есе та інші форми інформації є частиною медійних жанрів. Кожен із цих жанрів має свої особливості та використовується для досягнення певних цілей щодо впливу на аудиторію.

Наприклад, основним засобом розповсюдження інформації про поточні події є жанр новин. Вони повинні бути об'єктивними, заснованими на фактах і мати різні точки зору на ситуацію. Тим не менш, під час інформаційної війни інформація може бути спотворена або змінена з метою пропаганди та маніпуляції. Наприклад, через використання нечесних заголовків, вибіркове наведення фактів або використання неперевірених джерел.

Коментарі та аналітика використовуються для пояснення та інтерпретації подій, а також для висловлення думок і позицій експертів. Інформаційна війна може використовувати ці жанри для поширення власної пропаганди, впливу на громадську думку та формування позицій.

Документальні фільми та репортажі створені для того, щоб надати правдиву картину подій і передати реальну інформацію про те, що відбувається. Тим не менш, під час інформаційної війни ці жанри можуть бути використані для зміни точки зору, зосередження на певних елементах або зміни фактів, щоб вплинути на те, що бачать глядачі.

Для того, щоб критично мислити та аналізувати інформацію, яку ми отримуємо, важливо розуміти жанри, які використовуються в медіа. Це допомагає виявити потенційні маніпуляції та відрізняти об’єктивну інформацію від спотвореної. Створення медіаграмотності та розуміння різних жанрів медіа є важливими навичками для сучасного суспільства, які дозволяють людям стати більш критичними та самосвідомими споживачами інформації.

Вміння перевіряти інформацію: В епоху інформаційної війни надзвичайно важливо мати здатність перевіряти інформацію. Інформаційний простір переповнений різноманітними повідомленнями та джерелами, тому важливо мати здатність відрізняти правдиву інформацію від фейкової, аналізувати її достовірність і джерела, а також розуміти потенційні маніпуляції та приховані мотиви.

Важливо, перш за все, ретельно перевірити джерела інформації. При оцінці придатного матеріалу важливо звернути увагу на авторитетність джерела. Перевірте, чи має він відповідну освіту та досвід у цій галузі. Ретельно досліджуйте репутацію автора або видавця інформації, шукайте незалежні відгуки та коментарі.

Другим кроком є перевірка самих даних. Для цього потрібно шукати докази та перевіряти інформацію. Спирайтеся на різні джерела, щоб отримати підтвердження. Перевірте, чи подана інформація підтверджується фактичними даними, статистикою або доказами. Оскільки контекст, у якому була оприлюднена інформація, може вплинути на її розуміння, будьте уважні.

Вивчення способів маніпулювання та спотворення інформації є третім аспектом. Зверніть увагу на використання загальноприйнятих стереотипів, перекручення фактів або відсутність об’єктивності в повідомленнях. Будьте уважні до сенсаційних заголовків і заяв, які можуть приховувати недостовірну інформацію або недостатню аргументацію.

Зверніть увагу на власний критичний підхід. Завжди запитуйте та досліджуйте інформацію з різних точок зору. Пам’ятайте, що навіть найавторитетніші джерела можуть помилитися. Застосовуйте здоровий глузд і логічне мислення, щоб критично ставитися до інформації.

Та будьте уважні до контексту та цілей інформаційних повідомлень. Зверніть увагу на потенційні ідеологічні, економічні чи політичні тенденції інформації. Ви повинні подумати про те, які можуть бути причини для розповсюдження певної інформації, а також хто може отримати вигоду від її розповсюдження [9].

Останнє, але не менш важливе, пам’ятайте, що розвиток медіаграмотності є постійним процесом. Для свідомого споживання інформації необхідно постійно поглиблювати свої знання, практикувати свої навички та отримувати нові навички. Будьте відкритими до нових джерел інформації, навчайтеся відрізняти правду від брехні та практикуйте критичне мислення в повсякденному житті.

Самоконтроль та саморегуляція: Ці поняття охоплюють набір методів, стратегій і навичок, які допомагають ефективно взаємодіяти з інформацією, розрізняти правду від дезінформації та запобігати поширенню небажаної та шкідливої інформації.

Перш за все, самоконтроль означає здатність свідомо керувати своїми діями та реакціями на інформацію. Це включає бути уважним споживачем інформації, перевіряти достовірність інформації та переконатися, що вона об’єктивна, перш ніж робити висновки або поширювати її. Самоконтроль також передбачає вміння стримувати емоції та не розгублюватися під час отримання інформації, що може призвести до маніпуляції або негативної реакції.

Саморегуляція інформації є другим важливим компонентом. Це означає, що ви повинні мати контроль над тим, як інформація поширюється та розповсюджується з точки зору її цінності, достовірності та моральності. Це передбачає не лише здатність уникати поширення неперевірених чуток або фейкових новин, але й здатність критично оцінювати можливі наслідки поширення інформації на суспільство та міжнародні відносини. Вибір правильних способів поширення інформації, а також дотримання стандартів журналістської етики та відповідального відношення до інформації є важливою частиною саморегуляції. В інформаційній війні самоконтроль і саморегуляція інформації є життєво важливими для збереження інформаційної безпеки та створення об’єктивного та розумного інформаційного середовища.

Це вимагає не лише особистих зусиль кожного громадянина, але й розвитку медіаграмотності, саморегуляції в медіаорганізаціях і підтримки національних та міжнародних ініціатив щодо боротьби з дезінформацією та маніпуляціями в інформаційному просторі. Досягнення стійкого та впевненого інформаційного середовища, яке сприятиме розвитку суспільства та міжнародному співробітництву, є єдиним способом досягти цього [9].

Освіта та навчання: Важливо розвивати медіаграмотність та навички сприйняття інформації у формальній та неформальній освіті. Це може включати включення предмету «Медіаграмотність» у навчальні плани, проведення тренінгів та семінарів для громадськості та підтримку проектів, що спрямовані на розвиток медіаграмотності. Освіта та навчання є відіграє велику роль для розвитку медіаграмотності та взаєморозуміння в суспільстві. Забезпечити громадянам знання, навички та ресурси, необхідні для критичного мислення, ефективного реагування на маніпуляції та дезінформацію, є нашим обов’язком.

Розвиток медіаграмотності залежить від теоретичного навчання та практичних навичок. Вкрай важливо, щоб учні мали можливість активно застосовувати свої знання. Це можна досягти шляхом участі в симуляційних іграх або проектах, у яких вони можуть моделювати умови інформаційної війни та розробляти тактики боротьби. Такі практичні завдання допомагають учням розвивати навички критичного мислення та прийняття рішень у ситуаціях інформаційного протиборства.

Тим не менш, освіта та навчання в інформаційній війні повинні виходити за межі навчальних закладів. Різноманітні освітні ініціативи та підходи можуть досягти мети поширення інформаційної грамотності серед населення. Наприклад, проведення публічних семінарів і тренінгів, створення навчальних матеріалів і посібників з медіаграмотності, а також співпраця з медіа організаціями для поширення правди та виявлення дезінформації.

Оскільки методи та стратегії протиборства постійно змінюються, навчання в інформаційній війні має бути постійним процесом. Важливо впроваджувати нові методи та ресурси для виявлення та боротьби з новими формами дезінформації та

маніпуляцій. Співпраця з іншими країнами та міжнародними організаціями також важлива для обміну досвідом і розробки спільних стратегій боротьби з інформаційним тероризмом.

Отже, розвиток медіаграмотності та підвищення свідомості громадян залежить від освіти та навчання в інформаційній війні. Це процес, який вимагає постійного вдосконалення та адаптації до змін, які відбуваються в середовищі медіа та інформації. Освіта та навчання є життєво важливими для побудови стійкого та здорового інформаційного простору.

Розвиток медіаграмотності та сприйняття інформації є важливим елементом інформаційної безпеки, оскільки він допомагає людям бути критичними споживачами інформації та захищає від маніпуляцій та дезінформації.

Дослідження показало, що сторони конфлікту активно використовують такі інформаційні технології та методи, як кібератаки, дезінформація, пропаганда та соціальні мережі. Ці інструменти розпалюють конфлікти в людських стосунках, змінюють уявлення громадськості та знижують довіру до ЗМІ.

Військові дії та інформаційна війна пов’язані, що свідчить про те, що інформаційне протиборство впливає на громадську думку та стратегію війни. Дезінформація та маніпуляції можуть зіпсувати воєнні операції, надаючи перевагу одній стороні конфлікту.

ЗМІ відіграють важливу роль у російсько-українській інформаційній війні через їхню важливість як засобу впливу та маніпуляції громадською думкою. ЗМІ використовуються для стратегічних цілей, включаючи поширення дезінформації, створення образів ворога та створення сприятливої атмосфери.

У російсько-українській війні інформаційна війна впливає на суспільство, воєнні операції та міжнародні відносини. Використання різноманітних інформаційних технологій і методів маніпулювання громадською думкою та створення образів ворога вимагає відповідної уваги та дій, щоб протидіяти цим загрозам. Розуміння ролі ЗМІ, взаємодії з військовими діями та використання

інформаційних технологій є важливими для розробки ефективних планів і заходів забезпечення інформаційної безпеки в умовах конфлікту.

ВИСНОВКИ

У даній науковій роботі, присвяченій підходам та методам інформаційної війни, були розглянуті різні аспекти цієї проблематики в контексті російсько-української війни, яка розпочалася у 2022 році.

Інформаційна війна стала невід'ємною складовою сучасного світу, де інформація є одним з найцінніших ресурсів. У світі, де люди користуються інтернетом, соціальними мережами та медіа платформами, інформаційна війна може мати серйозні наслідки для політики, соціальної сфери, економіки та культури.

Основними характеристиками інформаційної війни є використання різних каналів для передачі інформації, зміна світогляду та переконань громадськості, маніпулювання емоціями та дезінформація. Інформаційна війна може мати серйозні наслідки, такі як загострення міжнародних відносин, збільшення конфліктів та розкол у суспільстві.

Щоб захиститися від інформаційної війни, важливо бути критичним до отримуваної інформації та перевіряти її достовірність. Крім того, потрібно розвивати критичне мислення та критичний підхід до інформації, яку ми отримуємо, а також виховувати громадян, які мають здатність аналізувати та оцінювати інформацію. Важливо також розробляти та впроваджувати ефективні механізми захисту від дезінформації та інших форм інформаційної агресії.

Дослідження показало, що сторони конфлікту активно використовують різні інформаційні технології та методи, такі як кібератаки, дезінформація, пропаганда та соціальні мережі. Ці інструменти створюють напруженість у відносинах між людьми, змінюють світогляд громадськості та знижують довіру до ЗМІ.

Взаємодія між інформаційною війною та військовими діями була тісно пов'язана, оскільки кожна сторона використовувала інформаційні засоби для досягнення своїх військових цілей. Інформаційна війна впливала на внутрішню та зовнішню політику країн, формувала громадську думку, впливала на міжнародну підтримку та мобілізацію суспільства.

Це свідчить про те, що інформаційне протиборство впливає не лише на громадську думку, але й на стратегію та тактику війни. Дезінформація та маніпуляції можуть негативно вплинути на воєнні операції, надаючи перевагу одній стороні конфлікту. Важливість медіа як засобу впливу та маніпуляції громадською думкою підкреслюється роллю ЗМІ у російсько-українській інформаційній війні. ЗМІ використовуються для стратегічних цілей: поширення дезінформації, створення образів ворога та створення сприятливої атмосфери.

Загалом, інформаційна війна в російсько-українській війні впливає на суспільство, воєнні операції та міжнародні відносини. Використання різноманітних інформаційних технологій і стратегій маніпулювання громадською думкою та створення образів ворога вимагає відповідної уваги та дій, щоб протидіяти цим загрозам. Розробка ефективних стратегій і заходів забезпечення інформаційної безпеки в умовах конфлікту залежить від розуміння ролі ЗМІ, взаємодії з військовими діями та використання інформаційних технологій.

Дослідження показало, що сторони конфлікту активно використовують різні інформаційні технології та методи, такі як кібератаки, дезінформація, пропаганда та соціальні мережі. Ці інструменти створюють напруженість у відносинах між людьми, змінюють світогляд громадськості та знижують довіру до ЗМІ.

Інформаційна війна та військові дії взаємопов’язані, що свідчить про те, що інформаційне протиборство впливає не лише на громадську думку, але й на стратегію та тактику війни. Дезінформація та маніпуляції можуть негативно вплинути на воєнні операції, надаючи перевагу одній стороні конфлікту.

Важливість медіа як засобу впливу та маніпуляції громадською думкою підкреслюється роллю ЗМІ у російсько-українській інформаційній війні. ЗМІ використовуються для стратегічних цілей: поширення дезінформації, створення образів ворога та створення сприятливої атмосфери.

Загалом інформаційна війна в російсько-українській війні впливає на суспільство, воєнні операції та міжнародні відносини. Використання різноманітних інформаційних технологій і стратегій маніпулювання громадською думкою та

створення образів ворога вимагає відповідної уваги та дій, щоб протидіяти цим загрозам. Розробка ефективних стратегій і заходів забезпечення інформаційної безпеки в умовах конфлікту залежить від розуміння ролі ЗМІ, взаємодії з військовими діями та використання інформаційних технологій.

У сучасному світі, де інформація відіграє важливу роль у формуванні думок, інформаційна війна стає потужним інструментом впливу на політичні, соціальні та військові процеси. Розуміння підходів та методів інформаційного протиборства є критично важливим для розробки ефективних стратегій інформаційної безпеки, захисту суверенітету та національних інтересів. Продовження дослідження в цій галузі та розробка нових методик та підходів до протидії інформаційному протиборству є актуальними завданнями для подальшого розвитку наукової спільноти та практичного застосування в реальних умовах.

СПИСОК ВИКОРИСТАНИХ ДЖЕРЕЛ

1. Петрик В. М., Бедь В. В., Присяжнюк М. М. та ін. Інформаційно-психологічне протиборство: підручник. Видання друге перекладене, доповнене та перероблене. Київ: ПАТ «ВІПОЛ», 2018. 386 с.
2. Слюсаревський М. М. (ред.). Термінологічний словник російсько-української війни. Київ: НАПН України, 2022. С. 20.
3. Матеріали 2-ї міжнародної науково-практичної конференції Європейського науково-конгресу, 20-22 березня 2023, Мадрид.
4. Богдан А. І., Болтянська О. В., Гаврилова О. Г. та ін. Інформаційна війна: поняття, методи, інструменти. Смолій В. О. (ред.). Київ: НАДУ, 2015.
5. Головко О. В., Дмитрієва О. Г., Засаднюк А. М. та ін. Інформаційна війна: методи та прийоми. Київ: Видавничий дім «Ін Юре», 2018.
6. Авдєєнко Є. І., Головко О. В., Івасів О. М. та ін. Інформаційна війна: сутність, методи та захист. Авдєєнко Є. І. (ред.). Київ: Видавничий дім «Ін Юре», 2018.
7. Савчук І. Г. Інформаційна блокада. 2019.
8. Стаття «злом Equifax» на сайті New York Times URL: https://www.nytimes.com /2017/09/18/business/equifax-breach-federal-investigation.html (дата звернення 18.04.2023).
9. Кулеба Д. І. Війна за реальність, як перемагати у світі фейків, правд та спільнот. 2019. Київ: Видавничий дім «Київ-Могилянська Академія». С. 384.
10. Почепцов Г. Г. Сучасні інформаційні війни. Київ: Видавничий дім «Київ-Могилянська Академія», 2015.
11. Рижков М. Інформаційна війна // Політична енциклопедія. Левенець Ю. Шаповал Ю. та ін. Київ: Парламентське видавництво, 2011. С. 298.
12. Лазоренко О. А. Інформаційний складник гібридної війни Російської Федерації проти України: тенденції розвитку // Стратегічні пріоритети. — Національний інститут стратегічних досліджень, 2015.

13. Йозеф Геббельс уривок «Що поставлено на карту», Мюнхен: Центральне видавництво НСДАП, Німецький пропагандистський архів. 1944. URL: https://research.calvin.edu/german-propaganda-archive/goeb73.htm (дата звернення 17.04.2023).

14. Ткач В.Ф. Спецпропаганда як інформаційний складник гібридної війни Росії проти України // Стратегічні пріоритети. Національний інститут стратегічних досліджень, 2016.

15. Залєвська І., Удренас Г. Інформаційна безпека України в умовах російської військової агресії // Північноукраїнський правничий часопис. 2022. № 1. С. 20-26.

16. Стаття новин «Вокс Україна» про лабораторії в Україні URL: https://voxukraine.org/fejk-viktoriya-nuland-vyznala-shho-ssha-mayut-biolaboratoriyi-v-ukrayini (дата звернення 15.03.2023).

17. Косогов, О.М., Сірик, А.О. Завдання захисту національного інформаційного простору за досвідом ведення гібридної війни РФ на Сході України // Системи озброєння і військова техніка. 2017. С. 38-41.

18. 7 Заповідей російської пропаганди. Відео з сайту The New York Times. URL: https://www.nytimes.com/video/opinion/100000006188102/what-is-pizzagate.html

19. BRIEFING ДСЄП Дослідницька служба Європейського парламенту. Автор: Якуб Пшетачник із Сімоною Тарповою. Дослідницька служба євродепутатів PE 733.549 – жовтень 2022 року. «UK Війна Росії проти України: хронологія кібератак».

20. Інформаційна війна: нові виклики та загрози / О.О. Трохименко, М.І. Винничук, О.І. Мах. 2018. С. 42.

21. Стругацький, Василь. Маніпулятивні практики на тлі гібридної війни: Філософський аналіз. Київ: ФОП Халіков Р.Х., 2018. С. 166.

22. Інформаційна війна: фактори, причини, наслідки / О.А. Рак, С.І. Шпот, І.В. Бардас [та ін.]; за ред. О.А. Рака. - Київ: Видавничий дім «Ін Юре», 2017.

23. Конах В. К. Сучасні тенденції в захисті національних медіапросторів від російської пропаганди // Стратегічні пріоритети. — Національний інститут стратегічних досліджень, 2016.

24. Копаль О.С., Павленко Ю.В., Філіпенко В.І. (ред.) Інформаційна війна: проблеми та перспективи. Київ: НАДУ, 2015.

25. Смолій В.О., Романова О.Г., Богдан А.І. (ред.) Інформаційна війна в Україні: проблеми та виклики. Київ: НАДУ, 2016.

26. Єрмоленко В. (Інтерньюз-Україна) Слова та війни: Україна в боротьбі з російською пропагандою: аналітичне видання. Київ: К.І.С., 2017.

27. Курбан О.В. Медіавіруси та їх використання як інформаційної зброї. Наукові записки (Українська академія друкарства), 2016, № 1, С. 267-271.

28. Lucas, Edward. The New Cold War: How the Kremlin Menaces both Russia and the West. London: Bloomsbury Publishing PLC, 2009.

29. Мельник М.І. «ІНФОРМАЦІЙНА БЕЗПЕКА ЯК СКЛАДОВА БЕЗПЕКИ В АВІАЦІЇ». 2017, С. 191-193.

30. Ожеван М.А., Шевченко О.В. Війна інформаційна. Українська дипломатична енциклопедія: У 2-х томах. Київ: Знання України, 2004.

31. Політологічний енциклопедичний словник. Укладачі: Л.М. Герасіна, В.Л. Погрібна, І.О. Поліщук та ін. Ред. М.П. Требін. Харків: Право, 2015.

32. Почепцов Г.Г. «Сучасні інформаційні війни». Київ-Могилянська Академія, 2015.

33. Курбан О.В. Теорія інформаційної війни: базові основи, методологія та понятійний апарат. Науковий журнал «ScienceRise», 2015, № 11 (1), С. 95-100.

34. Горбулін В.П., Додонов О.Г., Ланд Д.В. Інформаційні операції та безпека суспільства: загрози, протидія, моделювання. Київ: Інтертехнологія, 2009.

35. Ланде Д. В., Додонов В. О., Коваленко Т. В. Інформаційні операції у комп'ютерних мережах: моделювання, виявлення, аналіз. Київ: ІПМЕ НАН України, 2016, С. 198-201.

36. Владлєнова І. В., Кальницький Е.А. Особливості інформаційної війни як засобу вирішення соціально-політичних конфліктів: філософський аналіз. Психолого-педагогічні проблеми в освітньому процесі: зб. наук. ст. / Харк. нац. пед. ун-т ім. Г. Сковороді, Х., 2012, С. 19-25.

37. Сенченко М. І. Латентна світова інформаційна війна. 2014, С. 384.

38. В. А. Ліпкан, Ю. Є. Максименко, В. М. Желіхолський. «Інформаційна безпека України в умовах євроінтеграції». 2006, С. 280.

39. Інформаційно-комунікаційні аспекти міжнародної та національної безпеки: розвиток інформаційного суспільства: колективна монографія в 10-ти томах. Том 10. Київ: ВНЗ «Університет економіки та права »КРОК», 2013. С.342.

40. Панченко В. М. Інформаційні операції в асиметричній війні Росії проти України: підходи до моделювання. Інформація і право, 2014, № 3, С. 13-16.

41. Онопрійчук А. Підходи та методи інформаційного протиборства в Російсько-Українській війні. Політ. Сучасні Проблеми Науки. Міжнародні відносини: Тези доповідей XXII Міжнародної науково-практичної конференції здобувачів вищої освіти і молодих учених, Київ, 2022, Національний авіаційний університет / Редакційна колегія М.Луцький [та ін.]. – К.: НАУ, 2022. С. 142.

42. 1. Павлюх М. Модель національної журналістики для безпеки особи, суспільства, держави: російсько-українська кібервійна // Глобальний і регіональний виміри міжнародної безпеки : колективна монографія / Мальський Маркіян, Вовк Роман, Чайковський Марек та ін.; за ред. Маркіяна Мальського, Романа Вовка, Пйотра Байора. − Львів : ЛНУ імені Івана Франка, 2020. – С. 288 – 301.

43. Патлашинська І.В. Сучасна Російсько-Українська інформаційна війна: завдання, методи та особливості використання // Регіональні Студії. – 2022. – № 84.

44. Синчак Б. Прямоефірна інформаційна війна та російсько-українська війна 2022-го на медійному плацдармі // Український інформаційний простір. – 2022. – № 2(10). – С. 85-97.