МІНІСТЕРСТВО ОСВІТИ І НАУКИ УКРАЇНИ
ХАРКІВСЬКИЙ НАЦІОНАЛЬНИЙ ЕКОНОМІЧНИЙ УНІВЕРСИТЕТ ІМЕНІ СЕМЕНА КУЗНЕЦЯ

ФАКУЛЬТЕТ МІЖНАРОДНИХ ВІДНОСИН І ЖУРНАЛІСТИКИ

КАФЕДРА МІЖНАРОДНИХ ВІДНОСИН, ПОЛІТИЧНИХ НАУК І ПРАКТИЧНОЇ ФІЛОСОФІЇ

Рівень вищої освіти	Другий (магістерський)
Спеціальність	Міжнародні відносини, суспільні комунікації та регіональні студії
Освітня програма	Міжнародні відносини
Група	8.01.291.020.22.1

ДИПЛОМНА РОБОТА

на тему: «Інформаційні війни в міжнародних відносинах: еволюція та адаптація до сучасності»

Виконала: студенткаАлінаГМИРЯ

Керівник: к.політ.н., доц. Дмитро КОРОТКОВ

Рецензент: д. політ.н., доц. ВасильБУСЛЕНКО

Харків – 2023 рік

РЕФЕРАТ

Інформаційні війни в міжнародних відносинах: еволюція та адаптація до сучасності

Об’єктомдослідження.Об'єктом дослідження є інформаційні війни в міжнародних відносинах загалом.

Предметдослідження.Предметом дослідження є еволюція та адаптація інформаційних війн у міжнародних відносинах.

Мета дипломної роботи полягає в вивченні еволюції інформаційних війн у міжнародних відносинах та їх адаптація до сучасних умов. Дослідження спрямоване на аналіз впливу інформаційних війн на міжнародну арену та розробку стратегій протидії їм.

Задлядосягненняпоставленоїметидослідженнябулопоставленонаступнізавдання:

1. Вивчити історію та еволюцію інформаційних війн у міжнародних відносинах.
2. Оцінити сучасні методи та технології, які використовуються у цих війнах.
3. Розглянути вплив інформаційних війн на міжнародні конфлікти та відносини.
4. Розробити рекомендації щодо підвищення стійкості міжнародних відносин до інформаційних війн.

Актуальність.Тема "Інформаційні війни в міжнародних відносинах: еволюція та адаптація до сучасності" вкрай актуальна в сучасному світі з кількох ключових причин.

По-перше, інформаційні війни стали невід'ємною складовою сучасних міжнародних конфліктів і конкуренції між державами. Вони впливають на політичну стабільність, національну безпеку та міжнародні відносини. Способи інформаційного впливу, такі як дезінформація, кібератаки, психологічні операції та пропаганда, стають все більшими викликами для держав та міжнародних організацій.

По-друге, швидкий розвиток інформаційних технологій та глобалізація зробили інформаційний простір ключовим фактором у міжнародних відносинах. Інтернет, соціальні мережі та інші медіа платформи створюють можливості для розповсюдження інформації великими масштабами та в реальному часі, що підвищує ефективність інформаційних війн.

По-третє, інформаційні війни вимагають від держав та міжнародних акторів розвивати нові стратегії та політики щодо інформаційної безпеки та протидії дезінформації. Вони також ставлять питання про права та свободи в інформаційному просторі, а також про міжнародну співпрацю у цій сфері.

Отже, тема інформаційних війн у міжнародних відносинах залишається дуже актуальною і вимагає подальших досліджень та адаптації до сучасних реалій.

Новизна цієї роботи полягає в її комплексному підході до теми, який враховує історичний розвиток, сучасні технології та виклики, а також майбутні перспективи

інформаційних війн в міжнародних відносинах.

До основних результатів

Робота висвітлює актуальні виклики, пов'язані із зростанням інформаційних війн у міжнародних відносинах, та пропонує стратегії захисту та адаптації до цих явищ, сприяючи кращому розумінню цього питання і визначенню можливих наслідків для міжнародних відносин.

На основі дослідження було складено наступні рекомендації:

1. Розвивати і підсилити зусилля у сфері кібербезпеки та захисту інформаційних систем, особливо важливо для держав та організацій у міжнародних відносинах.
2. Сприяти підвищенню інформаційної грамотності населення та розвитку критичного мислення для здатності аналізувати інформацію, що надходить.
3. Розвивати міжнародну співпрацю та обмін інформацією між державами для спільної боротьби проти інформаційних загроз.
4. Залучити міжнародні організації та фахівців до дослідження інформаційних війн та розробки стратегій адаптації до їхніх нових форм і методів.
5. Розглянути можливість створення міжнародних норм та стандартів, спрямованих на регулювання інформаційних війн у міжнародних відносинах.

Дослідні методи: структурно-функціональний метод, аналіз літератури, емпіричні дослідження, та аналіз прикладів інформаційних війн у минулому та сучасності (історичний підхід), порівняльний метод, аналіз інформації та застосування дедуктивного методу, узагальнення за допомогою визначення причинно-наслідкових зв’язків..

Структура та обсяг дипломної роботи: дипломна робота складається зі вступу, трьох розділів, висновку, переліку спеціальної літератури (65 позицій), 4 таблиць, 2 схем й 1 додаток (14 позицій);обсяг роботибез додатків і перелікулітератури– 56 сторінок.

Ключові слова:інформація, інформаційна війна, конфлікт, міжнародні відносини, інформаційна політика, інформаційна безпека.

ABSTRACT

Information Wars in International Relations: Evolution and Adaptation to the Present

Object of research.The object of research is information wars in international relations in general.

The subject of research is the evolution and adaptation of information wars in international relations.

The purpose of the thesis is to study the evolution of information wars in international relations and their adaptation to modern conditions. The research is aimed at analyzing the impact of information wars on the international arena and developing strategies to counter them.

In order to achieve this research goal, the following tasks were set:

1. To study the history and evolution of information wars in international relations.
2. To evaluate modern methods and technologies used in these wars.
3. To consider the impact of information wars on international conflicts and relations.
4. Develop recommendations for increasing the resilience of international relations to information wars.

The topic "Information Wars in International Relations: Evolution and Adaptation to the Present" is extremely relevant in the modern world for several key reasons.

First, information wars have become an integral part of modern international conflicts and competition between states. They affect political stability, national security, and international relations. Methods of information influence, such as disinformation, cyberattacks, psychological operations, and propaganda, are becoming increasingly challenging for states and international organizations.

Second, the rapid development of information technology and globalization have made the information space a key factor in international relations. The Internet, social networks, and other media platforms create opportunities for the dissemination of information on a large scale and in real time, which increases the effectiveness of information wars.

Thirdly, information wars require states and international actors to develop new strategies and policies on information security and countering disinformation. They also raise questions about rights and freedoms in the information space, as well as international cooperation in this area.

Thus, the topic of information warfare in international relations remains very relevant and requires further research and adaptation to modern realities.

The novelty of this work lies in its comprehensive approach to the topic, which takes

into account historical development, modern technologies and challenges, as well as future prospects for information wars in international relations.

The paper highlights the current challenges associated with the growth of information wars in international relations and proposes strategies for protecting and adapting to these phenomena, contributing to a better understanding of this issue and identifying possible consequences for international relations.

Based on the study, the following recommendations were made:

1. Developing and strengthening efforts in the field of cybersecurity and protection of information systems is especially important for states and organizations in international relations.
2. Promote information literacy among the population and the development of critical thinking for the ability to analyze incoming information.
3. Develop international cooperation and information exchange between states to jointly combat information threats.
4. Involve international organizations and experts in the study of information warfare and the development of strategies for adapting to its new forms and methods.
5. Consider the possibility of creating international norms and standards aimed at regulating information wars in international relations

Research methods: structural-functional method, literature analysis, empirical research, and analysis of examples of information wars in the past and present (historical approach), comparative method, information analysis and application of the deductive method, generalization by determining cause and effect relationships.

The structure and scope of the thesis: the thesis consists of an introduction, three chapters, a conclusion, a list of special literature (65 items), 4 tables, 2 diagrams and 1 appendix (14 items); the volume of the work without appendices and references is 56 pages.

Keywords:information, information warfare, conflict, international relations, information policy, information security.

ЗМІСТ

ВСТУП

Актуальність теми. Тема інформаційних війн в міжнародних відносинах вкрай актуальна у сучасному світі. Інформаційні війни стали важливим інструментом впливу держав і недержавних акторів на світову політику, і вони постійно еволюціонують, адаптуючись до нових технологій та зміненого світового ландшафту.

У наш час інформаційні війни впливають на думки та погляди суспільства. Використання методів дезінформації та маніпулювання спотворює сприйняття подій, учасників конфлікту та ідеологічні перспективи, що може мати негативні наслідки для соціальної стабільності, міжнародних відносин і довіри до ЗМІ.

Цифрова епоха надала інформаційній війні нові можливості завдяки інтернету та соціальним мережам, що стали ефективними засобами поширення інформації та впливу на громадську думку. Це породжує нові виклики і загрози для національної та міжнародної безпеки, що потребує розробки ефективних стратегій для протидії інформаційним загрозам.

Також, перш за все, ця тема безпосередньо стосується ситуації, яка відбувається в нашій країні вже майже 10 років. Російсько-українська війна триває вже тривалий час та демонструє необхідність глибокого вивчення методів та підходів, використовуваних сторонами конфлікту. Це сприяє розумінню специфіки цього конфлікту і виявленню загальних тенденцій та принципів інформаційного протиборства, які можуть бути корисними в інших ситуаціях.

Важливим аспектом є розвиток медіаграмотності, яка допомагає людям аналізувати, оцінювати та ставитися критично до інформації. Вона передбачає здатність розпізнавати маніпулятивні техніки, розуміти різні медійні формати та їх вплив, а також навички перевірки достовірності інформації та розпізнавання фейкових новин. Розвиток медіаграмотності сприяє формуванню у людей більш виразного критичного підходу та самосвідомості при

споживанні інформації.

Отже, важливо навчити людей розглядати інформацію з різних джерел, аналізувати її та розуміти контекст і можливі мотиви, які приховуються за інформаційними повідомленнями. Навички сприйняття інформації включають в себе здатність відрізняти об'єктивну інформацію від спотвореної, розуміти маніпулятивні методи та прийоми, які використовуються для впливу на громадську думку.

Аналіз спеціальної літератури за обраною темою.

Наукові дослідження щодо інформаційних війн і супутніх процесів представляють собою комплексні результати аналізу політологами, істориками, соціологами, філософами, психологами, правознавцями, теоретиками ЗМІ і іншими експертами. Інформаційні війни тісно переплітаються з загальною суттю масової комунікації, конфліктологією, властивостями політичних відносин, поведінкою окремих осіб, соціальними групами і суспільством в цілому, а також впливом ЗМІ. Тому як наукова проблема, вивчення цієї теми спостерігалося в основному через призму суміжних галузей знань і зацікавлювало як іноземних, так і вітчизняних дослідників протягом тривалого часу.

Основи вивчення даної теми були визначені зусиллями іноземних вчених на початку XX століття, і вони передбачають результати досліджень в галузі соціології, зокрема Г. Лассуелем і П. Лазарсфельдом, які досліджували вплив засобів масової комунікації на громадську думку. Актуальними є також питання захисту від інформаційної агресії. Останнім часом інтерес до проблем інформаційної безпеки розповсюджується на академічне співтовариство, що відображається у зростаючій кількості дипломних робіт та дисертацій на теми, пов'язані з інформаційною війною.

Питання інформаційних війн в міжнародних відносинах є однією з найбільш актуальних тем сучасної наукової системи. Серед вітчизняних науковців, які присвятили свою діяльність дослідженню цієї проблеми, можна виділити таких дослідників як О.А. Безвинний (відомий український експерт з

інформаційних війн та кібербезпеки), І.М. Заплатська (українська експертка з інформаційних війн та кібербезпеки) та інших. Подібно до вітчизняних дослідників, іноземні вчені грають важливу роль у формуванні теоретичної бази інформаційних війн. До них варто віднести таких вчених як Герберт Шілдс, Ельза Кунцевіч, Тім Флемінг та інших, які розширюють наше розуміння інформаційних війн у міжнародних відносинах та надають важливий теоретичний внесок у цю галузь[15].

Мета дослідження. Метою проведення дипломної роботи є вивчення еволюції інформаційних війн у міжнародних відносинах та їх адаптація до сучасних умов. Дослідження спрямоване на аналіз впливу інформаційних війн на міжнародну арену та розробку стратегій протидії їм.

Завдання дослідження:

1) Вивчити історію та еволюцію інформаційних війн у міжнародних відносинах.

2) Оцінити сучасні методи та технології, які використовуються у цих війнах.

3) Розглянути вплив інформаційних війн на міжнародні конфлікти та відносини.

4) Розробити рекомендації щодо підвищення стійкості міжнародних відносин до інформаційних війн.

Об’єктом дослідження: Об'єктом дослідження є інформаційні війни в міжнародних відносинах загалом.

Предмет дослідження: Предметом дослідження є еволюція та адаптація інформаційних війн у міжнародних відносинах.

Методи дослідження: структурно-функціональний метод, аналіз літератури, емпіричні дослідження, та аналіз прикладів інформаційних війн у минулому та сучасності (історичний підхід), порівняльний метод, аналіз інформації та застосування дедуктивного методу, узагальнення за допомогою визначення причинно-наслідкових зв’язків.

Джерельнабаза(інформаційнаоснова) роботи:

1. Наукова література та академічні статті: книги, наукові статті та монографії, що досліджують інформаційні війни, міжнародні відносини, кібербезпеку та суміжні теми. Пошук такої літератури був здійснений через наукові бази даних, такі як Google Scholar, JSTOR, або EBSCO.

2. Документи міжнародних організацій: офіційні звіти, резолюції та документи, видані міжнародними організаціями, такими як ООН, НАТО, або Європейський Союз. Ці документи надають інформацію про погляди та стратегії міжнародних установ щодо інформаційних війн.

3. Міжнародні угоди та конвенції, які стосуються кібербезпеки та інформаційних війн. Наприклад, Кіберконвенція Ради Європи або Договір засобів міжнародного співробітництва в сфері кіберкриміналу ООН.

4. Засоби масової інформації: Інформація з новинних джерел, які стосуються конкретних подій і ситуацій, може бути корисною для розгляду конкретних випадків інформаційних війн.

5. Комп'ютерні бази даних та аналітичні інструменти: Для аналізу кібератак та поширення дезінформації, використовані комп'ютерні бази даних і аналітичні інструменти, такі як інструменти для аналізу соціальних мереж або засоби моніторингу інтернет-публікацій.

Практичнезначенняодержаних результатів

Дана дипломна робота може послужити як основа для подальших досліджень у галузі інформаційних війн та їх впливу на міжнародні відносини. Інші дослідники можуть використовувати цю роботу для розширення знань в цій галузі та подальшого вивчення сучасних аспектів інформаційних війн.

Структура роботи.Дипломна робота складається зі вступу, трьох розділів, висновків до кожного розділу, загального висновку та списку використаних джерел. Загальний обсяг дослідження становить 73 сторінок, список використаних джерел містить 65 найменування.

Ключові слова: інформація, інформаційна війна, конфлікт, міжнародні відносини, інформаційна політика, інформаційна безпека.

РОЗДІЛ 1. ТЕОРЕТИЧНІ ЗАСАДИ ДОСЛІДЖЕННЯ ІНФОРМАЦІЙНИХ ВІЙН

1.1. Інформаційні війни: поняття та ключові аспекти

У сучасному інформаційному суспільстві, де інформаційні технології відіграють ключову роль, термін «інформаційна війна» став не лише публіцистичним виразом або політичним терміном, але й активно використовується як самостійна категорія у науковому дискурсі. Це означає, що вчені досліджують і аналізують явище інформаційних війн, розглядаючи його як складний процес впливу, де використовуються різні методи та інструменти, зокрема дезінформація, кібератаки та політична маніпуляція, для досягнення політичних, економічних або стратегічних цілей. Інформаційні війни відіграють важливу роль у формуванні сучасного світового порядку та потребують серйозного наукового дослідження та реагування.

Вперше термін «інформаційна війна» було вжито Т. Роном в звіті «Системи зброї і інформаційна війна», підготовленому ним в 1976 р. [53]. Він підкреслював, що інформаційна інфраструктура є ключовим аспектом американської економіки, в той же самий час вона стає і вразливою метою як у воєнний, так і в мирний час.

Інформаційні війни — це форма боротьби, в якій сторони використовують інформаційні ресурси та технології для досягнення своїх політичних, військових або економічних цілей. Ця боротьба може бути як відкритою, так і прихованою, і включати в себе різні засоби впливу, такі як дезінформація, кібератаки, політична маніпуляція та інші [30].

Тема дипломної работи«Інформаційні війни: поняття та ключові аспекти» відображає актуальну проблему сучасного інформаційного суспільства. Інформаційні війни стають все більш важливими у міжнародних відносинах, політиці, кібербезпеці та громадському дискурсі. Розглянемо цю тему докладніше, розкриваючи її поняття та ключові аспекти (див.табл 1.1).

Таблиця 1.1.

Ключові аспекти інформаційних війн

Дезінформація і фейки	Одним із головних інструментів інформаційних війн є поширення неправдивої інформації або фейків. Це може призвести до створення спотворених образів подій та осіб, а також до зміни громадської думки.
Кібератаки	Кіберпростір став важливим полем боротьби в інформаційних війнах. Кібератаки можуть спрямовуватися на інформаційні системи, комунікаційні мережі, електронні ресурси та навіть критичну інфраструктуру.
Політична маніпуляція	Інформаційні війни часто включають в себе спроби вплинути на політичні процеси та вибори, зокрема шляхом маніпуляції соціальними мережами та розповсюдженням дезінформації.
Вплив на міжнародні відносини	Інформаційні війни можуть мати міжнародний аспект, включаючи вплив на відносини між країнами, дипломатичний тиск та створення антиукраїнських або антиєвропейських наративів.
Кібербезпека та захист	Одним з важливих аспектів боротьби з інформаційними війнами є забезпечення кібербезпеки та захисту від кібератак.
Соціальні мережі та кіберпростір	Інформаційні війни використовують соціальні мережі та Інтернет для поширення повідомлень та маніпуляції громадською думкою.
Захист демократичних цінностей	Інформаційні війни загрожують демократичним цінностям, таким як свобода слова, свобода преси та вільний обмін інформацією.

Єдиного визначення «інформаційної війни» досі не існує і на сьогодні поняття «інформаційна війна» визначається по-різному. Це пов’язано з багатозначністю терміну «information warfare», що породило безліч різночитань при його перекладах. Зазначене поняття може трактуватися як «інформаційна війна», «інформаційне протиборство», «інформаційно-психологічна війна»[30].

Поняття «інформаційна війна» трактується, як «широкомасштабна боротьба в інформаційному просторі із застосуванням методів, прийомів, способів, каналів і засобів маніпуляції психікою людей, у першу чергу їх індивідуальною і суспільною свідомістю та колективним несвідомим, з метою досягнення цілей і вирішення завдань суб’єкту впливу шляхом трансформації світогляду мас» (див.смеху 1.1.).

Головною метою цієї війни є «забезпечення необхідного рівня власної національної безпеки в усіх сферах суспільного життя і максимальне зниження

рівня захищеності національної безпеки конфронтуючої сторони» [53].

Схема 1.1. Цілі інформаційних війн

Інформаційна війна представляє собою форму конфлікту, де використовуються різноманітні методи та технології для маніпулювання інформацією з метою впливу на погляди, переконання та поведінку цільової аудиторії. Цей вид конфлікту може бути проведений як міжнародними учасниками, так і державними або недержавними суб'єктами внутрішньої політики.

Інформаційна війна полягає у конкуренції між сторонами, яка включає в себе розповсюдження спеціально підготовленої інформації та протидію подібному зовнішньому впливу на себе [5].

Відмінності між інформаційною війною і звичайною війною можуть бути

узагальнені у наступних аспектах:

1. Інформаційна війна використовує різноманітні засоби та має високий рівень непередбачуваності.

2. У контексті інформаційної війни захоплення територій здійснюється поетапно.

3. В інформаційній війні можлива багаторазова зміна переконань або тематичних аспектів у свідомості людей, і вона базується на нечіткій логіці.

4. В інформаційній війні важко визначити приналежність до конкретної групи або виконання певної соціальної ролі.

5. Вплив у інформаційній війні є непомітним та може набирати доброзичливу форму.

6. В інформаційній війні впливи є вибірковими та впливають на різні соціальні групи різним чином.

7. Однією з основних небезпек інформаційної війни є відсутність видимих матеріальних руйнувань, що призводить до неактивації захисних механізмів суспільства[24].

Інформаційна війна являє собою процес змагання між двома чи більше сторонами, які використовують різноманітні засоби та технології в сфері інформації та комунікацій з метою досягнення політичних, економічних або військових цілей. Важливо зауважити, що ці засоби та цілі постійно змінюються і розширюються. Цифрова трансформація та нові технології лише сприяють цьому процесу. Розвиток інформаційної війни можна розглядати у різних контекстах і на різних етапах, включаючи наступне (див. табл. 1.2):

Інформаційна війна є складним та мінливим процесом. Для успішної боротьби з дезінформацією та пропагандою важливо розуміти та усвідомлювати розвиток різних етапів інформаційної війни. Це передбачає забезпечення доступу до правдивої та об'єктивної інформації, підвищення обізнаності громадян щодо медіа та розвиток критичного мислення. Крім того, важливо сприяти розвитку та застосуванню алгоритмів та технологій, які допомагають виявити та боротися з пропагандою та дезінформацією,

забезпечуючи при цьому дотримання прав людини та демократичних цінностей[13].

Таблиця 1.2.

Етапи розвитку інформаційної війни

Перший етап:	Використання радіо та телебачення для поширення пропаганди та впливу на громадську думку. У цей період засоби масової інформації активно використовувалися для маніпулювання переконаннями людей та формування їхнього світогляду.
Другий етап:	Запровадження 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 для аналізу та обробки інформації.
Четвертий етап:	Поява нових видів загроз та викликів, пов'язаних зі зростанням ролі кіберпростору. На цьому етапі збільшується кількість кібератак, використання штучного інтелекту в інформаційній війні та використання соціальних мереж як інструменту впливу на громадську думку.
П'ятий етап:	Ускладнення інформаційної війни через використання технологій, що створюють фальшиву або неповну інформацію. Технології глибокого навчання можуть бути використані 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 у боротьбі з інформаційною війною. На цьому етапі створюються нові правові та політичні механізми для запобігання та реагування на інформаційні загрози, а також збільшується відповідальність за поширення дезінформації та пропаганди.
Сьомий етап:	Розвиток технологій штучного інтелекту, які можуть бути використані для розпізнавання та боротьби з дезінформацією та пропагандою. На цьому етапі активно використовуються алгоритми машинного навчання та аналізу даних для виявлення неправдивої інформації та маніпулятивних методів в інформаційному просторі.

Інформаційна війна представляє собою вид війни, що використовується для досягнення переваги в політичних або військових конфліктах завдяки ефективному використанню масових комунікаційних засобів, включаючи інформаційні технології.

Це використання інформаційних технологій означає використання різноманітних засобів, таких як Інтернет, соціальні мережі, блоги, електронна пошта та інші, для поширення інформації та впливу на громадську думку.

Основні характеристики інформаційної війни включають такі складові:

а) Маніпулювання громадською думкою: інформаційна війна може включати в себе маніпуляцію громадською думкою, включаючи застосування психологічних технік для впливу на емоції та переконання людей.

б) Вплив на дії противника: інформаційна війна може бути використана для впливу на дії противника, такі як зниження бойової готовності, зміна позицій або зменшення підтримки.

в) Використання соціальних мереж: соціальні мережі стають важливим інструментом для поширення інформації та впливу на громадську думку в інформаційній війні.

г) Широкомасштабність: інформаційна війна може охоплювати велику кількість людей і територій та включати багато різних елементів, включаючи політичну пропаганду, маніпуляцію соціальними медіа, кібератаки та інші методи впливу на громадську думку.

ґ) Неформальний характер: інформаційна війна може бути неформальною і важко визначити чітко, оскільки вона може проводитися без відкритої військової агресії.

д) Суперечливість: інформаційна війна може включати суперечливу інформацію, яка намагається змішати людей та створити незрозумілість та хаос серед громадськості.

е) Психологічна бойова дія: інформаційна війна може включати в себе застосування психологічного тиску та насильства для досягнення своїх цілей.

є) Відкритість або таємність: інформаційна війна може бути відкритою або прихованою, залежно від обставин і мети проведення.

ж) Висока швидкість: інформаційна війна може включати в себе високу швидкість поширення інформації та впливу на громадську думку, навіть в реальному часі.

з) Залежність від технологій: інформаційна війна сильно залежить від сучасних технологій, таких як соціальні медіа, Інтернет, кіберпростір та інші. Вона використовує різні техніки та інструменти для досягнення своїх цілей.

и) Неспроможність розрізнити правду та брехню: в сучасному світі інформаційна війна може бути дуже складною, оскільки важко розрізнити правду від брехні. Вона може включати дезінформацію, фейки, пропаганду та інші методи, що можуть приховувати справжню картину подій.

і) Загроза національній безпеці: інформаційна війна може становити серйозну загрозу національній безпеці та стабільності держави, спричиняючи розкол у суспільстві, збільшення конфліктів та загострення міжнародних відносин [1].

Отже, інформаційна війна є серйозною загрозою для сучасного світу через широкий спектр можливих наслідків, включаючи загрозу національній безпеці, суперечливу інформацію, психологічний тиск та інші негативні наслідки. Для захисту необхідно бути обережними та критично налаштованими до отриманої інформації, розвивати критичне мислення та критичний підхід до інформації, та зберігати національну єдність та стабільність.

Це важливою, оскільки інформаційні війни можуть мати серйозний вплив на суспільство, політику та міжнародні відносини. Розуміння понять і ключових аспектів цього явища допомагає ефективно боротися з ним та захищати суспільство від маніпуляцій та загроз, пов'язаних з інформаційними війнами.

1.2. Роль акторів у сучасних інформаційних війнах: держави, неурядові організації, та інші суб'єкти

Інформаційна війна є складним і багатогранним явищем, що має різні визначення та способи розгляду. Можна розглядати її як процес використання інформації для досягнення певних цілей шляхом впливу на свідомість і поведінку інших осіб, груп або навіть держав.

Існують кілька етапів розвитку інформаційної війни: підготовчий, активний та завершальний. Підготовчий етап включає в себе збір інформації та підготовку, а також створення необхідної інфраструктури.Активний етап

передбачає інтенсивне використання інформації для досягнення визначених цілей, таких як поширення пропаганди та дезінформації.Завершальний етап полягає у вивченні результатів та аналізі досвіду.

Основні характеристики інформаційної війни включають в себе різні засоби та методи впливу, цілі та об'єкти впливу, а також акторів, які беруть участь у процесі.

Засоби та методи впливу можуть включати в себе використання різних засобів масової інформації, соціальних мереж, бот-акаунтів та інших інструментів. Мети та об'єкти впливу можуть варіювати від роз'єднання стабільності держави до впливу на індивідуальну поведінку людей. Різні суб'єкти можуть брати участь у процесі інформаційної війни, включаючи держави, терористичні організації, корпорації та інші[12].

Таким чином, розуміння основних рис інформаційної війни допомагає розробляти ефективні стратегії для боротьби з нею. Важливо виявляти та аналізувати різні форми дезінформації та пропаганди, розвивати медіаграмотність та критичне мислення серед громадян, а також вдосконалювати технології захисту інформації та протидії противникам.

Співпраця з іншими країнами та міжнародними організаціями для координації заходів протидії інформаційним загрозам та зловживанню інформацією є також надзвичайно важливою. Інформаційна війна стала невід'ємною частиною сучасного світу, де інформація є одним з найцінніших ресурсів. У світі, де люди користуються Інтернетом, соціальними мережами та медіаплатформами, інформаційна війна може мати серйозні наслідки для політики, суспільства, економіки та культури.

Основними характеристиками інформаційної війни є використання різних каналів для передачі інформації, вплив на світогляд та переконання громадськості, маніпулювання емоціями та дезінформація. Наслідки інформаційної війни включають загострення міжнародних відносин, збільшення конфліктів і розкол у суспільстві. Для захисту від інформаційної війни важливо бути критичними до інформації, яку ми споживаємо, та

перевіряти її достовірність. Треба навчати громадян критичному мисленню та критичному ставленню до інформації, яку вони отримують, а також розробляти та впроваджувати ефективні засоби захисту від дезінформації та інших форм інформаційної агресії.

Роль акторів у сучасних інформаційних війнах включає в себе діяльність держав, неурядових організацій і інших суб'єктів. Інформаційні війни стали складною системою взаємодії, де кожен з цих акторів має свої специфічні цілі, можливості і методи впливу на інформаційному полі.

Розглянемо роль кожного з цих суб'єктів більш детально:

1. Роль держави в інформаційних війнах:

а) Держави відіграють ключову роль у сучасних інформаційних війнах. Вони використовують цей інструмент як для досягнення своїх політичних, військових та економічних цілей, так і для впливу на міжнародну арену та глобальний порядок.

б) Військові аспекти: Держави вкладають значні ресурси в інформаційну складову своєї військової діяльності. Це включає в себе кібератаки, використання розвідувальних служб для збору інформації та психологічну війну для впливу на ворожі війська та цивільне населення.

в) Дипломатія: Держави використовують інформаційні канали для підтримки своєї зовнішньої політики. Вони розробляють інформаційні кампанії, щоб вплинути на своїх іноземних партнерів, обговорюючи та популяризуючи свої позиції.

г) Внутрішня політика: Внутрішня стабільність та легітимність правління є важливими. Для цього держави використовують інформаційні засоби для впливу на громадську думку, створення національного образу та контролю за інформаційним простором. Іноді це включає в себе соратництво з медіа, публікацію позитивних новин та маніпуляцію інформаційними потоками для створення певного політичного образу.

2. Роль неурядових організацій в інформаційних війнах:

а) Неурядові організації використовують інформаційні війни для

просування своїх ідей та громадських ініціатив. Вони можуть бути важливими джерелами необхідної інформації та розвитку громадянського суспільства.

б) Активізм і просування ідей: Неурядові організації використовують інформаційні канали для просування своїх ідей та цінностей. Вони можуть розповсюджувати інформацію про права людини, екологію, гендерну рівність та інші соціальні питання.

в) Моніторинг та звітність: Неурядові організації грають важливу роль у виявленні порушень прав людини, корупції та невідповідності стандартам. Вони використовують інформаційні засоби для привертання уваги до цих питань та вимог до влади.

3. Роль інших суб'єктів в інформаційних війнах:

а) Корпорації: Деякі міжнародні корпорації також мають інтереси в інформаційних війнах, оскільки цілісна репутація їх бренду може бути важливою для бізнесу. Вони можуть вести інформаційні кампанії для впливу на свою аудиторію та споживачів.

б) Журналістика: Журналісти та ЗМІ виконують важливу роль у відслідковуванні подій та поширенні об'єктивної інформації. Однак вони також можуть бути об'єктом маніпуляції або використовуватися для поширення дезінформації. Розуміння цієї ролі може допомогти виявити та запобігти маніпуляціям у ЗМІ.

в) Громадянське суспільство: Активні громадяни та соціальні рухи впливають на громадську думку та політичні процеси через соціальні мережі, петиції, інтернет-кампанії та інші інструменти. Їх роль в інформаційних війнах полягає в просуванні своїх цінностей та вимог до влади [51].

Загальна роль цих акторів у сучасних інформаційних війнах полягає в тому, щоб керувати і формувати глобальний інформаційний простір, впливати на громадську думку, розвивати політичні процеси та визначати світовий порядок. Взаємодія та конфлікти між цими суб'єктами визначають подальший розвиток сучасного інформаційного суспільства та глобального порядку, і вимагають ретельного вивчення та розв'язання.

Висновки до розділу 1

З настанням епохи інформаційних технологій, людство має справу з багатьма складнощами. Однією з таких проблем є загроза безпеці інформації, яка стосується як держав, так і їх громадян. На сьогоднішній день, в світі не існує ефективної системи захисту інформаційної сфери. В умовах максимальної комп'ютеризації суспільства, жодна держава не може бути впевненою в своїй безпеці, оскільки її громадяни можуть бути піддані впливу ворожого інформаційного впливу у будь-який момент. Відомо, що в наш час багато країн розглядають інформаційну боротьбу як ефективний інструмент для втілення власної зовнішньої політики. До таких країн можна віднести і Україну, яка в певних обставинах була вимушена розпочати інформаційну війну проти Росії.

У висновку можна підкреслити важливість і актуальність даної теми в контексті сучасних міжнародних відносин та геополітичних процесів. Інформаційні війни стали невід'ємною частиною глобального політичного ландшафту та впливають на прийняття рішень, репутацію країн, а також загрожують кібербезпеці та стабільності в сучасному світі.

Це визначається посиленою активністю держав та акторів на міжнародній арені в інформаційній сфері. Відбувається не лише збільшення кількості інформаційних конфліктів, а й поява нових технологій та підходів до інформаційних війн. Зростання ролі соціальних мереж, маніпуляція громадською думкою, кібератаки та дезінформація стають сталим супутником міжнародних відносин. Це свідчить про те, що інформаційні війни мають значний вплив на політичні процеси, внутрішню та міжнародну безпеку, тому вони вимагають ретельного вивчення та аналізу [29].

Дослідження стосується еволюції цих війн та адаптації до сучасних реалій, і у дипломній роботі ми дійшли до кількох важливих висновків.

Сучасна геополітична ситуація вимагає глибокого розуміння інформаційних війн та їх впливу на міжнародні відносини. Інформаційні війни стали складовою політичного ландшафту, де вони використовуються для

досягнення стратегічних цілей, впливу на суспільну думку та маніпуляції інформацією. Зараз важливою є не лише військова сила, а й інформаційна.

Аналіз спеціальної літератури показав, що багато вчених та дослідників приділяють увагу інформаційним війнам, розвиваючи теоретичні підходи та методи аналізу цього явища. Важливою є співпраця міжнародних університетів та наукових установ у галузі дослідження інформаційних війн.

Інформаційні війни вимагають комплексного підходу та співпраці між країнами та акторами в міжнародних відносинах. Для ефективного протидії інформаційним війнам необхідно розвивати кібербезпеку, зміцнювати роль міжнародних організацій, спільно розробляти стратегії та методи аналізу інформаційних війн.

Ми отримали глибше розуміння інформаційних війн та їх впливу на міжнародні відносини, але треба розуміти, що інформаційні війни мають наслідки, що спільні за своєю глобальністю і тривалістю навіть із наслідками збройних конфліктів. Із завдяки Інтернету та сучасним методам політтехнологій, вони виявилися надзвичайно витратними у порівнянні з іншими видами воєнних дій. Основна причина цього полягає у можливостях Інтернету, який є найефективнішим інструментом для проведення інформаційних війн[60].

Інформаційна війна є об'єктом підвищеного інтересу для розробників оборонних стратегій та політиків, але, незважаючи на її стрімкий розвиток, поки що не має чіткого визначення. Зростаючий інтерес до цього питання зумовлений інформаційною революцією, яка відбувається внаслідок швидкого розвитку кіберпростору, мікрокомп'ютерів та пов'язаних із ними технологій. Якщо говорити про військове використання інформаційних технологій, то кожна з військових сторін прагне максимально використовувати глобальну інформаційну інфраструктуру та передові технології для ведення інформаційної війни.

Коаліції, що беруть участь у взаємній інформаційній війні, мають значні ресурси, включаючи складні системи управління та інфраструктури, що

здійснюють жорсткий контроль над грошовими потоками, повітряними лініями зв'язку, електроенергією, природними ресурсами (зокрема газом і нафтою) і іншими об'єктами, які є важливими для інформаційного суспільства. З точки зору концепції, якщо противник намагається руйнувати ці системи та інфраструктуру за допомогою технологій інформаційної війни, то інформаційна війна стає стратегічно важливою для атакованої сторони.

Інформаційне суспільство — це нова соціально-політико-економічна реальність, що описує новий ступінь розвитку цивілізації. Воно суттєво змінило спосіб життя людей, їх робочий процес та спосіб спілкування, і призвело до підвищення продуктивності праці та покращання добробуту. Інформаційне суспільство має більш складену структуру в порівнянні з попередніми соціальними утвореннями, оскільки його основу становлять комп'ютерні комунікації, які не є окремими виробничими одиницями, а є результатом розвитку специфічної індустрії. Щоб ефективно протидіяти цим загрозам, необхідна спільна діяльність держав, міжнародних організацій та громадянського суспільства.

РОЗДІЛ 2. ІНФОРМАЦІЙНІ ВІЙНИ В ІСТОРИЧНОМУ КОНТЕКСТІ МІЖНАРОДНИХ ВІДНОСИН

2.1. Еволюція інформаційних війн: історія розвитку у міжнародних відносинах

В даному розділі ми розглянемо історію розвитку інформаційних війн у міжнародних відносинах. Від первинних форм інформаційних війн до сучасних кібератак та інформаційної пропаганди, ми розглянемо еволюцію цього явища протягом часу (см.схема 2.1.).

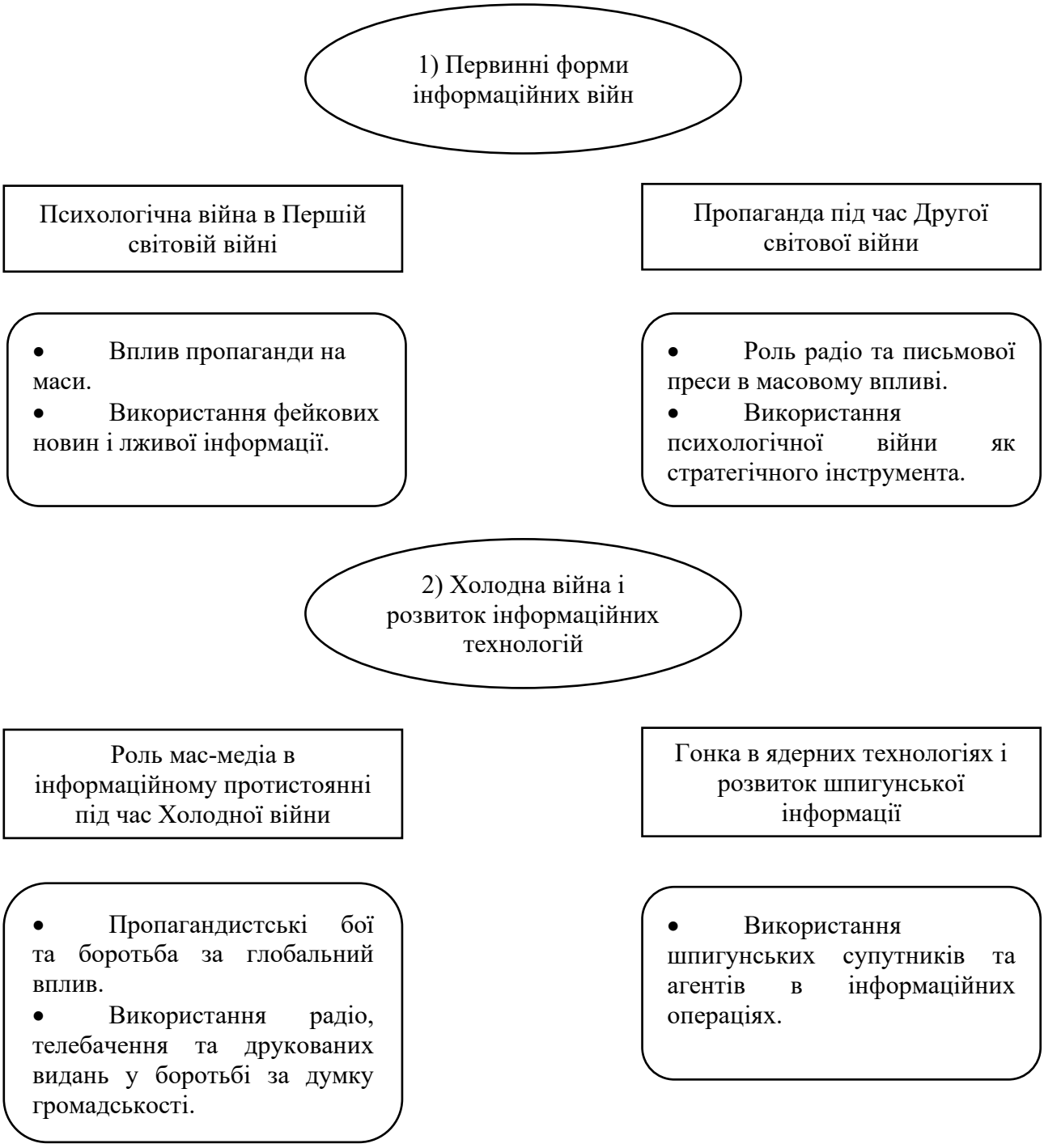

Схема 2.1. Історія розвитку інформаційних війн у міжнародних відносинах

1) Первинні форми інформаційних війн

Перша світова війна, що тривала з 1914 по 1918 роки, була однією з найкровопролитніших і руйнівних війн у світовій історії. Протягом цього конфлікту, окрім фізичних зіткнень на фронті, активно розвивалася психологічна війна, в якій пропаганда, фейкові новини та лжива інформація відіграли значущу роль. Психологічна війна – це один із важливих аспектів сучасних конфліктів, який виявив свою роль і в Першій світовій війні. Ця форма військової боротьби передбачає використання психологічних методів та засобів для впливу на свідомість, переконання і емоції ворога та власних військових і цивільного населення[6].

а) Пропаганда в Першій світовій війні

Пропаганда стала важливим інструментом військової стратегії у багатьох країнах, що брали участь в війні. У цей період було створено численні агентства та відділи пропаганди, які відповідали за розробку та поширення ідеологічних матеріалів. Газети, плакати, листівки, фільми та інші види масової інформації були активно використовані для розповсюдження пропагандистських повідомлень. Їх завданням було створити патріотичний національний дух, підтримати військовий ентузіазм і об'єднати націю навколо спільних цілей [6].

б) Вплив пропаганди на маси

Пропаганда впливала на маси, впорядковуючи їхню свідомість і переконання. Вона створювала образ ворога, демонізуючи його та підкреслюючи його загрожуючий характер. Власних військових, навпаки, презентували як героїв та захисників нації. Пропаганда використовувала емоції, страх та патріотизм для мобілізації громадської підтримки війни. Зображення ворога як жахливого і загрожуючого ворога були поширені в усіх країнах, що брали участь у війні.

в) Використання фейкових новин і лживої інформації

Фейкові новини та лжива інформація були поширені для посилення ефективності пропаганди. Це включало в себе створення надуманих історій про

злочини ворога, вигадані перемоги власних військ та розповсюдження спекулятивних та непідтверджених повідомлень. Наприклад, було розповсюджено розбійницькі історії про злочини ворога, які нерідко не мали підстав у реальності. Це призводило до зростання ненависті до ворога та підтримувало військову мобілізацію[14].

Підсумовуючи вище сказане, можна дійти висновку, що психологічна війна в Першій світовій війні підкреслила важливість впливу на громадську думку та психологію в сучасних конфліктах. Використання пропаганди, фейкових новин і лживої інформації стали ключовими інструментами в цій боротьбі. Зараз, у віці Інтернету та соціальних мереж, ці методи залишаються актуальними та навіть більш небезпечними, вимагаючи більше уваги до медійної грамотності та критичного мислення суспільства для розпізнавання дезінформації та фейкових новин. Психологічна війна залишається важливим аспектом сучасних конфліктів та міжнаціональних відносин, і розуміння її інструментів та методів стає важливим завданням для суспільства.

2) Холодна війна і розвиток інформаційних технологій

Холодна війна була періодом напружених відносин між США та Радянським Союзом, що тривав з кінця Другої світової війни приблизно до початку 1990-х років. Хоча не було жодного прямого військового конфлікту між цими двома світовими супердержавами, становилися очевидними інші форми змагань, включаючи гонку в ядерних технологіях і розвиток шпигунської інформації. Розвиток інформаційних технологій відіграв важливу роль у цьому періоді, створюючи нові можливості та загрози для обидві сторони [61].

а) Гонка в ядерних технологіях

Гонка в ядерних технологіях була однією з основних характеристик Холодної війни. Обидві сторони активно працювали над розвитком ядерних збройних систем, включаючи атомні бомби та ядерні ракети. Ця гонка спричинила великий технологічний прорив у ядерній науці та інженерії, що мало безпосередній вплив на сучасні технології. Наприклад, багато розробок,

пов'язаних з ядерною енергією, застосовуються в сучасних ядерних реакторах і дослідженнях в сфері ядерної фізики[43].

б) Розвиток шпигунської інформації

Однією з ключових аспектів Холодної війни був розвиток шпигунської інформації. Обидві сторони вкладали великі зусилля у здобуття секретної інформації про ворога. Інформаційні операції включали в себе використання шпигунських супутників та агентів, які проникли в ряди ворога.

Шпигунські супутники: Використання шпигунських супутників було революційним кроком у зборі інформації. Супутники здатні були відстежувати переміщення військових формувань, аналізувати будівлі та спостерігати за іншими діяльностями ворога з космосу. Це надавало змогу здобувати цінну інформацію про плани та наміри противника.

Агенти: Шпигунська діяльність на території ворога також була важливою складовою розвідувальної роботи. Агенти, які проникали в ряди противника, збирали інформацію про важливі військові, політичні та економічні події. Ця інформація допомагала уникнути можливих загроз та приймати інформовані рішення.

в) Вплив на сучасні інформаційні технології

Розвиток інформаційних технологій під час Холодної війни відіграв важливу роль у формуванні сучасного світу. Технологічні досягнення, які були зроблені під час цього періоду, включаючи розробку комп'ютерів та комунікаційних систем, послужили основою для подальшого розвитку інформаційних технологій[61].

Сучасні інформаційні системи, включаючи Інтернет, супутникову комунікацію та шифрування, сформовані внаслідок великої кількості досліджень та розробок, які здійснювалися під час Холодної війни. Крім того, усвідомлення загрози кібернетичних атак і важливість захисту інформації були закладені в цей період.

У висновку можна сказати, що Холодна війна була не лише конфліктом ідеологій, але і періодом, коли технології грали важливу роль в змаганні між

двома світовими супердержавами. Гонка в ядерних технологіях і розвиток шпигунської інформації суттєво вплинули на сучасні інформаційні технології та розвідувальну діяльність. Сучасний світ бореться з новими викликами і загрозами, пов'язаними з цифровими технологіями, історія Холодної війни надає цінний досвід і уроки для майбутнього.

г) Роль мас-медіа в інформаційному протистоянні під час Холодної війни

Період напружених відносин між США та Радянським Союзом під час Холодною війни був назван«війною ідеологій». Цей конфлікт спричинив появу нових засобів інформаційного впливу та пропаганди, і мас-медіа відіграли ключову роль у боротьбі за глобальний вплив і думку громадськості. Розглянемо, як радіо, телебачення та друковані видання використовувалися в інформаційному протистоянні під час Холодної війни [46].

г) Пропагандистські бої та боротьба за глобальний вплив.

Пропаганда була важливою складовою Холодної війни, і мас-медіа використовувалися обома сторонами для поширення власної ідеології та дискредитації противника. Радянський Союз створив масштабну медійну машину для пропаганди комуністичної ідеології. Зокрема, радіо «Голос Америки» і радіо «Свобода» (Radio Free Europe/Radio Liberty) поширювали інформацію та думки, які протистояли радянській пропаганді. Спроби обох сторін впливати на громадську думку іноземних країн через мас-медіа стали невід'ємною частиною цього інформаційного протистояння [6].

д) Використання радіо, телебачення та друкованих видань у боротьбі за думку громадськості.

I. Використання радіо

Радіо було одним із найпоширеніших засобів масової інформації під час Холодної війни. Радіомовлення було важливим інструментом для поширення пропаганди та інформації. Кожна сторона створила свої радіостанції для міжнародного мовлення. Наприклад, радіо «Свобода» вело мовлення на різних європейських мовах та створювало передачі, які підтримували ідеї свободи і демократії.

II. Телебачення

Телебачення стало потужним інструментом пропаганди та впливу. Телеканали, такі як BBC, Voice of America та телеканал «Радянська Україна»,транслювали телепередачі, які підкреслювали свої ідеологічні переконання та події, що стосувалися Холодної війни. Телебачення дозволило показати жахи війни, а також сприяло обміну культурними програмами та фільмами між східним і західним світом.

III. Друковані видання

Друковані видання, такі як газети та журнали, також використовувалися в інформаційному протистоянні. Газети, які представляли різні політичні погляди, були розповсюджені як в межах власних країн, так і за їх межами. Завдяки цьому, громадяни мали можливість отримувати різні точки зору та аналізувати інформацію.

У висновку можна сказати, що мас-медіа відіграли важливу роль в інформаційному протистоянні під час Холодної війни, сприяючи поширенню ідеологій, інформації та впливу. Використання радіо, телебачення та друкованих видань було ефективними засобами впливу на думку громадськості, і цей досвід має значення й у сучасному інформаційному просторі. Важливо пам'ятати, як мас-медіа можуть бути використані для маніпулювання громадською думкою та формування ідеологічного впливу.

3) Зміна парадигми в інформаційних війнах: кібербезпека та сучасні технології

Зростання кібербезпеки стало однією з найважливіших тем у міжнародних відносинах в наш час. Швидкий розвиток інформаційних технологій і кіберпростору створює нові можливості, але також і нові загрози для держав та їх критичної інфраструктури. Розглянемо стратегії, спрямовані на забезпечення кіберзахисту держав та обговоримо кібератаки на об'єкти критичної інфраструктури.

а) Стратегії та політики щодо кіберзахисту держав

Міжнародне співробітництво: Один із важливих аспектів зростання

кібербезпеки в міжнародних відносинах — це співробітництво між державами. Багатонаціональні організації, такі як ООН, НАТО та Європейський Союз, вже розробили документи та договори, спрямовані на забезпечення кіберзахисту та обмін інформацією про кіберзагрози.

Створення національних стратегій кібербезпеки: Багато держав розробили національні стратегії кібербезпеки, які включають в себе плани дій, заходи та регуляції щодо кіберзахисту. Ці стратегії часто визначають важливі об'єкти критичної інфраструктури та інші аспекти кібербезпеки.

Розвиток кіберзахисних здатностей: Держави вдосконалюють свої кіберзахисні здатності, включаючи створення військових кіберкоманд та реакційних груп для боротьби з кіберзагрозами.

Законодавчі заходи: Введення законодавчих норм і стандартів, спрямованих на забезпечення кібербезпеки, є важливою частиною стратегії. Держави розробляють та впроваджують закони, які регулюють кіберпростір і встановлюють відповідальність за кіберзлочини[65].

б) Кібератаки на об'єкти критичної інфраструктури

Кібератаки на об'єкти критичної інфраструктури можуть бути надзвичайно руйнівними і мають потенціал завдати серйозної шкоди суспільству та державі в цілому. До об'єктів критичної інфраструктури включаються енергетичні системи, водопостачання, транспортні мережі, медичні установи та інші, які необхідні для нормального функціонування суспільства.

в) Щоб запобігти кібератакам на об'єкти критичної інфраструктури, держави вживають наступні заходи:

Моніторинг та виявлення загроз: Впровадження систем моніторингу та виявлення загроз допомагає вчасно виявляти кібератаки та реагувати на них.

Захист та зміцнення інфраструктури: Держави вдосконалюють захисні заходи для своєї критичної інфраструктури, включаючи захист від вторгнень та відновлення систем після атак.

Міжнародне співробітництво: Держави співпрацюють між собою та з

міжнародними організаціями для обміну інформацією та розв'язання кіберзагроз.

У висновку можна сказати, щозростання кібербезпеки в міжнародних відносинах стає все важливішим завданням у сучасному світі. Стратегії та політики кіберзахисту держав, спрямовані на забезпечення безпеки в кіберпросторі, стають невід'ємною частиною національних та міжнародних дій. Боротьба з кібератаками на об'єкти критичної інфраструктури вимагає комплексного підходу та співробітництва між державами для забезпечення стійкості та безпеки суспільства [61].

г) Соціальні мережі та поширення дезінформації

Соціальні мережі стали неодмінною частиною життя багатьох людей і мають великий вплив на суспільство та політику. Проте, разом із їхніми позитивними аспектами, соціальні мережі також використовуються для поширення дезінформації та маніпуляцій. Розглянемо вплив соціальних мереж на поширення дезінформації та роль російського втручання в вибори в США та інших країнах.

г) Вплив соціальних мереж на поширення дезінформації.

Соціальні мережі надали звичайним користувачам можливість стати інформаційними джерелами та розповсюджувачами новин. Проте, ця демократизація інформаційного простору також відкрила можливості для поширення дезінформації. Основні фактори впливу соціальних мереж на поширення дезінформації включають:

Алгоритми підбору контенту: Соціальні мережі використовують алгоритми для підбору контенту, який користувачі бачать у своїх стрічках. Це може призводити до утворення «фільтру бульбашки», де користувачі практично не піддаються інформації, яка суперечить їхнім переконанням.

Швидкість поширення: Соціальні мережі дозволяють інформації швидко розповсюджуватися. Це дозволяє дезінформації поширюватися вразливим шаром суспільства перед тим, як факти встигають вийти на поверхню.

Анонімність та псевдоніми: Користувачі соціальних мереж можуть

приховувати свою ідентичність, що ускладнює відстеження джерела дезінформації[14].

д) Роль російського втручання в вибори в США та інших країнах

Російське втручання в вибори в інших країнах стало однією з найважливіших проблем у контексті поширення дезінформації. Росія використовує соціальні мережі та інші онлайн-платформи для впливу на вибори та політичні процеси у різних країнах.

Основні методи включають:

Створення фейкових акаунтів: Російські агенти створюють фейкові соціальні медіа-акаунти, які поширюють дезінформацію та пропаганду.

Розміщення реклами та контенту: Росія купує рекламу та розміщує контент на соціальних мережах, спрямований на вплив на громадську думку та підтримку конкретних кандидатів.

Підтримка публікацій: Російські агенти підтримують публікації, які сприяють дезінформації та розпалюють політичні розділи.

Підсумовуючи можна сказати, що соціальні мережі стали не тільки платформою для спілкування та обміну інформацією, але й інструментом для поширення дезінформації. Роль соціальних мереж у поширенні дезінформації вимагає ретельного вивчення та дії з боку держав, громадян та платформ для соціального медіа. Російське втручання в вибори стало серйозною загрозою для демократичних процесів, і є необхідність в утриманні цієї загрози від відповідних заходів та стратегій[34].

4) Висновки та перспективи

Інформаційні війни стали невід'ємною частиною сучасної глобальної політики і конфліктів. Ці війни відзначаються використанням інформаційних технологій, медіа та соціальних мереж для досягнення політичних та військових цілей. Розглянемо загальні тенденції та виклики в інформаційних війнах, зростаючу складність інформаційних загроз у сучасному світі та необхідність в міжнародних спільних діях щодо кібербезпеки та інформаційної безпеки.

а) Загальні тенденції та виклики в інформаційних війнах

Цифрова трансформація: Сучасні інформаційні війни зумовлені швидким розвитком цифрових технологій та їхнім використанням для впливу на глобальну аудиторію. Цифрова трансформація відкрила нові можливості для здійснення атак та маніпуляцій.

Соціальні мережі та медіа: Соціальні мережі стали ключовим інструментом в інформаційних війнах. Вони дозволяють інформації швидко поширюватися та впливати на громадську думку. Важливою частиною цього процесу є маніпуляція інформацією та створення фейкових новин.

Гібридні війни: Інформаційні війни часто поєднуються з іншими формами конфлікту, включаючи гібридні війни, які використовують економічний тиск, дипломатичний вплив і військові дії для досягнення цілей[11].

б) Зростаюча складність інформаційних загроз у сучасному світі

Технічна складність: Зростаюча технічна обізнаність зловмисників дозволяє їм розробляти більш складні і надійні засоби атаки, такі як хакерські методи.

Анонімність: Зловмисники можуть приховувати свою ідентичність та місце розташування, що ускладнює виявлення та протидію.

Масштаб та глобальність: Інформаційні атаки можуть мати глобальний масштаб і впливати на багато країн одночасно, що робить їх більш складеними для управління та захисту.

в) Потреба в міжнародних спільних діях щодо кібербезпеки та інформаційної безпеки.

Міжнародні договори та діалог: Міжнародні договори та діалог між країнами є важливими для встановлення міжнародних стандартів та правил щодо кібербезпеки. Міжнародні спільні дії можуть допомогти в обміні інформацією та спільному реагуванні на кіберзагрози.

Захист критичної інфраструктури: Країни повинні звернути особливу увагу на захист критичної інфраструктури, яка може бути метою кібератак.

Міжнародні стандарти та спільні підходи до захисту цієї інфраструктури є важливими.

Глобальне співробітництво: Глобальне співробітництво в області кібербезпеки є важливим для обміну інформацією про кіберзагрози та спільного реагування на них.

Інформаційні війни стали невід'ємною частиною сучасної глобальної політики, і вони вимагають нових підходів та міжнародних спільних дій для забезпечення кібербезпеки та інформаційної безпеки. Зростаюча складність інформаційних загроз вимагає спільних зусиль країн та міжнародних організацій для захисту суспільства та інфраструктури від інформаційних атак.

г) Роль міжнародних організацій та дипломатії в інформаційних війнах

Міжнародні стандарти та норми: Міжнародні організації, такі як ООН та Європейський Союз, грають важливу роль у розробці та встановленні міжнародних стандартів та норм щодо кібербезпеки та інформаційної безпеки. Ці норми сприяють зменшенню ризику конфліктів і забезпечують правила гри в кіберпросторі.

Дипломатія та міжнародні переговори: Дипломатія грає ключову роль у вирішенні конфліктів та встановленні міжнародних домовленостей щодо кібербезпеки. Міжнародні переговори дозволяють державам обговорювати спільні підходи до протидії інформаційним загрозам.

Обмін інформацією та спільна реакція: Міжнародні організації стимулюють обмін інформацією між державами щодо кіберзагроз та допомагають в спільній реакції на інформаційні війни. Це може включати в себе спільні вправи, аналіз інцидентів та розробку рекомендацій для політики.

Інформаційні війни та загрози кібербезпеці вимагають спільних дій та міжнародної координації. Міжнародні організації та дипломатія грають важливу роль у формуванні міжнародних стандартів, спільному реагуванні на інциденти та забезпеченні глобальної кібербезпеки та інформаційної безпеки. Тільки шляхом спільних зусиль можна забезпечити стабільність та безпеку в

кіберпросторі.

2.2. Перспективи розвитку інформаційних війн в майбутньому

Інформаційні війни стають все більш важливим аспектом сучасних конфліктів і глобальних відносин. Розвиток технологій впливає на еволюцію інформаційних війн і відкриває нові можливості та виклики. Перспективи розвитку інформаційних війн у майбутньому можна розділити на декілька важливих розділів:

Таблиця 2.1.

Перспективи розвитку інформаційних війн у майбутньому

Технологічні аспекти	Розгляд можливостей розвитку технологій та їхню вплив на інформаційні війни. Цей розділ включає в себе розгляд штучного інтелекту, квантових обчислень, кіберзброї, а також розвиток мережі 5G і Інтернету речей.
Стратегічні аспекти	Аналіз можливих сценаріїв розвитку інформаційних війн у майбутньому та їхній вплив на глобальну безпеку та геополітичні відносини.
Соціокультурні аспекти	Розгляд впливу інформаційних війн на суспільство, громадську думку, культуру та етику. Дослідження впливу соціальних мереж, дезінформації та медіа на суспільство.
Захист і кібербезпека	Розвиток методів та засобів захисту від інформаційних загроз і кібератак. Аналіз стратегій та політик для підвищення кібербезпеки.
Міжнародна співпраця	Розгляд можливостей спільної дії між країнами та міжнародними організаціями у питаннях кібербезпеки та боротьби з інформаційними загрозами.
Етичні аспекти	Дослідження етичних питань, пов'язаних з інформаційними війнами, включаючи питання приватності, свободи слова, інтернет-цензури тощо.
Економічні аспекти	Визначення впливу інформаційних війн на економіку, включаючи витрати на кіберзахист, втрати від кібератак та можливості для кіберекономіки.

1) Технологічні аспекти

Штучний інтелект вже зараз грає важливу роль в інформаційних війнах, а його розвиток обіцяє стати ще більш впливовим у майбутньому. Основні аспекти використання ШІ в інформаційних війнах включають:

Генерація фейкових контентів: ШІ може використовуватися для створення реалістичних фейкових зображень, відео та аудіофайлів. Це може викликати збентеження та недовіру в суспільстві.

Автоматизовані атаки: ШІ може використовуватися для виявлення та використання вразливостей у кіберінфраструктурі, здійснення масштабних кібератак та обходу захисних заходів.

Аналіз великих обсягів даних: ШІ допомагає аналізувати великі обсяги даних для виявлення трендів, що може бути використано в інформаційних війнах для впливу на громадську думку та прийняття рішень.

а) Квантові обчислення

Розвиток квантових обчислень має потенціал змінити ландшафт кібербезпеки. Квантові комп'ютери можуть ламати сучасні шифри і криптографічні системи значно швидше, ніж традиційні комп'ютери. Це створює великий виклик для кібербезпеки та інформаційної безпеки.

б) Мережа 5G та Інтернет речей (IoT)

Розвиток мережі 5G та розширення Інтернету речей відкриває нові можливості для інформаційних війн. Мережа 5G надає швидкий та надійний доступ до Інтернету, що дозволяє швидше поширювати дезінформацію та використовувати розширені медіаресурси. IoT привносить велику кількість підключених пристроїв, які можуть стати об'єктами кібератак та маніпуляцій.

в) Кіберзброя та хакерські атаки

Розвиток кіберзброї та хакерських атак обіцяє стати все більш складним та ефективним. Атаки можуть бути спрямовані на критичну інфраструктуру, об'єкти влади, економічні системи та громадську думку. Технології шифрування та анонімність можуть робити розслідування та протидію таким атакам більш складними.

Розвиток технологій обумовлює появу нових можливостей і викликів у сфері інформаційних війн. Штучний інтелект, квантові обчислення, мережа 5G, Інтернет речей та кіберзброя грають ключову роль у визначенні майбутніх сценаріїв інформаційних війн. Для забезпечення кібербезпеки та інформаційної

безпеки в майбутньому необхідно розробляти нові стратегії, технологічні рішення та міжнародні норми, щоб захистити суспільство та глобальну безпеку.

2) Стратегічні аспекти

а) Гібридні війни та кіберзброя

Однією з головних стратегічних тенденцій є зростання популярності гібридних війн, які поєднують інформаційні війни з традиційними формами конфлікту. Гібридні загрози можуть включати в себе дезінформацію, кібератаки, газ, фінансовий тиск і дипломатичний вплив. Стратегічне планування має враховувати можливість таких комплексних загроз і розвивати відповідні заходи для їх виявлення та протидії [28].

б) Геополітичні зміни

Геополітичні зміни впливають на характер інформаційних війн. Зміна ролі та впливу держав, зміщення економічних центрів, територіальні конфлікти та розширення впливу кількох ключових акторів у сфері інформаційних війн вимагають нових стратегій та підходів до глобальної безпеки.

в) Захист критичної інфраструктури

Забезпечення захисту критичної інфраструктури, такої як електроенергетика, транспорт, комунікації та фінанси, є ключовим стратегічним завданням. Інформаційні війни можуть спрямовуватися на знищення або заваду функціонуванню цих систем, що може призвести до серйозних наслідків для суспільства та національної безпеки.

г) Міжнародна співпраця та норми

Співпраця між державами у сфері інформаційних війн стає все важливішою. Розробка та дотримання міжнародних норм та стандартів, які регулюють поведінку в кіберпросторі, є стратегічно важливим завданням. Міжнародні спільні дії можуть допомогти створити систему взаємного захисту та відповідальності.

г) Етичні питання та права людини

Важливим стратегічним аспектом є захист прав людини та забезпечення етичного використання інформаційних технологій у військових операціях.

Заборона кіберзброї масового знищення, дотримання принципів гуманітарного права та забезпечення прозорості стають ключовими стратегічними завданнями.

Враховуючи вище сказане, розвиток інформаційних війн у майбутньому вимагає уважного аналізу та стратегічного планування. Зростання гібридних загроз, геополітичні зміни, захист критичної інфраструктури, міжнародна співпраця, етичні питання та права людини — це всі аспекти, які мають бути враховані в стратегіях протидії інформаційним загрозам у майбутньому. Лише завдяки комплексним стратегічним ініціативам можна забезпечити стабільність та безпеку в сучасному світі, де інформаційний простір набуває все більшого впливу[2].

3) Соціокультурні аспекти

а) Зміна медіа-пейзажу

З розвитком інтернету та соціальних мереж медіа-пейзаж зазнав кардинальних змін. Традиційні видання та телебачення втрачають позиції на користь онлайн-медіа та платформ соціальних мереж. Це створює можливості для розповсюдження дезінформації та маніпуляції громадською думкою. В майбутньому цей тренд може посилитися, створюючи складність у визначенні правдивої інформації.

б) Вплив соціальних мереж на суспільство

Соціальні мережі вже зараз впливають на формування суспільної думки та культурних цінностей. За допомогою алгоритмів та персоналізованого контенту вони можуть створювати ізольовані інформаційні «бульбашки», де користувачі підтверджують свої власні погляди та переконання, ігноруючи альтернативні точки зору. Це може підсилити поділ суспільства та ускладнити конструктивний діалог.

в) Розповсюдження дезінформації

З розвитком технологій стає все легше створювати та поширювати фейкові новини та дезінформацію. Це може викликати паніку, конфлікти та втрату довіри до інформації загалом. У майбутньому, з Штучним інтелектом та

автоматизованими системами, цей процес може стати ще більш втямливим.

г) Зміна культурних цінностей

Інформаційні війни можуть впливати на культурні цінності та переконання. Зміст та структура інформації, яка подається через масові медіа та соціальні мережі, може впливати на сприйняття різних культур та груп населення. Структуровані кампанії дезінформації можуть впливати на ідентичність та сприйняття інших культур.

На завершення, слід зазначити, що соціокультурні аспекти інформаційних війн у майбутньому стають все важливішими. Зміна медіа-пейзажу, вплив соціальних мереж, розповсюдження дезінформації та зміна культурних цінностей мають потенціал впливати на суспільство та глобальну стабільність. Розуміння цих аспектів допоможе розробити стратегії протидії інформаційним загрозам та зберегти культурну різноманітість та громадську гармонію.

4) Захист і кібербезпека

а) Зростання кіберзагроз

З розвитком технологій кіберзагрози стають більш складними та розповсюдженими. Атаки можуть бути спрямовані на різні сфери, включаючи державні структури, корпорації, критичну інфраструктуру та громадянське суспільство. Кіберзлочинці використовують різноманітні методи, включаючи вимагання викупу Ransomware (рансомвар), крадіжку даних та кібершпигунствво. У майбутньому, зростання кіберзагроз та масштаб атак може стати навіть більшим.

б) Розвиток кіберзброї та технік

Кіберзброя та техніки здійснення кібератак постійно еволюціонують. Вони стають більш смертоносними та складними, здатними завдавати шкоду критичній інфраструктурі, фінансовим системам та військовим об'єктам. Такі атаки можуть мати глобальний вплив, що ставить під загрозу національну безпеку.

в) Штучний інтелект та кіберзахист

З використанням штучного інтелекту (ШІ) кіберзахист може бути

покращений. ШІ може виявляти та відсіювати загрози на ранніх стадіях, що дозволяє вчасно реагувати на потенційні атаки. Прогнозується, що в майбутньому ШІ буде грати ключову роль у захисті від кіберзагроз та виявленні порушень кібербезпеки.

г) Міжнародна співпраця та норми

Забезпечення кібербезпеки вимагає співпраці між державами та розробки міжнародних норм та стандартів для кіберпростору. Міжнародні обговорення та угоди можуть сприяти встановленню правил гри та мінімізації конфліктів у кіберпросторі.

Отже, перспективи розвитку інформаційних війн у майбутньому вимагають підвищеної уваги до кібербезпеки. Зростання кіберзагроз, розвиток кіберзброї, використання ШІ та необхідність міжнародної співпраці вимагають комплексних стратегій та заходів. Захист кіберпростору та кібербезпека стають критичними аспектами для забезпечення національної та глобальної безпеки в майбутньому.

5) Міжнародна співпраця

а) Зростання глобальних загроз

Інформаційні війни в майбутньому можуть стати більш глобальними та масштабними. Зростання кіберзагроз, дезінформації та маніпуляції глобальною громадською думкою можуть призвести до загрози міжнародній стабільності та безпеці. Для подолання цих загроз необхідна співпраця між державами та міжнародними організаціями.

б) Міжнародні норми та стандарти

Розробка та прийняття міжнародних норм та стандартів є важливим кроком у боротьбі з інформаційними загрозами. Захист кіберпростору та встановлення правил гри у цій сфері можуть допомогти у попередженні конфліктів та зниженні ризику кібератак. Міжнародні домовленості також можуть встановлювати відповідальність за порушення правил у кіберпросторі.

в) Обмін інформацією та співробітництво

Ефективний захист від інформаційних загроз вимагає обміну

інформацією та співробітництва між державами. Спільне виявлення та реагування на кібератаки може значно підвищити ефективність заходів з кібербезпеки. Міжнародні організації, такі як ООН, можуть грати важливу роль у координації цього співробітництва.

г) Дипломатичні зусилля

Дипломатія також може відігравати важливу роль у боротьбі з інформаційними загрозами. Міжнародні домовленості та переговори можуть сприяти вирішенню конфліктів у кіберпросторі та встановленню довгострокових відносин між державами.

Загалом, перспективи розвитку інформаційних війн у майбутньому вимагають міжнародної співпраці та спільних зусиль. Зростання глобальних загроз, розробка міжнародних норм та стандартів, обмін інформацією та дипломатичні зусилля можуть допомогти у забезпеченні стабільності та безпеки в кіберпросторі. Міжнародна співпраця стає ключовим чинником в запобіганні та протидії інформаційним загрозам у майбутньому.

6) Етичні аспекти

а) Збільшення ролі дезінформації та фейкових новин

З розвитком соціальних мереж та онлайн-медіа збільшується поширення дезінформації та фейкових новин. Це може завдавати шкоду громадській думці, підірвати довіру до інформації та створювати ситуації, коли правда стає суб'єктивною. Питання етики включають в себе відповідальність за розповсюдження недостовірної інформації та важливість фактчекінгу.

б) Прапаганда та маніпуляція громадською думкою

Інформаційні війни часто використовують прапаганду та маніпуляцію громадською думкою для досягнення політичних цілей. Це може включати в себе створення псевдоінформації, маніпуляцію суспільними настроями та підштовхування до конфліктів. Етичні питання в цьому контексті стосуються використання інформаційних технологій для маніпуляції громадською думкою та необхідності прозорості у процесі впливу на неї.

в) Порушення приватності та прав людини

Інформаційні війни можуть призводити до порушення приватності та прав людини. Наприклад, зламані бази даних та розповсюдження особистої інформації можуть стати інструментами для переслідування та дискредитації активістів, журналістів та громадян. Захист приватності та прав людини є важливим аспектом етики в інформаційних війнах.

г) Роль міжнародної співпраці та норм

Для вирішення етичних питань інформаційних війн необхідна міжнародна співпраця та розробка міжнародних норм та стандартів. Міжнародні обговорення можуть визначити етичні принципи та правила для використання інформаційних технологій у політичних та військових цілях.

Важливо відзначити, етичні аспекти інформаційних війн в майбутньому стають все більш важливими. Збільшення дезінформації, прапаганди та порушення приватності вимагає уважності та відповідальності використання інформаційних технологій. Міжнародна співпраця та розробка етичних норм можуть допомогти створити більш справедливий та прозорий інформаційний простір в майбутньому.

7) Економічні аспекти

а) Кіберзлочини та економічна шкода

Зростання кіберзагроз і кіберзлочинів може завдати значної шкоди економіці. Кібератаки на корпорації, фінансові установи та інфраструктуру можуть призвести до великих фінансових втрат. Плата за відновлення та підвищення кібербезпеки може стати значним обтяженням для підприємств та держав. Оцінюється, що річна вартість кіберзлочинів досягає багатьох мільярдів доларів, і ця сума може зростати в майбутньому.

б) Кібершпигунство та конкурентне шпигунство

Кібершпигунство в майбутньому може виявити значний вплив на конкурентну боротьбу між компаніями та країнами. Злочинні групи або держави можуть намагатися отримати конфіденційну інформацію про інновації, плани розвитку та інші комерційні секрети. Це може призвести до втрати конкурентної переваги та погіршити економічний стан компаній та

національних економік.

в) Вплив на фінансові ринки

Кібератаки на фінансові установи можуть створити турбулентність на фінансових ринках. Наприклад, злам біржових систем або маніпуляція фінансовими даними можуть призвести до значних коливань вартості акцій та інших фінансових інструментів. Це може вплинути на інвесторів, пенсійні фонди та інші фінансові інтереси.

г) Зростання витрат на кібербезпеку

З масштабними кіберзагрозами компанії та уряди будуть змушені вкладати значні ресурси у зміцнення кібербезпеки. Це включає в себе витрати на кадри, технології та профілактичні заходи. Зростання витрат на кібербезпеку може мати вплив на фінансову стійкість організацій та держав[58].

На завершення, слід зазначити, що економічні аспекти інформаційних війн в майбутньому вимагають серйозного уваги. Зростання кіберзагроз, кіберзлочинів та кібершпигунства може призвести до значних економічних втрат та обтяжити фінансові системи. Зростання витрат на кібербезпеку стає важливим завданням для підприємств та держав, і ефективний захист цифрових активів стає ключовою складовою економічної безпеки.

Висновки до розділу 2

У другому розділі дипломної роботи інформаційні війни розглядаються у контексті міжнародних відносин. Була розглянута еволюція інформаційних війн в історії розвитку міжнародних відносин і розглянуті перспективи їхнього розвитку в майбутньому.

У першому підрозділі було досліджено історичний розвиток інформаційних війн у міжнародних відносинах. Були переглянуті епохи від давніх часів до сучасності та з'ясовано, як інформаційні війни впливали на події та розвиток міжнародних стосунків. Було зрозуміло, що інформаційні війни завжди були важливим інструментом політичних, економічних та військових

стратегій. Вони використовувалися для впливу на суспільство, зміни режимів та забезпечення безпеки національних інтересів.

Звідси можна зробити висновок, що інформаційні війни завжди були невід'ємною частиною міжнародних відносин і вони продовжують зростати важливість в сучасному світі. Розуміння їхньої історії допомагає розвивати стратегії та заходи для протидії інформаційним загрозам [40].

У другому підрозділі були розглянуті перспективи розвитку інформаційних війн в майбутньому. Сучасні технології, зокрема Інтернет, соціальні мережі та кіберзброя, роблять інформаційні війни більш доступними і деструктивними. Вони можуть впливати на політичні рішення, національну безпеку та світовий порядок. Таким чином, майбутнє інформаційних війн заповнене викликами та можливостями.

Заходи з кібербезпеки, розвиток міжнародних норм та стандартів для кіберпростору і зусилля з попередження дезінформації стають ключовими аспектами в роботі з інформаційними війнами у майбутньому.

Розділ 2 даної дипломної роботи дав можливість прослідкувати історичний контекст інформаційних війн у міжнародних відносинах та спрогнозувати їхні перспективи в майбутньому. Важливо розуміти, що інформаційні війни стають все більш важливим елементом геополітичного ландшафту і глобальної безпеки. Розвиток технологій і зростання залежності від цифрового простору роблять їх більш актуальними та складними.

Отже, розуміння інформаційних війн та їхніх впливів у міжнародних відносинах є важливим завданням для політиків, аналітиків та громадян. Спільні зусилля національних та міжнародних громадських структур, правительств та активістів можуть допомогти забезпечити стійкість і безпеку у світі, де інформація стала найціннішим ресурсом і знаряддям впливу.

РОЗДІЛ 3. АДАПТАЦІЯ ДЕРЖАВ ДО СУЧАСНИХ ВИКЛИКІВ У СФЕРІ ІНФОРМАЦІЙНИХ ВІЙН

3.1. Сучасні виклики для держав: кібершпигунство та фейкові новини як ключові складові інформаційних війн

Інформаційні війни складаються з різних компонентів та складових, які спільно створюють стратегію впливу на громадську думку, політичні рішення та безпеку держав. Ось деякі зі складових інформаційних війн(див.табл.3.1):

Таблиця 3.1

Складові інформаційних війн

Дезінформація	Це включає в себе поширення неправдивої або обманливої інформації з метою змінити громадську думку або перекрутити факти. Дезінформація може включати в себе фейкові новини, спекуляції, чутки та інші методи впливу.
Кібератаки	Ця складова включає в себе атаки на комп'ютерні системи з метою витоку інформації, завдання шкоди інфраструктурі або заволодіння критичними системами. Кібератаки можуть бути спрямовані на виборчі системи, урядові органи, бізнес-сектор, енергетичні об'єкти тощо.
Соціальні мережі та онлайн-платформи	Інформаційні війни активно використовують соціальні мережі, форуми та інші онлайн-платформи для поширення дезінформації, маніпуляції громадською думкою та координації дій. Вони можуть створювати фейкові облікові записи, групи та кампанії для впливу на користувачів.
Спільноти та боти	Інформаційні війни можуть створювати штучні спільноти та використовувати ботів для поширення дезінформації та маніпуляції громадською думкою. Це дозволяє швидко поширювати повідомлення та створювати враження широкої підтримки або обурення.
Кібершпигунство	Як вже розглядалося раніше, кібершпигунство передбачає здобуття розвідувальної інформації, яка може бути використана для формування стратегії впливу та маніпуляції.
Політичні кампанії та лобіювання	Держави та інші актори можуть створювати політичні кампанії та лобіювання з метою впливу на рішення політиків та формування законодавства.
Заходи протидії	Щоб протистояти інформаційним війнам, держави повинні розробляти та впроваджувати заходи, включаючи кіберзаходи безпеки, підвищення медіаграмотності громадян, регулювання діяльності на соціальних мережах, співпрацю з міжнародними партнерами тощо.
Міжнародний аспект	Інформаційні війни можуть мати міжнародний характер, оскільки держави можуть втручатися в справи інших держав, що викликає міжнародні конфлікти та напруженість у міжнародних відносинах.

Усі ці складові доповнюють одна одну, створюючи складну та впливову стратегію інформаційних війн. Зрозуміння цих складових допомагає справлятися з цими викликами та розробляти ефективні стратегії протидії інформаційним війнам.

1) Кібершпигунство як ключова складова інформаційних війн

Кібершпигунство стало не тільки найактуальнішим питанням у світі кібербезпеки, але й ключовою складовою інформаційних війн у сучасному глобальному ландшафті. У цьому розділі докладно розглянемо природу, методи та вплив кібершпигунства на сучасне суспільство та політику.

1. Поняття кібершпигунства

Кібершпигунство — це діяльність, що передбачає використання кіберзасобів та технологій для отримання розвідувальної інформації. Головною метою кібершпигунства є здобуття конфіденційної інформації про військові, політичні, економічні або технічні аспекти інших держав. Кібершпигуни можуть діяти на користь своєї країни або на шкоду іншим.

2. Методи кібершпигунства

Кібершпигуни використовують різні методи для досягнення своїх цілей:

Кібератаки: Вони включають атаки на комп'ютерні системи для викрадення чутливої інформації або руйнування інфраструктури. Це може включати в себе атаки на військові об'єкти, урядові системи, або комерційні підприємства.

Фішинг та соціальна інженерія: Ці методи включають в себе обман осіб або співробітників, щоб отримати доступ до системи або інформації. Це може включати в себе відправку підроблених листів електронною поштою, створення фальшивих веб-сайтів та імітацію легітимних ситуацій.

Використання шпигунського програмного забезпечення: Шпигунське програмне забезпечення, відоме також як «шпигунські віруси» або «малвар», встановлюється на комп'ютерах або мережах для стеження за діяльністю та збору інформації.

3. Вплив кібершпигунства на інформаційні війни

Маніпуляція громадською думкою: Здобута розвідувальна інформація може бути використана для створення фейкових новин, дезінформації та маніпуляції громадською думкою. Це може впливати на вибори, політичні рішення та громадську довіру.

Втручання в політичні процеси: Кібершпигунство може бути спрямоване на втручання в політичні процеси і вибори в інших країнах, з метою впливу на результати та структуру політичного уряду.

Захист власних інтересів: Кібершпигунство також важливе для забезпечення безпеки власної країни. Виявлення загроз, розробка стратегій кіберзахисту та попередження атак стають критичними завданнями.

4. Міжнародний вимір кібершпигунства

Кібершпигунство має міжнародний вимір, оскільки воно може впливати на міжнародні відносини і співпрацю між державами. Вирішення цього питання вимагає міжнародного співробітництва та розробки міжнародних норм та стандартів у кіберпросторі[65].

Отже, кібершпигунство стало ключовою складовою інформаційних війн у сучасному світі. Воно має значущий вплив на політичні рішення, громадську думку та безпеку держав. Для ефективного протистояння цій загрозі необхідно розвивати кібербезпеку, закріплювати міжнародну співпрацю та вдосконалювати законодавство щодо кібершпигунства.

2) Фейкові новини як ключові складові інформаційних війн

Фейкові новини (іноді відомі як «фейки» або «дезінформація») виступають як ключова складова інформаційних війн. Вони є потужним інструментом маніпуляції громадською думкою, створення паніки та впливу на політичні рішення. Ось, як фейкові новини стають ключовою складовою інформаційних війн:

1. Поширення дезінформації: Фейкові новини нерідко містять неправдиву або обманливу інформацію, яка може бути спрямована на досягнення конкретних цілей. Це може включати в себе створення історій про події, які ніколи не трапилися, чи перекручення фактів.

2. Маніпуляція громадською думкою: Фейкові новини можуть бути використані для маніпуляції громадською думкою та формування негативного або позитивного ставлення до певних подій, осіб або ідеологій. Це може впливати на виборчі рішення, погляди на глобальні питання і соціокультурні тенденції.

3. Вплив на політичні процеси: Фейкові новини можуть впливати на політичні процеси, зокрема на вибори та прийняття політичних рішень. Це може включати в себе розповсюдження дезінформації про кандидатів або партії з метою впливу на результати виборів.

4. Поширення обурення та конфліктів: Фейкові новини можуть сприяти поширенню обурення, непокоїв та конфліктів. Вони можуть підкріплювати антиглобалізаційні настрої, релігійні розбіжності, расову ненависть та інші форми соціальної напруженості.

5. Використання соціальних мереж та медіа: Фейкові новини ефективно розповсюджуються через соціальні мережі та інтернет-медіа, де вони можуть викликати широкий імпакт. Вони роблять маніпуляцію громадською думкою та розповсюдження дезінформації легшою завдяки цифровим платформам.

6. Міжнародний аспект: Фейкові новини часто мають міжнародний характер, оскільки їх можуть створювати та розповсюджувати зокрема іноземні актори для досягнення своїх геополітичних цілей.

7. Заходи протидії: Для боротьби з фейковими новинами, держави та міжнародні організації розробляють механізми виявлення та відповіді на дезінформацію, вдосконалюють медіаграмотність громадян та сприяють розробці стандартів та кодексів етики для журналістів та медіа.

Фейкові новини стають потужним інструментом інформаційних війн, і їх вплив на глобальну політику та громадську думку продовжує зростати. Виявлення та протидія фейкам стають важливою складовою безпеки інформаційного простору [62].

3) Дезінформація як ключові складові інформаційних війн

Дезінформація є ключовою складовою інформаційних війн і грає важливу роль у впливі на громадську думку, політичні процеси та безпеку держав. Ось, як дезінформація виступає як ключова складова інформаційних війн:

а) Поширення неправдивої інформації: Дезінформація передбачає поширення неправдивої або обманливої інформації з метою створення збентеження або маніпуляції громадською думкою. Це може включати в себе створення фейкових новин, чуток та неправдивих заяв.

б) Маніпуляція громадською думкою: Дезінформація може бути використана для маніпуляції громадською думкою та впливу на переконання та ставлення громадян до різних питань. Це може включати в себе спрямовану маніпуляцію політичними переконаннями, релігійними уявленнями та іншими аспектами громадського життя.

в) Поширення обурення та конфліктів: Дезінформація може сприяти поширенню обурення, непокоїв та конфліктів. Вона може створювати образи та ворожнечу, а також поглиблювати суспільні розбіжності.

г) Вплив на політичні рішення: Дезінформація може бути використана для впливу на прийняття політичних рішень. Це може включати в себе розповсюдження неправдивої інформації про кандидатів, партії або питання, які знаходяться на голосуванні.

ґ) Зміна реальності: Дезінформація може створювати враження, що реальні події відбуваються інакше, ніж це відбувається насправді. Це може призвести до змін у сприйнятті подій та спричинити плутанину серед громадян.

д) Використання медіа та соціальних мереж: Дезінформація часто використовує медіа та соціальні мережі для поширення. Вона може легко набути широкого розповсюдження через цифрові платформи, де вона стикається з великою аудиторією.

е) Міжнародний аспект: Дезінформація може мати міжнародний характер, оскільки іноземні держави або актори можуть втручатися в справи інших країн, створюючи дезінформацію для досягнення своїх цілей.

є) Заходи протидії: Для боротьби з дезінформацією, держави та

міжнародні організації розробляють механізми виявлення та відповіді на дезінформацію, вдосконалюють медіаграмотність громадян та сприяють розробці стандартів та кодексів етики для журналістів та медіа[47].

Дезінформація є потужним засобом впливу у сучасному інформаційному ландшафті і створює серйозні виклики для суспільства та політичних процесів. Виявлення та протидія дезінформації стають важливими завданнями для збереження довіри до інформації та функціонування демократичних суспільств.

4) Стратегії та принципи інформаційної безпеки

Основна мета забезпечення інформаційної безпеки полягає у захисті інформаційного середовища від небажаного доступу, маніпуляцій та дезінформації. Нижче наведено декілька стратегій і принципів, які використовуються в сфері інформаційної безпеки:

Концепція повного циклу інформаційної безпеки: Ця стратегія передбачає застосування комплексного підходу до інформаційної безпеки, охоплюючи всі етапи життєвого циклу інформації — збір, обробка, передача та збереження. Цей підхід забезпечує захист інформації на кожному етапі, включаючи джерела і кінцевих користувачів[3].

а) Принцип обмеження доступу: Відповідно до цього принципу, конфіденційна та важлива інформація повинна бути доступна лише авторизованим особам. Це досягається через контроль користувачів, обмеження прав доступу, використання шифрування та інших технологічних заходів для запобігання несанкціонованому доступу до інформації. Принцип також передбачає впровадження систем аутентифікації та авторизації, використання різних рівнів доступу та ролей користувачів, керування розподілом прав доступу, регулярне оновлення паролів і моніторинг дій користувачів для виявлення можливих порушень.

б) Моніторинг і реагування: Цей принцип включає систематичний моніторинг інформаційного середовища для виявлення потенційних загроз та атак на інформаційну безпеку. Для цього використовуються системи моніторингу мережі, системи виявлення вторгнень і спеціалізовані програми.

Швидкі та ефективні заходи приймаються для ліквідації цих загроз та відновлення інформаційної безпеки у випадку виявлення потенційних загроз або інциденту. Блокування атак, відновлення інформаційних систем та інші заходи спрямовані на мінімізацію збитків від інцидентів.

в) Освіта та свідомість: Освіта та підвищення свідомості відіграють важливу роль у захисті інформації від загроз, маніпуляцій та дезінформації. Це досягається наданням людям правильної інформації та навичок безпечного користування нею. Головною метою є підвищення обізнаності користувачів, щоб вони могли розуміти та ефективно реагувати на потенційні загрози. Навчання безпеці в мережі, включаючи використання надійних паролів, уникнення підозрілих посилань і небезпечних файлів, є важливим елементом освіти та свідомості користувачів. Забезпечення освіти та свідомості є ключовим кроком у забезпеченні інформаційної безпеки та запобіганні багатьом інцидентам.

г) Співпраця та партнерство: 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 можливий завдяки обміну інформацією про загрози та кращими практиками, спільній боротьбі з дезінформацією та координації заходів. Співпраця сприяє розвитку інформаційного середовища, стійкості та впровадженню нових політик і технологій, а також виявленню нових загроз.

Ці стратегії та принципи створюють основу для забезпечення ефективного захисту інформації в контексті інформаційних війн. Використання комплексного підходу, обмеження доступу, моніторингу та реагування, освіти та свідомості, а також співпраці та партнерства допомагають досягти інформаційної безпеки та ефективно протидіяти дезінформації та маніпуляціям у рамках російсько-українського конфлікту [55].

3.2 Україна в просторі інформаційних війн: поразки та перемоги

У сучасних умовах, у контексті конфлікту між Росією та Україною, наші зусилля необхідні для захисту національної інформаційної сфери від негативних впливів і психологічних операцій, забезпечення інформаційної безпеки та інформаційного суверенітету для наших громадян. Подолання цих загроз важливе для збереження національної ідентичності України та забезпечення її як суверенної та незалежної держави.

Серед завдань системи забезпечення інформаційної безпеки країни можна виділити наступні аспекти:

а) Планування, яке включає в себе виявлення, моніторинг та прогнозування загроз національним інтересам.

б) Координація, яка означає визначення та реалізацію повноважень системи управління національною безпекою.

в) Стимулювання, яке передбачає розробку та впровадження політичних рішень, законодавчих та нормативно-правових актів для забезпечення системи управління національними інформаційними ресурсами.

г) Контроль за станом, порядком і правилами формування, розвитку та використання інформаційних ресурсів.

ґ) Державне регулювання сфери інформатизації з метою забезпечення науково-технічних та організаційно-економічних умов для створення та використання інформаційних технологій [8].

Серед інститутів, що сприяють інформаційній безпеці, можна виділити верховенство закону, незалежний та компетентний суд, відсутність корупції та інші фактори. Інституційний механізм, що гарантує інформаційну безпеку, є важливою структурною складовою державного механізму, який визначає норми та правила взаємодії різних економічних суб'єктів в інформаційній сфері з метою запобігання загрозам інформаційній безпеці.

Таким чином, національний інформаційний простір України на жаль, піддається значним загрозам та викликам, які становлять ризику для

функціонування держави, її політичного та економічного розвитку, а також для інтеграції в європейські та євроатлантичні структури. Проблема забезпечення механізмів інформаційної безпеки вимагає подальшого глибокого вивчення та розв'язання.

Роль ЗМІ (Засобів масової інформації) у російсько-українській інформаційній війні виявилася важливою. Росія активно використовувала свої медіа ресурси для поширення пропаганди, маніпуляції громадською думкою та впливу на сприйняття конфлікту, як в Україні, так і за її межами.

Основні аспекти ролі ЗМІ в цьому контексті включають:

а) Поширення дезінформації: Російські ЗМІ активно використовувались для поширення фейкових новин та дезінформації про події в Україні, включаючи вигадані історії, маніпуляції фактами та спотворення подій.

б) Створення пропагандистських наративів: Російські ЗМІ формували пропагандистські наративи, демонізуючи українську владу та підтримуючи російську агресію, щоб створити ілюзію широкої підтримки російським діям.

в) Залучення «експертів» та коментаторів: Російські ЗМІ залучали «експертів» та коментаторів, які підтримували російську версію подій та надавали публічні коментарі, що відповідали їхній пропаганді.

г) Використання медіа для психологічного впливу: Російські ЗМІ використовувались для створення загрозливого образу ворога, розповсюдження страху та невпевненості в населенні України, а також для підтримки розділу та конфлікту між українцями.

г) Заперечення правдивої інформації: Російські ЗМІ активно заперечували правдиву інформацію, яка суперечила їхнім наративам, намагаючись відхилити критику та змінювати факти.

Україна також використовувала ЗМІ для інформаційної війни проти Росії, але обмежена кількість ресурсів порівняно з Росією обмежувала її можливості. Українська влада та ЗМІ приймали ряд заходів для протидії російській пропаганді та дезінформації:

а) Розповсюдження правдивої інформації: Українська влада та ЗМІ

намагалися активно розповсюджувати правдиву інформацію про події в Україні, надаючи достовірні факти та статистику для спростування фейкових новин.

б) 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.

в) Розвиток власних медіа ресурсів: Україна поступово розвивала власні медіа ресурси, включаючи телебачення, радіо та онлайн-платформи, які спрямовані на передачу правдивої інформації та боротьбу з російською пропагандою.

г) Сприяння громадській журналістиці: Україна підтримувала громадські журналістські ініціативи, допомагаючи висвітлювати реальну ситуацію в країні та боротися з дезінформацією.

ґ) Контрпропаганда та демаскування: Україна активно використовувала контрпропаганду та демаскування російської пропаганди через аналіз і розкриття фейкових новин та маніпуляцій, щоб показати справжню картину подій та відповідність їхніх тверджень реальності [4].

Інформаційна війна має серйозний вплив на суспільство, воєнні операції та міжнародні відносини. Розуміння ролі ЗМІ, їхньої взаємодії з військовими діями та використання інформаційних технологій є важливим для розробки ефективних планів та заходів щодо забезпечення інформаційної безпеки в умовах конфлікту.

Україна стала однією з країн, яка активно бореться з інформаційними війнами, особливо після подій Євромайдану в 2013-2014 роках та анексії Криму Росією. В просторі інформаційних війн, Україна зазнала як поразок, так і перемог. Ось деякі ключові моменти:

Поразки:

а) Анексія Криму та війна на сході України: Росія вдалося використовувати інформаційні війни для виправдання своєї агресії на сході України та анексії Криму. Російська пропаганда та дезінформація сприяли

створенню іншого вигляду подій для міжнародної аудиторії, і це вплинуло на сприйняття подій в Україні.

б) Використання соціальних мереж та медіа: Росія активно використовує соціальні мережі та медіа для поширення пропаганди та дезінформації. Це включає в себе створення фейкових аккаунтів, спонсоровану пропаганду та розповсюдження конспіративних теорій змови [39].

Перемоги:

а) Спротив дезінформації: Україна вживає заходів для боротьби з дезінформацією. Наприклад, створено Факт-чекінг(з англ. Fact checking — перевірка фактів) — це один з напрямків журналістського контролю. Перевірка фактів являє собою процес перевірки фактичної достовірності звітів і заяв, що викликають сумнів. Також діє проект «СтопФейк», який активно розкриває дезінформацію.

б) Медіаграмотність громадян: Україна активно працює над підвищенням медіаграмотності громадян, освічає їх щодо виявлення фейків та навчає критично відноситися до інформації.

в) Міжнародна підтримка: Україна отримує підтримку від міжнародних партнерів, які надають технічну, інформаційну та фінансову допомогу для боротьби з інформаційними загрозами.

г) Зміцнення кібербезпеки: Україна вдосконалює свої кіберзахисні можливості для захисту критичних інфраструктур та інформації від кібератак.

г) Міжнародні ініціативи: Україна долучилася до міжнародних ініціатив щодо боротьби з інформаційними війнами, співпрацюючи з іншими країнами для розробки стратегій протидії дезінформації.

Україна продовжує бути полем боротьби в інформаційних війнах, і її досвід в цій галузі може бути корисним для інших країн, які також стикаються з схожими викликами. Незважаючи на труднощі, Україна демонструє свою відданість принципам демократії та інформаційній безпеці[11].

Висновки до розділу 3

Тема «Адаптація держав до сучасних викликів у сфері інформаційних війн» є дуже актуальною у сучасному світі, оскільки інформаційні війни стають все більш серйозною загрозою для національної безпеки країн. Ця тема передбачає вивчення та аналіз того, як держави адаптують свої підходи до збору, обробки та поширення інформації, а також як вони реагують на інформаційні атаки та впливові кампанії. Основні аспекти цієї теми включають:

1. Інформаційна безпека: Держави повинні приділяти особливу увагу захисту своїх інформаційних ресурсів та інфраструктури. Це включає заходи щодо кібербезпеки, захисту державних баз даних, а також захисту критично важливих інформаційних систем від потенційних атак.

2. Дезінформація і фейкі: Держави повинні розробляти стратегії для виявлення, відслідковування та боротьби з дезінформацією та фейками, які можуть використовуватися для маніпуляції громадською думкою та дезорієнтації громадян.

3. Інформаційні війська: Деякі країни використовують інформаційні війська для поширення своєї інформації та впливу на інших. Адаптація до цього явища включає розробку власних стратегій інформаційної війни та контрпропаганди.

4. Міжнародні виміри: Інформаційні війни можуть мати міжнародні аспекти, коли одна держава втручається у справи інших через інформаційні атаки. Адаптація до цього вимагає розвитку міжнародних стандартів та співпраці для боротьби з інформаційними загрозами.

5. Захист громадської свободи та приватності: Держави повинні балансувати заходи із захисту національної безпеки і прав громадян на інформаційну свободу та приватність. Адаптація до цього вимагає розвитку правових та етичних рамок.

6. Кібербойова готовність: Держави повинні бути готові до кібербойових дій і розробляти відповідні стратегії та кадровий потенціал для захисту власних інформаційних ресурсів.

У сучасному світі інформаційні війни стали важливою складовою міжнародних відносин та політичного процесу. Держави, незалежно від свого розміру та впливу, стикаються з новими викликами у сфері інформаційної безпеки, включаючи кібершпигунство та поширення фейкових новин. У цьому розділі ми розглянемо, як держави адаптуються до цих сучасних викликів і як Україна долає їх у контексті інформаційних війн[42].

Сучасні виклики для держав

Кібершпигунство – це процес збору розвідувальної інформації через мережу Інтернет та інші комп'ютерні технології. Ця загроза стала надзвичайно актуальною у сучасному світі, де практично всі сфери життя перетинаються з інформаційним простором. Держави та організації ведуть кібершпигунство для здобуття конфіденційної інформації, включаючи важливі військові, політичні та економічні дані. Для адаптації до цього виклику держави повинні розвивати сучасні кіберзаходи та політику кібербезпеки[23].

Фейкові новини або дезінформація стали іншим ключовим викликом для сучасних держав. Ця проблема полягає у поширенні неправдивої або маніпулятивної інформації з метою вплинути на громадську думку, виборчий процес або міжнародні відносини. Для боротьби з цим викликом, держави повинні розвивати механізми перевірки інформації та підвищення медіаграмотності громадян.

Україна в просторі інформаційних війн

Поразки. Україна стала свідком і активним учасником інформаційних війн вже після Майдану 2014 року та анексії Криму Росією. Під час цих подій дезінформація та кібершпигунство були важливими інструментами для досягнення політичних та військових цілей. Україна зазнала значних поразок у відповідь на ці загрози, включаючи втрату територій та економічні втрати.

Перемоги. Проте Україна також досягла певних перемог у сфері

інформаційних війн. Зокрема, українські ЗМІ та активісти ведуть інформаційну війну проти дезінформації та фейкових новин, розкриваючи правду та відстоюючи свої позиції. Крім того, Україна співпрацює з міжнародними партнерами та організаціями, щоб підсилити свою кібербезпеку та захистити важливу інформацію від кіберзагроз.

Для розробки національної політики у сфері інформаційної безпеки насамперед потрібно об'єктивно оцінити сучасний стан справ, особливості та майбутні перспективи розвитку інформаційної зброї та методів її використання. Ця оцінка є ключовою передумовою для розробки зовнішньої і внутрішньої політики держави, включаючи військові та військово-технічні аспекти, які могли б запобігти загрозам і забезпечити безпеку країни.

Необхідно розуміти, що загроза інформаційної війни і інформаційної злочинності широко розглядається як фактор прихованого воєнно-політичного тиску і інструмент залякування, який може підірвати світову і регіональну стабільність і безпеку. Тому необхідно систематично моніторити загрози, пов'язані з використанням інформаційної зброї та постійно оцінювати ефективність систем протидії цим загрозам.

Цей моніторинг повинен включати аналіз не лише науково-технічних досягнень у розробці інформаційної зброї та засобів протидії їй, але і враховувати зміни у зовнішньо-політичній ситуації, прогноз глобальних і локальних конфліктів та протиріч, що можуть призвести до інформаційної війни.

Зрозуміло, що важливо також стежити за внутрішнім і міжнародним законодавством та нормативно-правовими аспектами, що стосуються інформаційної безпеки.

Вирішення проблем інформаційних загроз дозволить забезпечити захист інтересів суспільства та держави, а також гарантуватиме громадянам право на отримання якісної та об'єктивної інформації.

Отже, сучасні виклики у сфері інформаційних війн, такі як кібершпигунство та фейкові новини, стали неот'ємною частиною міжнародних

відносин та політичного процесу. Для адаптації до цих викликів, держави повинні розвивати сучасні підходи до кібербезпеки та медіаграмотності громадян. Україна, не зважаючи на втрати та труднощі, активно працює над тим, щоб захистити свою інформаційну безпеку та боротися з дезінформацією, що свідчить про важливість цих питань у сучасному світі.Адаптація до сучасних викликів у сфері інформаційних війн є критично важливою для забезпечення національної безпеки та стабільності в світі, де інформація має величезну владу і вплив.

ВИСНОВКИ

У ході вивчення проблеми інформаційних війн у міжнародних відносинах в цій дипломній роботі були виявлені та проаналізовані ключові аспекти цього явища. В розділі 1 розкрито теоретичні засади інформаційних війн, включаючи їх поняття та роль різних акторів у цьому контексті. В розділі 2 досліджено історичний розвиток інформаційних війн у міжнародних відносинах, їх еволюцію та перспективи майбутнього. Розділ 3 розглядає адаптацію держав до сучасних викликів у сфері інформаційних війн, зокрема кібершпигунство та поширення фейкових новин.

Інформаційна війна стала невід’ємною складовоюсучасного світу, де інформація має величезне значення. У цьому світі, де інтернет, соціальні мережі та медіа-платформи є поширеними, вплив інформаційної війни може суттєво вплинути на політику, суспільство, економіку та культуру. Основними рисами інформаційної війни є використання різних каналів для поширення інформації, зміна поглядів та переконань громадськості, маніпулювання емоціями та розповсюдження дезінформації. Інформаційна війна може призвести до серйозних наслідків, таких як загострення міжнародних відносин, збільшення конфліктів та розкол у суспільстві.

Головною метою інформаційної війни є послаблення моральних і матеріальних ресурсів супротивника або конкурента, одночасно підсилюючи власні позиції. Ця стратегія включає в себе пропагандистські дії, спрямовані на вплив на ідеологічні та емоційні аспекти свідомості людей. Очевидно, що інформаційна війна є невід'ємною частиною ідеологічної боротьби.

У сучасних умовах постійний технологічний прогрес сприяє послідовному зростанню обсягу та швидкості поширення інформації. Вдосконалюються можливості охоплення інформацією великих територій та численних груп людей за найкоротший час. На фоні позитивних аспектів глобальної інформатизації чітко виокремлюються нові міжнародні проблеми. Однією з найбільш актуальних є сфера інформаційної безпеки та

інформаційного протиборства. З використанням вже доступних публічно даних можна зазначити, що на світовому рівні нині відбувається значущий розвиток інформаційних і кібернетичних конфліктів.

Інформаційні конфлікти не ведуть безпосередньо до насильства, руйнувань або жертв. Жоден з її учасників не залишається без їжі або притулку. Та саме це може створити певну хибну перцепцію інформаційної війни як безпечного явища. Водночас, руйнування, що виникають в результаті інформаційних конфліктів, мають значущий вплив на психологію суспільства та окремих осіб, і за своєю масштабністю та наслідками можуть бути порівняні з наслідками збройних конфліктів.

Вплив на свідомість через ЗМІ є основним методом проведення інформаційних війн і полягає в прямому втручанні в психологічний стан людей. Цей маніпулятивний вплив організовується так, щоб думка, уявлення та образи стають частиною свідомості і закріплюються в ній як беззаперечні та вже доведені факти. Ця задача часто ставиться перед ЗМІ, які можуть бути контрольовані державними урядами.

Для захисту від інформаційної війни важливо розвивати критичний підхід до отриманої інформації та перевіряти її надійність. Крім того, необхідно сприяти розвитку критичного мислення та аналітичних навичок у громадян, щоб вони могли адекватно оцінювати інформацію. Надзвичайно важливо розробляти та впроваджувати ефективні механізми захисту від дезінформації та інших форм інформаційної агресії.

Отже, глобальні соціальні трансформації та події, які відбулися в кінці XX століття, потребують об'єктивного аналізу інформаційного середовища на міжнародному рівні. До цього моменту питання інформаційної безпеки в нашій країні не лише не вивчалося, але і в загальному ігнорувалося. Раніше вважалося, що можна забезпечити безпеку шляхом суворої конфіденційності та обмежень. Проте, вже в 2014 році Україна стикалася з інформаційною агресією з боку Російської Федерації. Виклики, які виникли перед Україною, настановлюють населення здійснити негайні заходи для розробки нової

Доктрини національної безпеки України та модернізації всієї системи інформаційної безпеки держави.

Зараз інформація має визначальне значення для формування громадської думки, тому інформаційна війна стає значущим інструментом впливу на різні аспекти, включаючи політичні, соціальні та військові процеси. Розуміння різних стратегій та підходів до інформаційної боротьби є ключовим для створення ефективних стратегій інформаційної безпеки та захисту національних інтересів та суверенітету. Дослідження в цій галузі та розробка нових підходів для протистояння інформаційним загрозам залишаються актуальним завданням для наукової спільноти та їхнього практичного використання в реальних умовах.

Загальний висновок полягає в тому, що інформаційні війни є невід'ємною частиною сучасних міжнародних відносин і продовжують еволюціонувати, адаптуючись до нових технологій і сучасних викликів. Роль різних акторів, зокрема держав та неурядових організацій, стає все більш важливою у цьому контексті. Важливою складовою адаптації держав є вміння боротися з кібершпигунством та фейковими новинами, що може впливати на інформаційну безпеку країн та їхню інтернаціональну репутацію. Україна є яскравим прикладом країни, яка стикалася з інформаційними війнами на власному досвіді та висловила певні вчення з подолання цих викликів. Досягнення та недоліки України у цьому контексті важливі для подальшого розуміння та вирішення проблем інформаційних війн в міжнародних відносинах.

ДОДАТКИ

Термінологічний словник

1) EBSCOhost - доступні через вебінтерфейс бази даних наукової інформації з галузей медицини, фізики, хімії, економіки та інших наук, що періодично оновлюються.

2) GoogleScholar або Google Академія - пошукова система вільного доступу, яка індексує повний текст наукових публікацій всіх форматів і дисциплін.

3) JSTOR - цифрова повнотекстова база даних англомовних наукових журналів.Доступ до статей надається здебільшого для корпоративних організацій (таких як університети, дослідницькі центри тощо) за платну передплату.

4) StopFake - український інтернет-проект, створений у 2014 році, який займається фактчекінгом. На сайті проєкту публікуються відомості про фейкові новини з різних джерел і пояснюється, чому матеріали не відповідають дійсності.

5) Інформаційна безпека - стан інформації, в якому забезпечуєтьсязбереження визначених політикою безпеки властивостей інформації.

6) Інформаційна війна - використання і управління інформацією з метою набуття конкурентоздатної переваги над супротивником.

7) Інформаційна зброя - сукупність спеціалізованих (фізичних, інформаційних, програмних, радіоелектронних) методів і засобів тимчасового або безповоротного виводу з ладу функцій і служб інформаційної інфраструктури в цілому або окремих її елементів.

8) Інформація - це нові відомості, які прийняті, зрозумілі і оцінені її користувачем як корисні.

9) Кібершпигунство - термін, що позначає, як правило, несанкціоноване отримання інформації з метою отримання особистого,

економічного, політичного чи військової переваги, здійснюваний з використанням обходу(злому) систем комп'ютерної безпеки, з застосуванням шкідливого програмного забезпечення, включаючи «троянських коней»і шпигунських програм.

10) Пропаганда - форма комунікації, спрямована на поширення фактів, аргументів, чуток та інших відомостей для впливу на суспільну думку на користь певної спільної справи чи громадської позиції.

11) Троянські програми, трояни, троянці (англ. Trojan Horses, Trojans) — різновид шкідницького програмного забезпечення, яке не здатне поширюватися самостійно (відтворювати себе) на відміну від вірусів та хробаків, тому розповсюджується людьми.

12) Фейк - підробка, фальсифікація. Спершу даний термін почав вживатися в мережі інтернет, а потім почав широко використовуватись і у повсякденному житті. Так, наприклад, поряд з часто вживаними виразами «фейкова сторінка», «фейковий аккаутн», «фейковий сайт» також можна почути вирази «фейкові продукти», «та він фейк» (про людину) та інші.

13) Шкідливий програмний засіб (англ. malware - скорочення від malicious - зловмисний і software - програмне забезпечення) - програмне забезпечення, яке перешкоджає роботі комп'ютера, збирає конфіденційну інформацію або отримує доступ до приватних комп'ютерних систем. Може проявлятися у вигляді коду, скрипту, активного контенту, і іншого програмного забезпечення.

14) Шпигунський програмний продукт (англ. spyware) - це програмний продукт особливого виду, що встановлений і вживається без належного сповіщення користувача, його згоди і контролю з боку користувача, тобто несанкціоновано встановлений. Саме у цьому вузькому сенсі термін шпигунський програмний продукт є дослівним перекладом англійського терміну spyware [24] [13].

СПИСОК ВИКОРИСТАНИХ ДЖЕРЕЛ

1) 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. 532 с.

2) Арістова І. В. Державна інформаційна політика: організаційно-правові аспекти /за заг. ред. О.М. Бандурки. Харків: Університет внутрішніх справ 2016. 366 с.

3) Богуш В. М. Інформаційна безпека держави. Київ: МК-Прес, 2005. 432 с.

4) Бондарсук О. В. Відображення у дискурсі ЗМІ пропагандистських кампаній. *Political science*. № 12 (104). 2013. С. 56-66.

5) Валюшко І. О. Основні виклики і загрози в епоху інформаційних війн. *Науковий вісник Дипломатичної академії України*. Зовнішня політика і дипломатія: традиції, тренди, досвід. Частина ІІ. Серія «Політичні науки». 2016. С. 157-162 .

6) Васильчук Г.М., Маклюк О.М., Бессонова М.М. Феномен пропагандита антипропаганди у сучасному світі: історико-політологічний дискурс. Запоріжжя: Інтер-М, 2018. 386 с.

7) 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, Харків, 2012, 75 с.

8) Додонов А. Г., Горбачик Е. С., Кузнєцова М .Г. Сучасні технології та проблеми інформаційної безпеки. Інформаційні технології та безпека: Збірник наукових праць. Київ: Інститут проблем реєстрації інформації НАН України, 2006. 259 с.

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

10) Іваницька Б. Основні методи пропаганди в російському інтернет ЗМІ pravda.ru. *Вісник Національного університету «Львівська політехніка».* Серія: Журналістські науки. 2018. № 896. С. 46-58.

11) Конах В. К. Сучасні тенденції в захисті національних медіапросторів від російської пропаганди. Національний інститут стратегічних досліджень, *Стратегічні пріоритети*. 2016. С. 27-38.

12) Кондратюк М. О. Інформаційна війна та роль мас-медіа в міжнародних конфліктах. *Вісник Харківської державної академії культури.* 2013. Вип. № 41. С. 3-11.

13) Копаль О.С., Павленко Ю.В. Інформаційна війна: проблеми та перспективи. Київ: НАДУ, 2015. 192 с.

14) Кулеба Д. І. Війна за реальність, як перемагати у світі фейків, правд та спільнот. 2019. Київ: Видавничий дім «Київ-Могилянська Академія». С. 384.

15) Леонтьєва Л.Є. Пропаганда як інформаційно-психологічний складник політичних процесів. Львівський нац. ун-т ім. Івана Франка. Львів, 2004. 298 с.

16) Ліпкан В. А., Максименко Ю. Є., Желіхолський В. М. Інформаційна безпека України в умовах євроінтеграції. 2006. Київ: КНТ. 280 с.

17) Магда Є. Виклики гібридної війни: інформаційний вимір. *Наукові записки Інституту законодавства Верховної Ради України*. 2014. № 5. С. 138-142.

18) Малькова Т. В. Маси. Еліта. Лідер. / Т. В. Малькова. Харків.: Яуар, 2015. 232 с.

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

20) 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. К.: НАУ, 2022. 142 с.

21) Петрик В. М., Бедь В. В., Присяжнюк М. М. та ін. Інформаційно-психологічне протиборство: підручник.. Київ: ПАТ «ВІПОЛ», 2018. 386 с.

22) Пєвцов Г.В. Інформаційна безпека у воєнній сфері: проблеми, методологія, система забезпечення: Монографія. Харків: Цифрова друкарня № 1, 2013. 272 с.

23) Політологічний енциклопедичний словник. / Укладачі: Л.М. Герасіна, В.Л. Погрібна, І.О. Поліщук та ін. Ред. М.П. Требін. Харків: Право, 2015. 32 с.

24) Почепцов Г. Г. Сучасні інформаційні війни. Київ: Видавничий дім «Київ-Могилянська Академія», 2015. 498 с.

25) Прибутько П.С. Інформаційні впливи: роль у суспільстві та сучасних воєнних конфліктах. Київ: Вид. А. В. Паливода, 2007. 252 с.

26) Присяжнюк М. Аналіз засобів ведення інформаційної боротьби з використанням інформаційних технологій, форм і способів їх застосування. *Вісник Київського національного університету імені Тараса Шевченка.* Сер. Військово-спеціальні науки. 2007. №14. С. 31- 48.

27) Притула А. М. Пропаганда – компонент гібридної війни: шляхи протидії засобами кримінального права. *Юридична наука*. 2015. № 3. С. 113-122

28) Радковець Ю.І. Ознаки технологій «гібридної війни» в агресивних діях Росії проти України. *Наука і оборона*. 2014. № 3. С. 45-55.

29) Рак О.А., Шпот С.І.,Бардас І.В. Інформаційна війна: фактори, причини, наслідки за ред. О.А. Рака. Київ: Видавничий дім «Ін Юре», 2017. 62 с.

30) Рибак М. І., Атрохов А. В. До питання про інформаційні війни. *Наука і оборона*. № 2. 2018. С. 65-77.

31) Рижиков М. М. Міжнародна інформаційна безпека: Сучасні виклики та загрози. К.: Центр вільної преси, 2015. 916 с.

32) Рижков М. Інформаційна війна. Політична енциклопедія. Левенець Ю. Шаповал Ю. та ін. Київ: Парламентське видавництво, 2011. 298 с.

33) Саєнко О.Г. Інформаційна війна як прояв інформаційного

протиборства. Збірник наукових праць Військового інституту Київського національного університету ім. Т. Шевченка. 2008. Вип. 12. 147 с.

34) Синчак Б. Прямоефірна інформаційна війна та російсько-українська війна 2022-го на медійному плацдармі. Український інформаційний простір. 2022. № 2(10). С. 88-97.

35) Слюсаревський М. М. Термінологічний словник російськ-оукраїнської війни. Київ: НАПН України, 2022. 20 с.

36) Смолій В.О., Романова О.Г. Інформаційна війна в Україні: проблеми та виклики. Київ: НАДУ, 2016. 213 с.

37) Солодка О. М. Пріоритети удосконалення інформаційної безпеки України. *Інформація і право*. 2015. С. 36-42.

38) Стругацький В. Маніпулятивні практики на тлі гібридної війни: Філософський аналіз. Київ: ФОП Халіков Р.Х., 2018. 166 с.

39) Ткач В.Ф. Спецпропаганда як інформаційний складник гібридної війни Росії проти України. *Стратегічні пріоритети*. Київ: Національний інститут стратегічних досліджень, 2016. 109 с.

40) Ткач Д.І. Розвиток інформаційного суспільства: В 10-ти томах. Т.10: Інформаційно-комунікаційні аспекти міжнародної та національної безпеки: колективна монографіяза наук.ред.: Університет економіки та права "КРОК", 2013. 342 с.

41) Толубко В.Б. Підготовка і ведення інформаційної боротьби в Збройних Силах України: Навчальний посібник. Київ: НАОУ, 2004. 280 с.

42) Трофименко О.Г., Дубовой Я.В. Еволюція поглядів на інформаційні війни в епоху інформаційного суспільства. Порівняльно-аналітичне право: електронне наукове фахове видання. Ужгород, 2017. № 1. С. 189–192.

43) Чирва Р. Інформаційна війна – зброя, страшніша за ядерну. *Профспілкові вісті*. 2014. № 13.С.2- 14.

44) Чистоклетов Л. Г. Інформаційно-психологічні впливи як невід’ємна складова парадигми інформаційної безпеки. Науковий вісник Львівського державного університету внутрішніх справ. 2012. 192 с.

45) Шпига П.С. Основні технології та закономірності інформаційної війни. Проблеми міжнародних відносин. 2014. Вип. 8. 339 с.

46) Шуляк Н. Інформаційні війни в інтеграційних процесах. Міжнародні інтеграційні процеси: історичний досвід, сучасні виклики та перспективи. 46 с.

47) Яковлєва Н. І. Пропаганда як складова політичної комунікації: автореф. дис. канд. політ. наук: 23.00.02; Київ. нац. ун-т ім. Т. Шевченка. Київ, 2010. 18 с.

48) Горбань Ю. О. Інформаційна війна проти України та засоби її ведення. *Вісник НАДУ*. 2015. Вип. № 1 URL: http://visnyk. academy.gov.ua/wp-content/uploads/2015/04/20.pdf

49) Доктрина інформаційної безпеки України: Затв. указом Президента України від 8 лип. 2009 р. № 14/2009. URL: http://zakon.rada.gov.ua/laws/show/514/2009

50) Єрмоленко В. (Інтерньюз-Україна) Слова та війни: Україна в боротьбі з російською пропагандою: аналітичне видання. Київ: К.І.С., 2017 URL:https://issuu.com/internews-ukraine/docs/words_and_wars_ukr

51) Іжутова І. Мартін Лібікі: «Що таке інформаційна війна?» ВійськоУкраїни. 2014. URL : http://viysko.com.ua/texnologiji-voyen/martin-libiki-shhotake-informacijna-vijna

52) Малик Я. Інформаційна війна і Україна. Науковий вісник. 2015. Вип. 15. URL: http://www.lvivacademy.com/vidavnitstvo_1/visnyk15/fail/Malyk.pdf.

53) Мельник О. В. Інформаційна війна: теоретико-методологічні аспекти: URL: https://journals.iir.kiev.ua/index.php/npi/article/view/215/195

54) Патлашинська І. В. Сучасна російсько-українська інформаційна війна: завдання, методи та особливості використання. *Регіональні Студії*. 2022. № 84.URL: http://www.regionalstudies.uzhnu.uz.ua/archive/28/15.pdf

55) Петрик В. І. Сутність інформаційної безпеки держави, суспільства і особи. URL: http://justinian.com.ua/article.php?id=3222

56) Пропаганда vs контрпропаганда у медіа просторі: минуле, сучасне, майбутнє: матеріали міжнародної науково-практичної конференції (Запоріжжя, 12 лютого 2018 р.) Запоріжжя: Інтер-М, 2018. 406 с. URL:https://istznu.org/index.php/journal/article/view/243/192

57) Стратегія національної безпеки України. URL: http://zakon2.rada.gov.ua/laws/show/389/2012

58) Цуканова О.В. Інформаційні війни: вплив на суспільство. URL: http://www.sworld.com.ua/konfer34/800.pdf

59) Шевчук П. Інформаційно-психологічна війна Росії проти України: як їй протидіяти. *Демократичне врядування*. 2014. Вип. 13. URL: http://lvivacademy.com/visnik13/zmist. html

60) Bondarsuk O.V. Reflection in the discourse of the media of propaganda campaigns. *Political science*. No. 12 (104). 2013. P. 49-53. URL: http://example.com.

61) Cold War in Space: Reconnaissance Satellites and US-Soviet Security CompetitionURL:https://doi.org/10.4000/ejas.20427

62) Fake News and Information Warfare: An Examination of the Political and Psychological Processes From the Digital Sphere to the Real World URL:https://www.researchgate.net/publication/348129387

63) Ivanytska B. Basic methods of propaganda in Russian Internet media pravda.ru. *Journal of Lviv Polytechnic National University*. Series: Journalistic Sciences. 2018. No. 896. P. 54–58. URL: http://example.com.

64) Strategic Information Warfare: A New Face of War. RAND Corp, 2014. URL: http://www.rand.org/pubs/monograph_reports/MR661/index2.html.

65) The Ethics of Cyberweapons in Warfare URL:https://faculty.nps.edu/ncrowe/ethics_of_cyberweapons_09.htm