Міністерство освіти і науки України
Державний заклад «Південноукраїнський національний
педагогічний університет імені К. Д. Ушинського»

Кваліфікаційна наукова
праця на правах рукопису

Руцький Сергій Васильович

УДК 327.8(470+571)

ДИСЕРТАЦІЯ

«Інформаційне протиборство в сучасному світовому політичному процесі в умовах цифрової реальності»

052 – політичні науки
Подається на здобуття ступеня доктора філософії в галузі політології.
Дисертація містить результати власних досліджень. Використання чужих ідей, результатів і текстів мають посилання на відповідне джерело

_____
(підпис, ініціали та прізвище здобувача)

Науковий керівник
доктор політичних наук, професор
Наумкіна Світлана Михайлівна

Одеса – 2025

Анотація

Руцький С.В. ***Інформаційне протиборство в сучасному світовому політичному процесі в умовах цифрової реальності.*** **– Кваліфікаційна наукова праця на правах рукопису.**

Дисертація на здобуття ступеня доктора філософії за спеціальністю 052 – Політологія – Державний заклад «Південноукраїнський національний педагогічний університет імені К. Д. Ушинського», Одеса, 2025.

Дисертаційна робота присвячена комплексному, багатоаспектному та міждисциплінарному дослідженню феномену інформаційного протиборства, що є однією з найбільш визначальних та складних характеристик сучасного світового політичного процесу. Актуальність обраної теми дослідження є надзвичайно високою та зумовлена фундаментальними трансформаціями, які переживає людство на початку XXI століття. Ключовою рушійною силою цих змін є стрімкий та всеосяжний розвиток інформаційно-комунікаційних технологій, що призвело до формування якісно нової реальності – цифрового простору. Саме в цьому віртуальному середовищі розгортаються основні події політичного життя, формується громадська думка, здійснюється комунікація між політичними акторами та громадянами, а також все інтенсивніше проявляються різноманітні форми політичної конкуренції та конфронтації, які отримали загальну назву інформаційного протиборства.

Сьогодні інформаційний простір перетворився на стратегічно важливу арену боротьби за владу, вплив та ресурси. Традиційні форми політичного протистояння все частіше доповнюються, а іноді й повністю замінюються сучасними методами, що базуються на використанні технологічних інновацій у сфері зв'язку та інформатизації. Експертне співтовариство, як у галузі політичної науки, так і в сфері міжнародних відносин, одностайно визнає, що інформація набула безпрецедентної ролі, якісно змінюючи природу політичних процесів як на національному, так і на глобальному рівнях. Аналіз сучасних та прогнозування майбутніх міжнародних політичних відносин неможливі без глибокого розуміння сутності, механізмів та наслідків інформаційного

протиборства, мистецтво ведення якого стає ключовим фактором успіху в сучасному світі.

У цьому контексті виникає нагальна потреба в системному та всебічному дослідженні політичних процесів, що відбуваються в інформаційному просторі, а також у поглибленні цифрової політичної грамотності як політичних еліт, так і широких верств громадянського суспільства. Недостатнє розуміння сутності інформаційного протиборства, його методів та потенційних наслідків може призвести до прийняття неефективних політичних рішень, зростання соціальної напруги та дестабілізації політичних систем.

Дисертаційне дослідження є складовою частиною комплексної науково-дослідної теми кафедри політичних наук і права Державного закладу «Південноукраїнський національний педагогічний університет імені К. Д. Ушинського» в межах науково-дослідної теми «Сучасні виклики соціально-політичного розвитку: політико-правові та соціально-економічні виміри», що свідчить про його відповідність актуальним науковим пріоритетам та планам досліджень у галузі політичних наук.

Основною метою дисертаційної роботи є здійснення комплексного аналізу сутності, характерних рис, різноманітних форм, методів та ключових чинників інформаційного протиборства, що активно розгортається в сучасному світовому політичному процесі в умовах домінування цифрової реальності. Для досягнення поставленої мети передбачається вирішення низки взаємопов'язаних дослідницьких завдань, спрямованих на розкриття багатогранності досліджуваного феномену.

Об'єктом дисертаційного дослідження виступає інформаційне протиборство як складний соціально-політичний феномен. Предметом дослідження є особливості інформаційного протистояння в умовах збройного конфлікту, що розгортається в цифровій реальності.

Наукова новизна дослідження в цілому полягає у комплексному та системному підході до вивчення інформаційного протиборства в сучасному світі, що враховує специфіку цифрової реальності. В рамках роботи вперше

здійснено глибокий аналіз взаємодії трансформаційних процесів цифрового простору, змін у формах політичної комунікації та зростання латентних проявів політичної агресії в інформаційному середовищі. Запропоновано авторську концептуальну модель інформаційного протиборства в сучасному світовому політичному процесі в умовах цифрової реальності, яка інтегрує аналіз технологічних, політичних та соціокультурних детермінант інформаційного протистояння. Ідентифіковано та класифіковано новітні форми конфронтаційної поведінки суб'єктів політики в цифровому інформаційному просторі, а також розроблено теоретико-методологічні засади для розмежування понять «інформаційне протиборство» та «інформаційна війна» в контексті цифрової реальності. Уточнено роль та значення цифрової пропаганди, вплив інформатизації на ефективність інформаційних ефектів та розуміння інформаційного аспекту загроз у сучасному політичному процесі. Удосконалено розуміння загроз, пов'язаних з інформаційним аспектом, запропоновано авторське бачення феномену інформаційного протиборства та удосконалено аналіз конфронтаційної взаємодії суб'єктів політики в інформаційному просторі.

У дисертаційному дослідженні використано широкий спектр загальнонаукових та спеціалізованих методів дослідження, що забезпечило об'єктивність та наукову обґрунтованість отриманих результатів.

Практична значимість дисертаційної роботи є значною та полягає у можливості використання її результатів державними органами, політичними інститутами, засобами масової інформації, науково-педагогічними працівниками та громадськими організаціями для підвищення рівня обізнаності щодо проблем інформаційного протиборства та розробки ефективних стратегій протидії негативним інформаційним впливам на різних рівнях суспільно-політичного життя.

Апробація результатів дисертації здійснювалася на міжнародних та всеукраїнських наукових і науково-практичних конференціях. Основні ідеї,

положення та висновки дисертаційного дослідження викладені автором у ряді наукових публікацій.

Структура дисертаційного дослідження обумовлена метою та завданнями і складається зі вступу, трьох розділів, поділених на підрозділи, висновків до розділів, списків посилань та загальних висновків.

Ключові слова: цифрова реальність, цифрова пропаганда, мережева війна, інформаційна війна, інформаційне протиборство, інформаційний простір, політичні кіберконфлікти, кібербезпека, політичні технології, інформаційний простір, політичний вплив, політична активність, політична комунікація, інформаційна безпека, політичні загрози.

Abstract

Rutskyi S.V. ***Information confrontation in the modern world political process in the context of digital reality.*– Qualifying scientific work as a manuscript.**

Dissertation for the degree of Doctor of Philosophy in the specialty 052 – Political Science – State Institution "South Ukrainian National Pedagogical University named after K.D. Ushynsky", Odesa, 2025.

The dissertation by Serhii Vasylovych Rutskyi undertakes a comprehensive, multifaceted, and interdisciplinary investigation into the phenomenon of information warfare, a defining and complex characteristic of the contemporary global political process, which is increasingly unfolding within the dominance of digital technologies and the global Internet network. The topicality of this research is exceptionally high, driven by the fundamental transformations humanity is undergoing at the beginning of the 21st century. A key driving force behind these changes is the rapid and all-encompassing development of information and communication technologies, leading to the formation of a qualitatively new reality – cyberspace. It is within this virtual environment that the main events of political life unfold, public opinion is formed, communication between political actors and citizens takes place, and various forms of political competition and confrontation, collectively termed information warfare, are increasingly manifested.

Today, the information space has transformed into a strategically important arena for the struggle for power, influence, and resources. Traditional forms of political confrontation are increasingly supplemented, and sometimes entirely replaced, by modern methods based on the use of technological innovations in the field of communication and informatization. The expert community, both in political science and international relations, unanimously recognizes that information has acquired an unprecedented role, qualitatively changing the nature of political processes at both national and global levels. The analysis of contemporary and the forecasting of future international political relations are impossible without a deep understanding of the essence, mechanisms, and consequences of information warfare, the art of conducting which is becoming a key factor for success in the modern world.

In this context, there is an urgent need for a systematic and comprehensive study of political processes occurring in the information space, as well as for deepening digital political literacy among both political elites and broad segments of civil society. An insufficient understanding of the essence of information warfare, its methods, and potential consequences can lead to the adoption of ineffective political decisions, increased social tension, and the destabilization of political systems.

The primary aim of the dissertation is to conduct a comprehensive analysis of the essence, characteristic features, diverse forms, methods, and key determinants of information warfare actively unfolding in the contemporary global political process under the dominance of digital reality. To achieve this aim, a series of interconnected research tasks are set, directed at revealing the multifaceted nature of the phenomenon under study.

The object of the dissertation research is information warfare as a complex socio-political phenomenon. The subject of the research is the specifics of information confrontation in the context of armed conflict unfolding in digital reality.

The scientific novelty of the research as a whole lies in the comprehensive and systematic approach to studying information warfare in the modern world, taking into account the specifics of digital reality. Within the framework of the work, a deep analysis of the interaction between the transformational processes of cyberspace,

changes in the forms of political communication, and the growth of latent manifestations of political aggression in the information environment is carried out for the first time. An author's conceptual model of information warfare in the contemporary global political process under the conditions of digital reality is proposed, integrating the analysis of technological, political, and socio-cultural determinants of information confrontation. Novel forms of confrontational behavior of subjects of the political process in the digital information space are identified and classified, and theoretical and methodological foundations for distinguishing between the concepts of "information warfare" and "information war" in the context of digital reality are developed. The role and significance of digital propaganda, the impact of informatization on the effectiveness of information effects, and the understanding of the information aspect of threats in the contemporary political process are clarified. The understanding of threats associated with the information aspect is improved, the author's vision of the phenomenon of information warfare is proposed, and the analysis of the confrontational interaction of subjects of politics in the information space is improved.

A wide range of general scientific and specialized research methods were used in the dissertation research, which ensured the objectivity and scientific validity of the results obtained.

The practical significance of the dissertation is significant and lies in the possibility of using its results by state authorities, political institutions, analytical centers, specialized structures responsible for information security, mass media, scientific and pedagogical workers, and public organizations to raise awareness about the problems of information warfare and develop effective strategies for countering negative information influences at various levels of socio-political life.

The approbation of the dissertation results was carried out at international and all-Ukrainian scientific and practical conferences. The main ideas, provisions, and conclusions of the dissertation research are presented by the author in a number of scientific publications.

The structure of the dissertation research is determined by the aim and objectives and consists of an introduction, three chapters divided into subsections, conclusions to the chapters, lists of references, and general conclusions.

Keywords: digital reality, digital propaganda, network warfare, information warfare, information confrontation, information space, political cyber conflicts, cybersecurity, political technologies, information space, political influence, political activism, political communication, information security, political threats.

Список публікацій здобувача за темою дисертації

Праці, в яких опубліковані основні наукові результати дисертації

1. Руцький *С. (2023)* Конфронтація взаємодії суб'єктів політики в інформаційному просторі. *Науковий журнал «Політикус».* №5. С. 82-86. URL: http://politicus.od.ua/5_2023/12.pdf
2. Руцький *С. (2024)* Ц*и*фрова пропаганда в аспекті сучасного інформаційного протиборства. *Вісник Львівського університету. Серія філос.-політолог. студії.* Випуск 55. С. 437–443. URL: http://fps-visnyk.lnu.lviv.ua/archive/55_2024/53.pdf
3. Руцький *С. (2025)* Медіаграмотність, як фактор розповсюдження політичної інформації. *Науковий журнал «Політикус*». №1. С. 94-100.

Праці, які засвідчують апробацію матеріалів дисертації

4. Руцький *С. (2023)* Загрози в сучасному політичному процесі: інформаційний аспект. *The 3rd International Scientific and Practical Internet conference «Modern Political Processes: Global and National Dimensions», Odesa, 2023. http://dspace.onua.edu.ua/handle/11300/26884*
5. Руцький С. *(2024)* Кіберконфлікти у протиборстві суб'єктів політики на території європейських країн. *Сучасні виклики соціально-політичного розвитку: політико-правові та соціально-економічні виміри: матеріали всеукраїнської науково-практичної конференції*, м. Одеса, 24 травня 2024 року. Одеса: ДЗ «Південноукраїнський національний педагогічний університет імені К. Д. Ушинського», Центр соціально-політичних досліджень «Politicus». С. 60-62. URL: http://dspace.pdpu.edu.ua/jspui/handle/123456789/dspace.pdpu.edu.ua/jspui/handle/123456789/19629
6. Руцький С. (*2024)* Особливості цифрової пропаганди в умовах воєнного стану. *Матеріали III Всеукраїнської наукової конференції «Державно-*

правові засади формування безпекового середовища в Україні в умовах сучасних викликів», Одеса, 2024. ОДУВС.

7. Наумкіна С., Руцький С. (2025) Парадипломатія як стратегічний інструмент боротьби з дезінформацією в умовах інформаційного протиборства. *Міжнародна наукова конференція «Сталий розвиток регіонів, міст та спільнот в умовах глобальних перетворень: виклики, можливості, сценарії майбутнього».* м.Одеса, 16-17 травня 2025 р. Одеса:ОНУ імені І. І. Мечникова. 2025.

Зміст

Вступ

Актуальність обраної теми дослідження полягає в тому, що відкриття нових інформаційних технологій суттєво вплинуло на процес протистояння політичних суб'єктів, які перейшли від традиційних форм протистояння до сучасних форм, заснованих на використанні технологічних винаходів у сфері зв'язку та інформатизації. На думку експертів, роль інформації як в теорії політології, так і в практиці міжнародних відносин створила якісно нову ситуацію. Її аналіз наочно показує, що стан і розвиток сучасних та майбутніх міжнародних політичних відносин багато в чому визначається мистецтвом ведення інформаційного протиборства. Тому виникає потреба в дослідженні політичних процесів в інформаційному просторі та поглиблення цифрової політичної грамотності політиків та громадян.

Зв’язок із науковими програмами, планами, темами. Тема і зміст дисертаційного дослідження є складовою частиною комплексної науково-дослідної теми кафедри політичних наук і права Державного закладу «Південноукраїнський національний педагогічний університет імені К. Д. Ушинського» в межах науково-дослідної теми «Сучасні виклики соціально-політичного розвитку: політико-правові та соціально-економічні виміри (№ державної реєстрації 0120U002016), одним із виконавців якої є дисертант.

Мета та завдання. Метою дослідження є визначення сутності, характерних рис, форм, методів та ключових чинників інформаційного протиборства, що розгортається в сучасному світовому політичному процесі в умовах цифрової реальності. Досягнення цієї мети передбачає розробку теоретико-методологічних засад для дослідження зазначеного феномену, виявлення новітніх тенденцій та проявів інформаційної конфронтації, а також визначення їхнього впливу на політичні процеси та безпеку на національному і міжнародному рівнях. Досягнення поставленої мети здійснюється за рахунок послідовного вирішення наступних дослідницьких завдань:

– дослідити бібліографію проблеми та визначити аспекти, які потребують дослідження;

– розробити теоретико-методологічні засади дослідження інформаційного протиборства в умовах збройного конфлікту чи війни;

– обґрунтувати концепцію інформаційної переваги як основу мережевої війни;

– визначити та проаналізувати алгоритми, форми та ключові умови реалізації інформаційних операцій;

– проаналізувати конфронтацію взаємодії суб'єктів політики в інформаційному просторі;

– охарактеризувати та вивчити прояви інформаційних атак в інформаційних протистояннях;

– визначити характерні ознаки та проаналізувати прояви цифрової пропаганди, як інструменту інформаційного протиборства.

Об'єктом дисертаційного дослідження є інформаційне протиборство. *Предметом* даного дослідження є особливості інформаційного протистояння в умовах збройного конфлікту в цифровій реальності.

Наукова новизна дослідження в цілому полягає в тому, що тема дисертації в запропонованому формулюванні розробляється вперше; в рамках розроблених теоретичних, методологічних і практичних питань інформаційного протиборства в умовах цифрової реальності. Також новизна в отриманих висновках та сформульованих практичних рекомендаціях щодо удосконалення підготовки та ведення інформаційної війни як засобу вирішення завдань України в військових операціях. Більш конкретно наукова новизна полягає в:

Вперше:

- Здійснено комплексний аналіз інформаційного протиборства в сучасному світовому політичному процесі в умовах цифрової реальності, що охоплює трансформаційні процеси в цифровому просторі, зміни у формах політичної комунікації та зростання латентних проявів політичної агресії в інформаційному середовищі. Дослідження вперше системно розглядає

взаємодію цих факторів та їхній вплив на характер, методи та інтенсивність політичного протистояння.

- Запропоновано концептуальну модель інформаційного протиборства в сучасному світовому політичному процесі в умовах цифрової реальності, яка інтегрує аналіз трансформаційних процесів цифрового простору (зокрема, поширення цифрової пропаганди, кіберконфліктів) з дослідженням еволюції політичної комунікації та зростанням гібридних форм політичної агресії. Модель вирізняється системним підходом до вивчення взаємодії технологічних, політичних та соціокультурних детермінант інформаційного протистояння.
- Ідентифіковано та класифіковано новітні форми конфронтаційної поведінки суб'єктів політичного процесу в цифровому інформаційному просторі, що виходять за межі традиційних методів інформаційного впливу. Виокремлено специфічні цифрові інструменти та стратегії, що використовуються для публічного підтвердження власної позиції (включаючи технології автоматизованого поширення наративів) та дискредитації опонентів (наприклад, використання deepfake-технологій, скоординованих кампаній дезінформації в соціальних мережах).
- Розроблено теоретико-методологічні засади для розмежування понять «інформаційне протиборство» та «інформаційна війна» в контексті цифрової реальності, що базуються на якісних критеріях інтенсивності впливу, характеру цілей (від політичної конкуренції до повного соціокультурного та політичного домінування) та ступеня використання цифрових технологій як основних засобів ведення конфлікту.

Уточнено:

- Уточнено роль та значення цифрової пропаганди як ключового інструменту сучасного інформаційного протиборства, розкрито її характерні ознаки в цифровому середовищі, такі як автоматизація, масштабованість та анонімність, а також поєднання технологій з креативністю операторів для швидкого створення та поширення пропагандистського контенту.

- Уточнено вплив інформатизації та діяльності в інформаційному просторі на ефективність інформаційних ефектів, підкреслено залежність політичної влади від здатності здійснювати інформаційне протистояння у зовнішній та внутрішній політиці в умовах швидкого поширення інформації та охоплення великих мас людей.

- Уточнено розуміння інформаційного аспекту загроз у сучасному політичному процесі, зокрема, шляхом аналізу конкретних прикладів кіберконфліктів на території європейських країн (згідно з публікацією автора), що ілюструють нові форми та методи інформаційного протиборства в цифровій реальності.

Удосконалено:

- Удосконалено розуміння загроз у сучасному політичному процесі, пов'язаних з інформаційним аспектом, зокрема, ризиків ескалації конфліктів, дестабілізації політичних систем та маніпулювання суспільною свідомістю за допомогою цифрових технологій.

- Запропоновано авторське бачення феномену інформаційного протиборства в умовах цифрової реальності, яке враховує як теоретичні аспекти проблеми, так і практичні прояви конфронтаційної взаємодії суб'єктів політики в інформаційному просторі, що відображено у наукових публікаціях автора.

- Удосконалено аналіз конфронтаційної взаємодії суб’єктів політики в інформаційному просторі шляхом дослідження конкретних механізмів та інструментів, які використовуються для публічного підтвердження власної позиції та дискредитації опонентів в умовах цифрової комунікації (що частково відображено у згадці про відповідну наукову публікацію автора).

Методи дослідження. У ході дисертаційного дослідження були використані загальнонаукові методи, такі як: аналіз, синтез, абстрагування, порівняння, узагальнення, історико-логічний підходи, метод аналогії, моделювання та формалізації, а також системний метод. Широке застосування отримали також методи політологічних досліджень, такі як: політичний аналіз;

контент-аналіз політичних та військових документів, спеціальної політичної літератури, архівних матеріалів, публікацій у засобах масової інформації; експертні опитування; експертні оцінки. Крім того, автор використовував спеціальні методи військової науки, такі як: узагальнення досвіду ведення воєн і операцій; аналіз досвіду навчань та військових ігор; методи військового прогнозування та ін., метод правового аналізу.

Методологічна складова наукового дослідження теми містить ряд методів, які допомагають привернути увагу до суспільно-важливих питань та створюють умови для ефективних висновків. Тому під час дослідження використано статистичний метод, він допоміг усвідомити сучасний стан конфронтації та кіберзагроз в інформаційному просторі, що створює умови для кібернетичного прояву небезпеки у формі кібервійни. Також метод моделювання, продемонстрував різні шляхи розвитку політичних процесів, для зменшення напруги у суспільстві та прояву проблематики в інформаційному середовищі, яка має вплив на політико-військові процеси. Разом з тим, використано порівняльний метод, що аналізує різні події, які уже продемонстрували суспільне обговорення з конструктивним варіантом вирішення, а метод спостереження показав, що українське суспільство використовує інформаційний простір для комунікації та розуміння політиковійськової ситуації у країні, тому виникає потреба у визначення ролі політичної грамотності в періоди конфронтації в інформаційному просторі.

Застосовані загальнонаукові та спеціалізовані методи дозволили проаналізувати особливості поняття цифрової пропаганди та дослідницькі методи впливу на масову свідомість громадян України. Було розглянуто характеристики змін політичного вибору під впливом абстракцій, спостережуваних через вивчення реакцій у соціальних мережах. Метод наукового аналізу використовувався для дослідження мереж з акцентом на вплив реакціонерів, а також для вивчення наукової літератури, що стосується теми дослідження.

У дослідженні використовуються такі методи, як критичний аналіз дискурсу, метод лінгвістичного спостереження, аналіз визначень словникових записів, кейс-метод, контент-аналіз.

Суть авторського підходу до вирішення проблем інформаційного протиборства в цифровій реальності полягає в його здатності орієнтуватися в складній динаміці конфліктної взаємодії між багатогранними системами. Визначено, що за допомогою методів моделювання можна висвітлити складну взаємодію факторів, що впливають на інформаційне протиборство, на його каскадний вплив на суспільне сприйняття та суспільно-політичну поведінку. Ключові компоненти нашого підходу охоплюють розробку моделей, можливості моделювання, інтеграцію даних та інструменти візуалізації.

Практична значимість дисертаційної роботи полягає у наступному:

- Для державних органів та органів безпеки: результати дослідження можуть бути використані для розробки стратегій інформаційної безпеки держави, виявлення та протидії деструктивним інформаційним впливам, зокрема цифровій пропаганді та кіберзагрозам. Аналіз новітніх форм конфронтаційної поведінки в цифровому просторі може допомогти у вдосконаленні механізмів захисту національних інтересів в інформаційній сфері.
- Для політичних інститутів та політичних партій: розуміння сутності та методів інформаційного протиборства в умовах цифрової реальності може сприяти розробці ефективних комунікаційних стратегій, спрямованих на формування позитивного іміджу, протидію політичній дезінформації та мобілізацію електорату в онлайн-середовищі.
- Для засобів масової інформації та журналістів: матеріали дисертації можуть бути корисними для підвищення рівня медіаграмотності, розуміння механізмів поширення фейкових новин та пропаганди, а також для вдосконалення стандартів журналістської етики в умовах інформаційного протистояння.

- Для науково-педагогічних працівників та здобувачів: теоретичні положення, аналітичні матеріали та висновки дисертації можуть бути використані в навчальному процесі при викладанні дисциплін політичних наук, міжнародних відносин, інформаційної безпеки та комунікативістики. Розроблені теоретико-методологічні засади можуть слугувати основою для подальших наукових досліджень у цій галузі.
- Для громадських організацій та активістів: результати дослідження можуть допомогти у розробці стратегій протидії дезінформації та маніпуляціям у громадському просторі, сприяти підвищенню рівня критичного мислення громадян та формуванню стійкості суспільства до негативних інформаційних впливів.

Таким чином, практична значущість роботи полягає в її здатності сприяти підвищенню рівня обізнаності щодо проблем інформаційного протиборства в цифровій реальності та надати інструменти для ефективної протидії його негативним наслідкам на різних рівнях суспільно-політичного життя.

Апробація результатів дисертації. Концептуальні положення, ідеї, дискусії та висновки дисертаційного дослідження представлялися та обговорювалися на міжнародних, всеукраїнських наукових та науково-практичних конференціях. Зокрема, прийнято участь в роботі The 3rd International Scientific and Practical Internet conference «Modern Political Processes: Global and National Dimensions» (Odesa, 2023); Всеукраїнської науково-практичної конференції «Сучасні виклики соціально-політичного розвитку: політико-правові та соціально-економічні виміри» (Одеса, 2024); III Всеукраїнської наукової конференції «Державно-правові засади формування безпекового середовища в Україні в умовах сучасних викликів» (Одеса, 2024); Міжнародної наукової конференції «Сталий розвиток регіонів, міст та спільнот в умовах глобальних перетворень: виклики, можливості, сценарії майбутнього», (Одеса, 2025).

Публікації. Основні ідеї, положення та висновки дисертаційного дослідження викладені автором у 7 публікаціях, 3 з яких надруковані у фахових

наукових виданнях із політичних наук та 4 публікаціях тез виступів нп матеріалах ауково-практичних конференціях.

Структура дисертаційного дослідження. Мета та завдання дослідження, логіка досягнення наукової мети визначили структуру дисертації, яка складається зі вступу, трьох розділів, які поділяються на підрозділи, висновків до розділів, списків посилань після кожного розділу, загального висновку до роботи. Загальна кількість використаних джерел складає 165 джерел. Загальний обсяг дисертаційного дослідження складає 229 аркушів (з них 22 аркуші – списки посилань).

Розділ 1
Концептуально-методологічні підходи дослідження інформаційного протиборства в умовах цифрової реальності

1.1. Бібліографія та розвиток наукових досліджень інформаційного протиборства та цифрової реальності.

Науковий напрям досліджуваної теми затребуваний викликами сьогодення. Трансформаційні процеси в цифровому простірі стають щоденною діяльністю із залученням великої кількості громадян, які активно підтримують сучасні тренди у різних галузях суспільно-політичного розвитку. Катаклізми, які переживає людство, також внесли корективи у форму людського спілкування, а тому суб'єкти політики перемістилися до інформаційного простору, який став головною платформою для політичної комунікації, а певні публічні механізми спілкування з іншими учасниками політичного процесу стали офіційними формами спілкування. В такому спілкуванні основною метою є публічне підтвердження об'єктивності власної позиції, її аргументованості у сучасних політичних процесах. Але й проявилася латентність окремих проявів політичної агресії щодо опонента. У зв'язку з цим, актуальним є дослідження щодо конфронтаційної поведінки суб'єктів політичного процесу на стадії безпосереднього протиборства, яке відбувається в інформаційному просторі, адже усі публічні процеси демонструють ступінь небезпеки та потребу у протидії, або навпаки – зниження інформаційної активності, як ознаки суспільної байдужості щодо об'єкта протиборства.

Загальна характеристика інформаційного протиборства свідчить про те, що це цілеспрямоване використання інформації для досягнення політичних, економічних, військових та інших цілей, воно притаманне людському суспільству з моменту його виникнення. Сьогодні є активний науковий інтересу до цієї проблеми, що пояснюється різким зростанням ефективності

інформаційних ефектів у зв'язку з інформатизацією та діяльністю в інформаційному просторі. В сучасних умовах постійно розвиваються технології, які не тільки збільшують обсяг та швидкість поширення інформації. Вони надають можливість інформаційного охоплення величезних мас людей в найкоротші терміни. Спостерігаємо залежність політичної влади від здатності здійснювати інформаційне протистояння у зовнішній і внутрішній політиці.

Слід зазначити, що досвід використання інформаційних потоків і ресурсів різними державами під час військових операцій, війн чи збройних конфліктів дозволяє говорити про те, що цілеспрямоване використання інформаційних засобів стає одним з вирішальних чинників, які не тільки сприяють перемозі чи поразці, але і здатних запобігти відкритому збройному протистоянню. Прорахунки в питаннях інформаційного протиборства, організації та використання інформації, інформаційних засобів і технологій з боку держави, ескалації військових дій в Україні, на тлі постійної підвищеної інформаційної активності сепаратистів, суттєво сприяли досягненню цілей деструктивних сил під час окупації Криму та частини Донбасу.

Слід зазначити, що на сьогодні в українській та зарубіжній політичній, філософській, соціологічній, військовій та іншій науковій літературі існує значна кількість ідей та обґрунтованих пропозицій теоретичного та практичного характеру, що стосуються проблем цілеспрямованого використання інформації, інформаційних засобів та технологій у ході досягнення політичних, економічних, соціальних, військових та інших цілей. Положення та висновки, викладені в дисертації, ґрунтуються на фундаментальних та прикладних дослідженнях вітчизняних та зарубіжних авторів, безпосередньо пов'язаних з проблемами інформаційного протистояння в політиці та військовій справі.

Ступінь наукового розвитку теми безпосередньо пов'язана з підвищеною увагою до питань інформаційної проблематики в цілому, інформаційного протистояння зокрема, що в останнє десятиліття призвело до появи великої кількості монографій і дисертаційних досліджень, наукових статей і публікацій

у періодичній пресі з цього питання. За змістом їх можна розділити на три основні групи.

Група 1: Дослідження, присвячені загальним аспектам цифровізації та інформаційного суспільства.

Почнемо з колективної монографії «Базові аспекти цифровізації та їх правове забезпечення» (К. В. Єфремова, Д. І. Шматков, В. П. Кохан та ін.), в якій автори дослідили правовий аспект «забезпечення цифрової трансформації суспільства та економіки, серед яких розкриті питання контролю та управління цифровими інфраструктурами, розвитку цифрових навичок і компетенцій як базових аспектів цифрової економіки». В роботі вченими представлено «дослідження з актуальних напрямків правового забезпечення цифрового суверенітету, визначені аспекти права інтелектуальної власності в змісті цифрової компетентності, правове регулювання цифрових платформ та актуальні питання обробки та обігу даних у цифрових інфраструктурах, новітні підходи до регулювання цифрових інформаційних послуг, розкриті конкурентні переваги та конкурентоспроможність цифрових підприємств тощо» [4].

В 2017 році вийшла монографія «Інформаційне суспільство в світі та Україні: проблеми становлення та закономірності розвитку». Монографія містить «теоретико-методологічні, концептуальні та праксеологічні засади становлення і розвитку інформаційного суспільства в Україні та світі». Автори особливу увагу приділили «питанням еволюції від homo sapiens до homo informaticus в контексті антропологічних вимірів, управлінню науково-освітнім простором інформаційного суспільства, еволюції та інформаційного суспільства в «суспільство знань» та закономірностям становлення smart-суспільства» [30].

Також у 2017 році маємо монографію М. Кириченка «Формування ідеології інформаційного суспільства в умовах глобальної інформатизації: тенденції, парадигми, перспективи розвитку», де автор спрямував свій аналіз «концептуалізацію когнітивно-комунікативних та інформаційно-семіотичних вимірів ідеології інформаційного суспільства у гуманітарно-науковому

дискурсі XXI століття. В роботі досліджено ідеології інформаційного суспільства, що формується на основі інформаціоналізму, в контексті якого здійснюється оптимізація напрямів становлення і розвитку ідеології інформаційного суспільства, яка ще не сформована в Україні» [36]. Науковець є автором багатьом наукових публікацій за тією тематикою, які також були проаналізовані на етапі дослідження бібліографії предмета даної дисертаційної праці. Це публікації, які направлені на аналіз інформаційно-семіотичних вимірів інформації в рамках інформаційного суспільства, питання цінностей мережево-онлайнової культури в віртуальній реальності та ін. [33; 34; 35].

Серед монографічних досліджень в 2021 році вийшла колективна праця під редакцією А. Кротюка «Війни інформаційної епохи: міждисциплінарний дискурс. В дослідженні представлено розуміння «сучасної війни в онтологічному, культурно-історичному, структурно-функціональному, аксіологічному вимірах. У даному виданні на системній основі поєднані різнорівневі методологічні підходи до дослідження основних аспектів збройного протиборства в інформаційному просторі». Вчений визначає, що «сутність ключових категорій безпекової сфери слід розглядати крізь призму інтерсуб'єктивної філософської парадигми» [10].

В рамках дослідження цифрового суспільства можна зазначити наукові розробки Ю. Крилової, яка висвітлює «проблеми формування інформаційного (цифрового) суспільства. Досліджено основні проблеми впровадження інформаційно-комунікаційних технологій у сфери життєдіяльності сучасного суспільства та держави» [39].

Група 2: Дослідження, що фокусуються на інформаційному протиборстві та інформаційній безпеці.

Слід відзначити монографію під авторством П. Лісовського та Ю. Лісовської, яка вийшла в 2024 році «Воєнна мережева криптосистема: державотворчий інноваційний контекст». В монографії з позиції історичного підходу досліджуються «латентні війни другої половини XX століття, між тодішнім СРСР та іншими державами світу, як формування криптосистеми

управління в міжнародному лідерському процесі». В роботі проанадізовано «клановий олігархат у біогенному середовищі, в якому контррозвідувальний режим відіграє особливу роль щодо вирішення епідеміологічної безпеки у державотворчому процесі. При цьому, особливу увагу звернуто на квантову комп'ютеризацію як інноваційно-цифрову комунікацію криптосистеми державотворення». Автори сходяться на думці, що «в умовах війни, виникнення якісно нового лексико-семантичного стану особи та суспільства як рушій нейробіолінгвістичного контролю щодо дифузії державної влади в системі сучасної ентропії» [42].

Серед наукових публікацій цього напрямку слід зазначити розробки таких науковців як О. Доренський, О. Улічев, К. Задорожний, які досліджують проблеми «підвищення ефективності інформаційного протиборства, що проводиться координаційним органом з питань національної безпеки і оборони – центром протидії дезінформації» [22].

У 2018 році загальне розуміння інформаційно-психологічного протиборства викладено у підручнику такими вченими як В. Петрик, В. Бедь, М. Присяжнюк та ін. У підручнику розкриваються «концептуальні основи інформаційної безпеки держави та еволюція інформаційно-психологічного протиборства. Розглядаються особливості сучасного етапу інформаційно-психологічного протиборства» [31].

Генеза інформаційної безпеки аналізується в публікаціях М. Шевчука з позиції права. Зокрема, автор акцентує увагу на розгляді «інформаційної безпеки як складової національної безпеки» [75]. Слід відзначити наукові публікації В. Котлярова, який в своїх роботах досліджує «питання щодо стратегічного управління інформаційною безпекою України» [38].

Неординарний напрямок дослідження ризиків формування нових форм тиску як прояви цифрового тоталітаризму представлений в публікаціях С. Наумкіної [48]. Проблеми аналізу сучасних загроз кібертехнологій у політичному процесі представлені в статтях А. Пехник та Ю.Завгородньої [54]. Зокрема, Ю. Завгородня робить акцент на аналізі кіберконфліктів як елеменут

політичних технологій в інформаційному просторі [23]. Питання розуміння «інформаційної війни» розкривається в публікаціях І. Пронози [57; 58]. В цьому ж напрямку працює І. Фещенко, який аналізує інформаційну війну, як складову збройно-політичного конфлікту [73].

Філософське дослідження інформаційної війни в рамках медіапростору представлено в публікаціях О.Данильян та О.Дзьобань. Науковці розглядають інформаційну війну, як складну технологію соціального маніпулювання, яка реалізується завдяки ЗМІ [15; 16; 17]. Аналіз ЗМІ в умовах інформаційної війни представлений в публікаціях Н.Аксьонової [1]. Важливі аспекти «застосування засобів масової інформації у інформаційно-психологічній війні» представлено М.Браїловським, Т.Пірцхалавою, В.Хорошко та В.Хохлачовою [24]. Цікаві висновки містяться в публікаціях О.Курбана, який проаналізував питання «бойових наративів в системі сучасних геополітичних інформаційних війн, на прикладі досвіду російсько-української гібридної інформаційної війни 2014–2021 рр.» [40]. Науковець грунтовно проаналізував питання «критичності мислення при споживанні медіаконтенту в умовах інформаційної війни» [41].

І. Юзова та П. Пацек досліджують «інформаційно-психологічний вплив противника та протидія йому в умовах ведення гібридних війн» [81]. Вербальним засобам інформаційно-психологічної війни присвячений аналіз В.Тарасової [68]. На питаннях «дискурсу політичної пропаганди в умовах інформаційно-психологічної війни» зосереджено публікації Н.Вітюка [9]. Особливостям «пропаганди в умовах інформаційно-психологічної війни» присвячує свій аналіз В.Алещенко [2].

Технологіям інформаційної війни присвячені публікації ААлімпієва, В.Баранніка, Т.Белікової, С.Сідченка, які аналізують «інформаційні атаки в сучасній гібридній війні» [70]. В цьому ж напрямку працюють О.Білобородов та А.Довгополий, які розглядають озброєння та військову техніку в аспекті технологій «інформаційно-психологічних війн та інформаційно-психологічна зброї [6]. О.Младьонова звернулася в своїх дослідженнях до аналізу «маніпулювання суспільною свідомістю як технологією ведення інформаційної

війни» [47]. Такий напрямок обраний і А.Стадником, який розглядає «інформаційну війну як комунікативна технологія впливу на масову свідомість та громадську думку» [66]. П.Шпига та Р.Рудник також досліджують «технології та закономірності інформаційної війни» [79]. Маніпуляціям, «як засібу інформаційно-психологічного впливу в інформаційній війні» присвятили свій аналіз О.Невельська-Гордєєва та В.Нечитайло [49]. А такі вчені, як О.Юдін, О.Матвійчук-Юдіна та О.Супрун досліджують «інформаційно-психологічну війну та технології соціального інжинірингу» [80].

За останні роки було видано навчальні посібники та підручники за цим тематичним напрямком. Зокрема, слід відзначити підручник «Інформаційна безпека», виданий колективом авторів у 2021 році [27]; «Інформаційна безпека у контексті сучасних технологій інформаційно-психологічного протиборства» та «Інформаційна безпека та кібербезпека держави», які були видані вже у 2025 році колективами авторів [28; 53].

Цікавим напрямком в рамках дослідження кібербезпеки є аналіз «протидії методам комп'ютерної лінгвістичної стеганографії», який проведений І.Федотовою-Півнем [72].

Група 3: Дисертаційні дослідження, присвячені інформаційній війні та інформаційній безпеці:

У 2012 році була захищена кандидатська дисертаційна робота О.Марунченко на тему «Інформаційна війна в сучасному політичному просторі», де автор досліджував процес «переміщення конфліктів із традиційного фізичного простору в кіберпростір». Вченим було визначено, що це «збільшує ризик виникнення локальних збройних конфліктів: технології інформаційної війни є привабливими саме через їхню відносну дешевизну, доступність та ефективність, а, отже, інтенсивність їх використання в політичній боротьбі буде тільки наростати». В дослідження також було проаналізовано «політичні чинники розгортання інформаційної війни всередині країни. Виявлено технічні фактори сучасного розвитку інформаційної війни» [44].

В 2014 році А.Руднєва представила дослідження на тему «Інформаційні війни як фактор впливу на політичну культуру в сучасній Україні», де було проаналізовано вплив «інформаційних воєн на політичну культуру сучасного українського суспільства». Авторка розглянула «сутність, методи, джерела впливу з точки зору конструктивних і деструктивних наслідків». В роботі зроблено висновок, що «активізація уваги до значимості ролі інформаційних впливів на демократизацію політичної культури посилюється в умовах трансформаційних процесів політичної системи України» [60].

У 2018 році була представлена робота Н.Семена «Російські інтернет-ресурси як чинник інформаційної війни проти України» (напрямок – соціальні комунікації). Автор роботи надав власне бачення «феномену інформаційної війни». На підставі окреслення поняття «інформаційної війни, вивчення організаційної бази функціонування російських інтернет-ресурсів та за результатами контент-аналізу публікацій на інтернет ресурсах виявлено ключові контентні характеристики цих публікацій як атрибутів інформаційної війни, чинниками якої і виступають дані веб-медіа». Вчений з'ясував «пропагандистський характер заголовків матеріалів та проаналізував антиукраїнський контент новин про події в Україні, що їх подають російські веб-ресурси правда.ру та российский диалог». В роботі також було окреслено «перспективи протидії інформаційній війні Росії проти України» [64].

Ще у 2018 році представлено до захисту роботу І.Валюшко на тему «Інформаційна безпека України в контексті російсько-українського конфлікту». В роботі «здійснено аналіз інформаційної безпеки України у контексті російської агресії. На основі різноманітних джерел та наукової літератури проаналізовано сутність інформаційної безпеки суспільства та держави в сучасній системі міжнародних відносин. Проведено аналіз факторів та передумов інформаційно-військової агресії російської федерації проти України, визначено основні її методи, інструменти» [7].

У 2020 році представлена дисертація Л.Верголяса на тему» Правове забезпечення спеціальних інформаційних операцій», де представлено правовий

погляд на проблеми та проаналізовано теоретичне визначення, обґрунтування та зміст «правового забезпечення та інформаційно-правових засад спеціальних інформаційних операцій, а також розробленню конкретних пропозицій щодо удосконалення правового забезпечення СІО» [8].

У 2021 році було здійснено дослідження А.Младьоновою на тему «Інформаційна війна і політика безпеки: політико-правовий вимір». Авторка роботи представила системне вивчення «інформаційних війн та засобів інформаційної безпеки з позицій сучасних теоретико-концептуальних напрацювань». В дослідженні «було введено значний масив науково-інформаційних джерел в науковий обіг, що дозволило найбільш повно розкрити природу та особливості перебігу інформаційних війн». Авторкою зроблено висновок, що «на сьогоднішній день проблеми виникнення та розвитку інформаційних війн та формування державами ефективних механізмів щодо запобігання їх згубному впливу на масову свідомість та психічний стан громадян є недостатньо розробленими в сучасній політичній науці» [46].

В 2023 році К.Захарченком було представлено дисертаційне дослідження на тему «Інституційний вимір інформаційної безпеки України: трансформаційні виклики, глобальні контексти, стратегічні орієнтири». Автором проаналізовано «основні тенденції процесу формування інформаційної безпеки в трансформаційному суспільстві, зокрема інституційний вимір такого процесу, роль державних і неурядових інститутів у забезпеченні інформаційної безпеки України» [26].

У 2023 році одеську школу політології поповнило дослідження В.Таркіна на тему «Інформаційні війни у сучасному політичному просторі як феномен XX-XXI ст.». В роботі автором проведений аналіз «інформаційних війн з позиції інтегрального підходу» [69].

У том же 2023 році представлено дисертаційне дослідження А.Колодки на тему «Механізми кризового менеджменту в умовах інформаційних загроз в гібридних середовищах» (ступень доктор філософії в галузі знань Публічного управління та адміністрування). В дисертаційній роботі «теоретично

узагальнено та вирішено завдання в галузі публічного управління щодо обґрунтування науково-теоретичних положень та розробки практичних рекомендацій з удосконалення механізмів кризового менеджменту в умовах ІЗ в гібридних середовищах» [37].

У 2023 році було представлено дисертацію С.Сунгурової на тему «Інформаційна війна як засіб політичного насилля» (на здобуття наукового ступеня доктора філософії у галузі знань 05 «Соціальні та поведінкові науки» за спеціальністю 052 «Політологія»). Метою даної роботи стало «розкриття сутності інформаційної війни як засобу політичного насилля, обґрунтування її теоретичних засад, інструментального забезпечення та особливостей практичної реалізації» [67].

У 2020 році В.Торічним було представлено докторську дисертацію на тему «Інформаційне забезпечення державної безпеки України в умовах трансформаційних викликів і загроз». Науковець ґрунтовно дослідив «сутність інформаційної політики як феномена інформаційного суспільства і забезпечення його безпеки за допомогою критеріїв систематизації та відповідних їм форм і видів інформаційного забезпечення національної безпеки» [71].

В 2021 році Б.Калініченко представлено дисертаційну роботу на тему «Роль засобів масової інформації в інформаційній війні: політичні детермінанти впливу та протидії». Головна увага приділена «дослідженню явища інформаційної війни і практичних засобів убезпечення від її наслідків та протидії негативним впливам, проаналізовано мінімізацію негативних наслідків впливу ЗМІ на індивідуальну та масову свідомість» [32].

У 2023 році захищено дисертаційну роботу «Гібридна війна як інноваційний феномен сучасної політики: український вимір». Її автор, О.Долженко, розкрив «суть гібридної війни, яке розуміють як різновид збройного конфлікту, що включає у себе політичну, ідеологічну, економічну, інформаційну та військову складові, необхідні для досягнення поставленої мети шляхом встановлення контролю над певною територією або соціальною

групою. На основі проведеного аналізу історичних етапів розвитку феномена гібридної війни встановлено причини його актуалізації та зроблено висновок, що цей феномен проявляє себе як одна із закономірностей розвитку людської цивілізації» [21].

В 2024 році відбувся захист дисертаційного дослідження Є. Міненка «Розвиток інститутів інформаційної безпеки сучасної України як чинник суспільно-політичної стабільності», де автор аналізує розвиток «інститутів інформаційної безпеки в Україні з огляду на їх роль у забезпеченні суспільно-політичної стабільності» [45].

Аналіз джерел з вказаної тематики свідчить про високу актуальність та значний науковий інтерес до дослідження інформаційного протиборства в сучасному суспільно-політичному просторі. Цей науковий напрям є затребуваним викликами сьогодення, зумовленими трансформаційними процесами в цифровий простір, змінами у формах політичної комунікації та зростанням латентних проявів політичної агресії в інформаційному середовищі.

Огляд окремих наукових праць (монографій та дисертаційних досліджень), проведений у тексті, демонструє різноманітність підходів та аспектів дослідження інформаційного протиборства. Досліджуються правові аспекти цифровізації, концептуальні основи інформаційної безпеки, еволюція інформаційно-психологічного протиборства, вплив інформаційних воєн на політичну культуру, роль російських інтернет-ресурсів в інформаційній війні проти України, питання інформаційної безпеки в контексті російсько-українського конфлікту, правове забезпечення спеціальних інформаційних операцій, політико-правовий вимір інформаційних війн та політики безпеки, інформаційні війни як феномен XX-XXI століть, механізми кризового менеджменту в умовах інформаційних загроз, інформаційна війна як засіб політичного насилля та роль засобів масової інформації в інформаційній війні.

Аналіз наукових праць також виявляє міждисциплінарний характер досліджуваної проблеми, що відображається у зверненні до філософських, історичних, правових, соціологічних та інших аспектів інформаційного

протиборства. Окремі дослідження зосереджуються на вивченні впливу інформаційних воєн на масову свідомість, розробці механізмів протидії негативним інформаційним впливам та дослідженні ролі криптосистем в інформаційному протиборстві.

Представлений огляд наукової літератури підкреслює, що, незважаючи на значний науковий інтерес та велику кількість досліджень, проблеми виникнення, розвитку та протидії інформаційним війнам та формуванню ефективних механізмів інформаційної безпеки залишаються актуальними та недостатньо розробленими в сучасній політичній науці. Це зумовлює необхідність подальших глибоких та комплексних досліджень у цій важливій сфері для забезпечення національної безпеки та стабільності суспільного розвитку в умовах зростаючої інформаційної активності та конфронтації.

1.2. Методологія дослідження інформаційного протиборства цифрової реальності в аспекті політичних процесів.

Останні досягнення в галузі інформаційних технологій і здатність організацій і окремих осіб використовувати можливості, які ці досягнення надають, глибоко змінюють природу світу, в якому ми живемо. Інформаційна епоха – це: зміна способу створення багатства; зміна розподілу влади; підвищення складності; скорочення відстаней по всьому світу; стиснення часу, що збільшує темп нашого життя.

Поява нової зброї породила нові терміни: «інформаційне протистояння», «інформаційні війни», «кібербезпека» тощо. Визначаючи дане поняття, слід зазначити, що в термінології даної сфери, з урахуванням динамічного розвитку інформаційних технологій, до сих пір відсутні єдині підходи і формулювання.

Виділимо основні групи теоретико-методологічних проблем та підходи до їх вивчення.

По-перше, це термінологічні та семантичні проблеми, які можна назвати «традиційними», оскільки їхнє коріння сягає XX століття. У цій області існує певний набір понять з недостатньо чіткою або такою, що перетинається семантикою. Ці поняття можна порівняти з відповідними англійськими термінами. Це «інформаційна війна», «психологічна війна», «інформаційно-психологічна війна». Додамо до цього терміни «інформаційне протистояння», «інформаційне протистояння», «інформаційна війна», які зараз використовуються в українській політиці. Різні автори використовують різні площини вираження для позначення однієї і тієї ж площини змісту. Наступна проблема в тому, що не встановлено загальноприйняту підпорядкованість термінів і явищ, що стоять за ними. Маються на увазі терміни «інформаційна операція», «інформаційно-психологічна операція».

По-друге, існують термінологічні та семантичні проблеми, породжені розвитком інформаційних технологій та змінами у військових стратегіях. Маємо терміни «кібервійна», «кіберзброя», «гібридна війна». У зв'язку з цим виникають питання про співвідношення інформаційної війни та кібервійни, інформаційно-психологічної війни та гібридної війни.

По-третє, це онтологічні проблеми, пов'язані з макросоціологічною інтерпретацією явища інформаційного протистояння або як норми, або як відхилення.

По-четверте, це деонтологічні проблеми інтерпретації явищ інформаційної війни, інформаційного протистояння, інформаційної операції. Проблеми такого роду пов'язані з розумінням відповідних явищ нормативним або об'єктивістським способом. Сюди ж ми віднесемо проблеми, пов'язані з використанням категорії «правда» в роботах, присвячених технологіям інформаційних операцій. До четвертої групи належать проблеми тлумачення впливу мінливого технологічного порядку на характер і характер інформаційних протистоянь і бойових інформаційних операцій.

До п'ятої групи належать проблеми побудови сучасної типології інформаційних протистоянь та інформаційних операцій. І, нарешті, шоста група

пов'язана з адекватним відображенням сучасного дискурсу технологічного, програмного та математичного забезпечення інформаційних протистоянь і захисту від інформаційних атак в сучасних мережевих комунікаційних структурах. Як правило, в одній предметно-тематичній хмарі існують військово-прикладні, геополітичні та політико-технологічні роботи з інформаційної війни, а в іншій – математичні, хоча необхідність зближення цих хмарних просторів очевидна.

Слід зазначити, що запропонувати повні варіанти вирішення кожної з виявлених проблем в рамках цієї роботи неможливо, але в даному дослідженні буде здійснено спробу відповісти на поставлені запитання на основі аналізу та узагальнення відповідної зарубіжної та російської літератури щодо інформаційних протистоянь та інформаційно-психологічних воєн. При цьому логіка нашої дискусії буде відповідати логіці послідовності теоретико-методологічних проблем, зазначеної вище.

Звернемося спочатку до базових понять і відразу зазначимо, що з середини XX століття терміни «війна» або «протистояння» найчастіше вживаються по відношенню до протистоянь в інформаційній сфері. При цьому склалися дві традиції, одна пов'язана з використанням поняття «інформаційна війна/інформаційне протистояння», інша оперує поняттям «психологічна війна». Основне поняття, яке нас цікавить в англомовних текстах, – це війна. На українську мову його можна перекласти по-різному, як війна, боротьба, протистояння, військові дії. Так роблять різні автори, обираючи ту величину, яка здається їм більш доречною. Щоб цього уникнути, звернемося до зарубіжних тлумачних словників. Наприклад, значення слова «війна» у словнику Webster [Warfare]: «Війна: 1. Військова служба; військове життя; змагання, що ведеться ворогами; бойові дії; війна. 2. Конкурс; З цього словникового визначення робимо висновок, що найбільш правильним перекладом словосполучення «інформаційна війна» буде «інформаційна війна» або «інформаційна війна». Переклад «інформаційна війна» також прийнятний, але його використання має бути конкретно обумовлене та обумовлене

особливостями ситуації, залученими акторами та засобами, що використовуються. Розмежування термінів «інформаційне протистояння» та «інформаційна війна» є тим більш важливим, що в англомовній науковій та військовій літературі, окрім «інформаційної війни», вживається ще й прямий термін «інформаційна війна».

У США з'явилося поняття «інформаційна війна», що використовується не як публіцистична метафора, а як повноцінний елемент термінологічного апарату стратегічного аналізу та військового планування. Вважаємо, що найбільш авторитетним джерелом є розробка корпорації RAND, прогнозно-аналітичної компанії, тісно пов'язаної з Пентагоном, в якій використовуються словосполучення «стратегічна інформаційна війна», а в більш ранніх випадках – «інформаційна війна». Поняття «інформаційна війна» офіційно використовується в Директиві Міністерства оборони США 3600 від 21 грудня 1992 року [Директива, 2013]. Документ фіксує намір керівництва Збройних Сил Сполучених Штатів Америки включити боротьбу в інформаційній сфері до числа стратегічних пріоритетів. Відповідно, на геополітичному рівні має бути поставлено питання про систему стратегічних військових операцій в інформаційному середовищі – «стратегічна інформаційна війна». Далі корпорація RAND на замовлення Пентагону розпочала дослідження у сфері інформаційної війни. Їх результати лягли в основу урядової концепції включення інформаційної війни в національну військову стратегію США, а через рік вони були представлені в MR-661-OSD (Strategic Information Warfare. Нове обличчя війни»). У цьому документі вперше знаходимо чітке визначення з офіційним статусом: «Стратегічна інформаційна війна – це використання державами глобального інформаційного простору та інфраструктури для проведення стратегічних військових операцій та зменшення впливу на власні інформаційні ресурси» [82].

Тут можна зробити перший висновок про те, що початковою категорією в досліджуваній предметній області є категорія інформаційного протистояння.

І. Проноза пропонує застосовувати психологічну парадигму, яка «дозволяє детально досліджувати механізми впливу на внутрішньоособистісні процеси індивідів, що викликає зміни в ментальній сфері, визначає корекцію логіки світосприйняття і відповідного йому політичної поведінки. В контексті соціально-комунікативного бачення проблеми можливе вирішення завдання по заповненню прогалин в знаннях про характер і способи інтеракций, що виникають між суб'єктами інформаційного протиборства. Геополітичний підхід дозволяє розглядати основні методи сучасної світової політики для досягнення політичної та економічної влади в мирний період. Конфліктологічний напрямок орієнтує на адекватну оцінку стратегічного значення інформації в досягненні домінуючих позицій як результату боротьби за владу, ресурси і політичний статус. Системний підхід дає релевантний інструментарій для комплексного дослідження інформаційної війни з урахуванням тісного взаємозв'язку її окремих елементів, їх рефлексії на дестабілізуючі чинники і тактик в рамках наступальних стратегій» [57].

На думку В.Шемчука, інформаційна війна представляє собою «суспільно-політичне явище, яке у політичному аспекті є продовженням домінуючих ідеологічних засад державної політики, що здійснюється за допомогою комплексу засобів інформаційно-технологічної індустрії, механізмів інформаційно-психологічного впливу на суспільство всередині держави чи населення країн-конкурентів в умовах політичного (воєннополітичного, економічного) конфлікту з метою формування в соціальному аспекті єдності суспільства, визначення його ідентичності та інформаційного захисту світоглядних цінностей, а також – деморалізації та фрагментації населення і силової компоненти держав-противників у межах глобального інформаційного простору» [77].

Історично склалося так, що інформаційне протистояння виникало в рамках збройної боротьби. Головною причиною його появи було прагнення атакуючої сторони підняти бойовий дух своїх солдатів і послабити волю противника. Пізніше інформаційне протистояння стало невід'ємною частиною

політики різних держав не тільки у воєнний, а й у мирний час (у дипломатичній, економічній та інших сферах).

Однак у попередніх військових зіткненнях, незважаючи на широке використання пропаганди та витончених методів дезінформації, вирішальну роль відігравало вогневе ураження противника. Розвиток інформаційного протистояння відбувалося за рахунок появи і масового поширення нових, більш ефективних носіїв і засобів доставки інформації в порівнянні з раніше існуючими. Інформаційні технології, все більш досконалі, все більш впевнено вторгалися в усі сфери життя суспільства. І, звичайно, вони вплинули на політичний процес. Результати цього впливу слід оцінювати двояко. З одного боку, спостерігається позитивна динаміка їх впливу на людину і суспільство, а з іншого – негативні тенденції, які відображають як складний характер взаємодії людини з новими комп'ютерними системами, так і спроби використання їх потенціалу для пропаганди насильства, тероризму, людиноненависницької моралі.

Таким чином, виник цілий ряд нових інформаційних загроз, що здійснюються за допомогою спеціально підібраної інформаційної системи і спрямованих на дестабілізацію суспільства. У політичній сфері відкриваються нові можливості для маніпулювання суспільною свідомістю, політичними установками та орієнтаціями різних соціальних груп. Технічні досягнення, їх широке проникнення і фактична доступність призводять до формування особливого світогляду. Віртуальна реальність суттєво трансформує сучасну політичну реальність.

В кінці XX століття і початку XXI століття важливим атрибутом перемоги є досягнення переваги в інформаційно-психологічній сфері. Термін «стратегічна інформаційна війна» з'явився наприкінці 1990-х років. Особливостями стратегічного інформаційного протистояння (СП) є відносно невисока вартість його коштів, відсутність статусу традиційних державних кордонів, складність виявлення початку інформаційної операції, а також виділення поля цієї операції в загальному потоці інформації.

Можна представити такі ключові особливості стратегічного інформаційного протиборства: відносно невисока вартість його коштів, відсутність статусу традиційних державних кордонів, складність виявлення початку інформаційної операції, а також виділення поля проведення цієї операції в загальному інформаційному потоці. Інформаційне протистояння – це вид протистояння з використанням всього спектру інформаційних можливостей, який спрямований на досягнення інформаційної переваги над противником у політичних, економічних та інших цілях. Низка держав відкрито проголосила курс на підготовку до інформаційної війни. Аналіз масштабів і змісту вжитих заходів, обсягів їх фінансування і військово-технічного забезпечення показує, що перевага в інформаційній сфері розглядається керівництвом цих держав як один з основних факторів досягнення цілей національної стратегії в конкретних умовах XXI століття.

Сучасний досвід проведення інформаційного протистояння дозволяє припустити, що його можна розглядати не тільки як специфічний спосіб незаконного ураження противника, а й як самостійну форму політичної боротьби. Інформаційно-психологічні методи впливу стають все більш масштабними та ефективними, за рахунок чого політичні суб'єкти все частіше використовуються для досягнення своїх цілей замість так званих «гарячих» воєн. У світовій практиці міждержавних відносин створюються умови не тільки для послідовного перетворення збройного протистояння в інформаційно-психологічне протистояння, а й для його трансформації в самостійний напрям зовнішньої політики розвинених держав.

Сформулювати наукове визначення поняття «інформаційне протиборство» досить складно. Це можна пояснити тим, що дане поняття пов'язане з іншими видами протистояння, зокрема, фізичним. Ключова обставина полягає в тому, що інформаційне протиборство має на увазі використання різних засобів і способів впливу на інформаційний ресурс опонента, захист і ефективне використання власного інформаційного ресурсу. Інформаційне протистояння в політиці представляється як змагальна взаємодія

політичних суб'єктів, в якій вони прагнуть завдати шкоди один одному за допомогою інформаційних та інших засобів і методів впливу, прагнучи при цьому захистити об'єкти власної інформаційної інфраструктури та інформаційного простору. А суть інформаційного протистояння полягає в конфліктній взаємодії соціальних суб'єктів (партій), які прагнуть досягти своїх політичних цілей за допомогою інформаційно-інформаційних засобів.

На думку дисертанта, інформаційне протиборство – це суперництво соціальних систем в інформаційно-психологічній сфері за вплив на певні сфери суспільних відносин і встановлення контролю над джерелами стратегічних ресурсів, в результаті чого одні учасники суперництва отримують необхідні для подальшого розвитку переваги, а інші їх втрачають. Дії учасників інформаційного протистояння можуть носити наступальний (агресія, війна) або оборонний характер. Важливим чинником виявлення, попередження та придушення зовнішньої інформаційної та психологічної агресії (війни) є державна інформаційна політика, яка в умовах безпосередньої загрози війни або на етапі реалізації противником своїх агресивних намірів набуває характеру системи профілактичних заходів щодо запобігання, виявлення та придушення агресії, а також заходів щодо застосування сил швидкого реагування та засобів придушення раптової агресії.

Слід звернути увагу на відмінності між двома поколіннями інформаційного протистояння. Якщо в першому поколінні під інформаційним протистоянням розуміти один з компонентів поряд з іншими засобами досягнення мети (ядерними, хімічними біологічне та ін.), друге покоління стратегічного інформаційного протистояння в умовах інформаційної революції трактується як довгостроковий (тижні, місяці та роки) вплив, що дає можливість в принципі відмовитися від застосування військової сили.

Під інформаційною війною розуміють інформаційне протистояння з метою завдання шкоди критично важливим структурам противника, дестабілізації його політичної та соціальної системи. Психологічна війна – це прихований вплив на свідомість всього населення або окремих його категорій,

що здійснюється спеціальними методами спотворення інформації або іншими технологіями, що впливають на процеси сприйняття світу і відключають раціонально-критичний рівень розуміння зовнішніх подразників.

У науковій літературі запропоновано два основні підходи до розгляду феномена інформаційної війни. На думку деяких дослідників, інформаційну війну слід аналізувати з урахуванням її впливу на масову свідомість, маніпулятивного потенціалу та психологічного впливу інформаційних повідомлень. Інформаційна війна – це автономна система в сучасному суспільстві, яку доцільно аналізувати за допомогою технічного, математичного понятійного апарату. Останнім часом виділився ще один підхід, що поєднує в собі два описаних вище підходи. Багато дослідників вважають цей підхід найбільш продуктивним.

Існує кілька тлумачень поняття інформаційної війни. Найбільш популярною з них є розуміння інформаційної війни як сукупності політичних, правових, соціально-економічних або подібних дій, які спрямовані на захоплення інформаційного простору, витіснення противника з інформаційної сфери, знищення його комунікацій, позбавлення його засобів передачі повідомлень, а також інші подібні цілі. Під інформаційною війною розуміють і найбільш гостру форму протистояння в інформаційному просторі. Акцент робиться на характері протистояння між суперниками. І тут першорядне значення мають такі властивості інформаційної взаємодії, як безкомпромісність, висока інтенсивність суперечки, а також короткочасний характер гострого суперництва. Це поняття тісно пов'язане з концепцією розгортання «сил спеціального призначення в медіа», сформованих і діючих за моделлю «спецназу». Однак ці сили озброєні медійною зброєю – цифровими камерами, супутниковими передавачами та іншими подібними засобами, які використовуються у суто військових цілях.

На думку експертів, інформаційна війна – це особливий тип відносин між державами, в якому для вирішення міждержавних протиріч використовуються методи, засоби і технології силового впливу на інформаційну сферу цих

держав. У науковій літературі описано кілька його різновидів. Придушення і знищення систем управління протиборчої сторони (Command-and-Control Warfare), спрямоване на фізичне знищення командних пунктів противника, порушення контролю його сил і засобів. Intelligence-Base Warfare, або стратегічна розвідка, спрямована на надання та використання інформації, зібраної інформаційними системами в ході бойових дій в системах командування та управління військами та озброєнням. Радіоелектронна боротьба спрямована на порушення функціонування каналів розповсюдження інформації протиборчої сторони та злам її криптографічного захисту.

Сам термін «інформаційна війна» вперше він був використаний Т. Роном у доповіді, яку він підготував у 1976 році для компанії Боїнг, під назвою «Системи озброєнь та інформаційна війна», де було зазначено, що інформаційна інфраструктура стає ключовою складовою американської економіки. Водночас вона стає вразливою мішенню як у воєнний, так і в мирний час. Публікація доповіді Т. Рона стала початком активної кампанії в засобах масової інформації. Сама постановка проблеми викликала великий інтерес у американських військових.

У дослідженні наводяться найбільш популярні формулювання поняття «інформаційна війна»: – це цілеспрямований вплив інформації (усної, друкованої, відео) на свідомість та емоційно-вольову сферу людей; – цілеспрямовані дії, що вживаються для досягнення інформаційної переваги шляхом нанесення шкоди інформації, інформаційним процесам та інформаційним системам при захисті власної інформації, інформаційних процесів та інформаційних систем .

Загалом, факти використання інформації для досягнення політичних і військових цілей можна зустріти ще багато років на початку нашої ери. Відомо, що Стародавній Єгипет часто вів війни, іноді програвав їх, але і в цьому випадку не переставав існувати як держава. Це свідчить про те, що у священників виробився певний принцип на випадок програшу війни, який умовно можна назвати «принципом культурної співпраці» з країнами-

переможницями. З появою засобів масової інформації та загальним зростанням рівня грамотності у XX столітті інформаційна війна стала більш ефективною. Яскравим прикладом ефективного інформаційного впливу на суспільну свідомість є діяльність головного ідеолога нацистської Німеччини Й. Геббельса. В цілому Третій Рейх надавав великого значення пропаганді як складовій частини кампанії по поневоленню інших народів збройними засобами. Тому в Німеччині було створено окремий департамент - Міністерство громадської просвіти і пропаганди, рейхсміністром якого був Геббельс. Діяльність цього відділу досі визнається зразком інформаційного впливу на маси в умовах війни. З подальшим розвитком IT-сектору інформаційна війна стала невід'ємною частиною сучасних військових кампаній. Наприклад, війну в Перській затоці обслуговували спеціальні фірми, що займаються зв'язками з громадськістю. Інформаційну кампанію під час війни в Іраку американські військові називають «інформаційно-психологічними операціями». «Міністерство оборони США заплатить приватним підрядникам в Іраку до 300 мільйонів доларів на виробництво політичних матеріалів, новин, розважальних програм і соціальної реклами для іракських ЗМІ, щоб залучити місцеві громади до підтримки Сполучених Штатів», – писала The Washington Post під час активної військової кампанії в Іраку.

З розвитком інтернету роль інформаційних технологій під час бойових дій зросла в рази. Завдяки цьому для інформаційної атаки на ворога сьогодні вже не обов'язково мати великі бюджети та величезну армію. Сьогодні боротьба в інформаційному полі не менш важлива, ніж прямі бойові дії. Інформаційна зброя стала ключовою у всіх конфліктах сучасності,

Хакерська війна – це проникнення в телекомунікаційні та інформаційні системи протиборчої сторони, що завдає шкоди їм і розташованим в них ресурсам. Економічна інформаційна війна ведеться з метою дестабілізації економіки шляхом встановлення економічної блокади або інформаційної агресії. Кібервійна спрямована на пошкодження інформаційних систем і розглядається насамперед як інформаційний тероризм. Психологічна війна, або

інформаційно-психологічна війна, пов'язана з впливом на психіку особистості. Вона передбачає інформаційно-психологічний вплив на населення, керівництво військами, політичних лідерів протиборчої сторони, операції з модифікації культури.

Інформаційно-психологічну війну як один з різновидів інформаційної війни правильніше називати інформаційно-психологічним протистоянням. В основі інформаційної війни лежить маніпулятивний вплив на аудиторію. Технології такого впливу різноманітні, але основні засоби універсальні – інформаційне повідомлення, що передається по каналах зв'язку. А від того, наскільки ефективно побудований меседж, залежить його маніпулятивний потенціал та ступінь впливу на аудиторію. Тому одним з найважливіших завдань для суб'єкта інформаційної війни є вміння кодувати повідомлення, що розповсюджуються в ході інформаційної війни.

В.Носов представляє наступне розуміння інформаційного протиборства: це така форма боротьби сторін, яка використовує «спеціальні політичні, економічні, дипломатичні, воєнні методи та засоби впливу на інформаційне середовище сторони, яка є противником, задля захисту «власного середовища та власних інтересів». На думку вченого, «інформаційне протиборство, залежно від виду операцій здійснюється на стратегічному, оперативному або тактичному рівнях за допомогою інформаційних засобів впливу, які застосовуються з метою нанесення відповідного інформаційного або психологічного впливу на середовище» [50].

В.Пилипчук виділяє такий термін як «глобальне інформаційне протиборство» і відзначає, що в «різних країнах світу активно розробляються і застосовуються на практиці інформаційно-психологічні засоби ведення глобального інформаційного протиборства. Насамперед, вони стосуються сфери використання інформації проти людського інтелекту». Вчений наводить американську термінологією, відповідно до якої «виділяються чотири основні категорії таких засобів». Сюди відносяться «операції проти волі нації, операції

проти командування противника, операції проти ворожих військ, операції на рівні національних культур» [55].

О.Даніл,ян та О.Дзьобань акцентують увагу на тому, що «інформаційна зброя є надзвичайно руйнівною і впливає на найважливіше – духовну сферу суспільства, і може бути віднесена до зброї масового ураження». Вчені зазначають, що «універсальність та ефективність інформаційної зброї зводить її в ранг абсолютної зброї, доступної для всіх організованих структур у мирний і, особливо, у воєнний час. Це єдина зброя, яка може бути використана приховано від супротивника. Треба розуміти, що в даний час інформаційна зброя становить серйозну небезпеку для будь-якої держави» [15].

Під інформаційним протиборством, на думку В. Шемаєва, слід розуміти «суперництво окремих людей, соціальних груп, державних чи міждержавних структур, країн або блоків країн в інформаційному просторі шляхом комплексних впливів на ті або інші суспільні відносини для встановлення контролю чи заволодіння життєво важливими ресурсами супротивника». В.Шемаєв визначає основні завдання інформаційного протиборства. До них він відносить здійснення цілеспрямованого впливу на людську свідомість і поведінку; досягнення переваг і безумовного лідерства в інформаційному просторі; створення сприятливих умов для переходу існуючої соціально-політичної системи до нової форми суспіль-них відносин». На думку вченого, «за допомогою ІП реалізується функція інформаційного стримування – управління кризовими ситуаціями шляхом превентивних інформаційних впливів на населення в зонах можливого виникнення конфлікту й ін.» [76].

Вчені І.Харченко, О.Сапогов, В.Шамраєв та А.Новіков виводять поняття інформаційного протиборства через поняття інформаційної переваги. На думку вчених, «вона являє собою здатність системи управління держави забезпечити стійкий процес своєчасного одержання достовірної інформації та доведення її до відповідних споживачів при одночасному отриманні можливості використання у своїх інтересах такої ж системи ймовірного противника або пониження ефективності роботи останньої. При цьому під такою системою

розуміють особовий склад та компоненти збирання, обробки, аналізу, кореляції, зберігання в пам'яті ЕОМ, відображення на дисплеях, записи на магнітних та інших носіях інформації, систематичного оновлення та уточнення, розподілу за пріоритетністю, передачі інформації споживачам. Для створення умов для досягнення інформаційної переваги необхідно вирішити п'ять взаємопов'язаних завдань. Перше завдання – створити інтегровану автоматизовану систему управління, зв'язку, розвідки та спостереження, що повинно значно підвищити фундаментальні можливості вирішення наступних завдань. Другим завданням є забезпечення примусового циркулярного доведення до виконавців важливої інформації в реальному масштабі часу та отримання конкретної інформації за запитами виконавців із баз даних вищих інстанцій. Третє завдання спрямоване на вирішення питань адекватного співробітництва у розподілі інформації, тобто на забезпечення командного складу штабів і військ за погодженою домовленістю необхідними засобами сполучення, отримання та розподілу інформації. Після вирішення четвертого завдання збройні сили одержують можливість спільного та узгодженого сприйняття та відображення різними командними інстанціями реальної оперативної ситуації, що дає можливість полегшити прийняття рішень, що відповідали б реальній ситуації, організацію та підтримку взаємодії під час операції. Вирішення п'ятого завдання, що полягає у можливості використання систем в інтересах радіоелектронної війни, зокрема усіх засобів боротьби з системами бойового управління противника, в цілому повинне дати можливість досягнення інформаційної переваги при проведенні інформаційних операцій за рахунок побудови та функціонування автоматизованих складних саморегулюючих систем» [74].

Слід згадати теорію мережевої війни, яка розроблена Пентагоном, і «виходить із необхідності контролювати світову ситуацію так, щоб основні глобальні процеси розгорталися в інтересах США, або щонайменше їм не суперечили». Як визначає О.Савченко, «специфіка мережевої війни полягає в тому, що вона ведеться постійно і безперервно та спрямована не лише проти

ворогів, яки–ми для США є країни осі зла Іран, Північна Корея, Сирія та інші, а й проти нейтральних сил, таких як Росія, Україна, Індія, Китай, і навіть проти союзників – країн Європи чи Японії. Метою мережевої війни є не перемога над супротивником при прямому зіткненні – не лише невеликий фрагмент конфлікту, а встановлення і підтримка тотального контролю, зокрема і над союзниками. Він реалізується різноманітними способами, але головним чином за рахунок численних мереж, побудованих за алгоритмами американських стратегів. Незважаючи на те, що ці алгоритми можуть бути прораховані й іншими центрами сил, ініціатива в їх створенні, розвитку і трансформаціях має знаходитися в американців. Захист мережевого коду, за допомогою якого безліч інформації дешифрується і структурується, — одне з головних завдань такої війни» [63].

Окремо слід виділити математичний підхід. Наприклад, В. Пасісниченко та І. Пасісниченко «вивчають дипломатію та війну, розробили рамки моделювання для аналізу чутливості міжнародних альянсів до змін у нерівному розподілі ресурсів між партнерами альянсу. Коли країна, що розвивається, знаходить нафту, досліджується, який вплив це має на військові чи торгові альянси. Складні моделі систем можуть дати можливість проаналізувати наслідки таких змін на рівні системи, які часто є нелінійними. Вчені також використовували теорії складності, аби виявити умови, за яких група різних людей із різними способами вирішення проблеми може вибрати більш ефективну публічну політику, ніж група однорідних осіб, які так само мають ту саму проблему. Різноманітність, за їх висновками, може в загальних обставинах покращити колективне ухвалення рішень у законодавчих органах та різних організаціях. Тому аналіз соціальних та політичних мереж так само все більше залучає моделювання складних систем. Існують моделі, які допомагають дослідникам краще розуміти умови, за яких соціальні мережі заохочують інновації та їх поширення серед своїх агентів» [52].

В. Пасісниченко та І. Пасісниченко наголошують на «відмінності теорій складності. Вона полягає в тому, що в основі теорія ігор, згідно Дж. фон

Нейману та Дж. Нешу, лежить припущення, що агенти є раціональні та розумні. Моделі систем складності можуть порушувати обидва ці припущення, особливо останнє. Тому значна частина досліджень складності у політичній науці зосереджує увагу на моделях, де агенти не є повністю раціональними і тому зображуються як адаптивні та обмежено раціональні. Загалом це означає, що агенти відображають наступні характеристики: вони не повністю оптимізують свої корисні функції з огляду на доступну їм інформацію; вони не дивляться наперед, аби мати можливість точно передбачити ймовірність результатів своєї поведінку у майбутньому; і вони короткозорі у тому, що не мають інформації за межами своєї локальної зони взаємодії. Отже, використання теорій складності щодо соціальних наук найкраще описується як набір інструментів для аналізу. Вони дозволяють краще зрозуміти мікрорівень мотивації та взаємодії між агентами, приймаючи до уваги їх інтеракцію, зворотні зв'язки та нелінійні ефекти. Наприклад, можна виявити причини переходу динаміки макрорівня від однієї фази до іншої. У цьому сенсі дослідники складних систем створюють щось аналогічне експериментальним лабораторіям, а складні моделі стають платформами для детального аналізу різноманітних питань, особливо про те, як взаємодії на мікрорівні формують шаблони на макрорівні» [52].

В.Воронковата Р.Андрюкайтене акцентують увагу на тому, що «дана теорія складності та інновацій включає ефективні управлінські теорії, які демонструють емерджентну поведінку управлінського істеблішменту та членів команди як активних суб'єктів, які утворюють єдине інтегративне управлінське ціле. Саме для цих складних умов слід використати теорію методології складності, в основі якої синергетична методологія, що здійснює великий внесок у сферу гнучкого публічного керування. Теорія складних систем стверджує, що інновації можуть бути лише емерджентним результатом, запланувати який неможливо. Основою упровадження теорії складності є взаємодія різних рівнів управління зі зворотним зв'язком функціонування, що складається з команди професіоналів, діяльність яких базується на цифрових

технологіях та роботі з інформацією, у контексті якої відбувається взаємодія між інноваціями та інформацією» [12].

Вчені акцентують увагу на тому, що «однією з важливих наукових проблем природознавства є вирішення завдання передбачення поведінки досліджуваного об'єкта в часі і просторі на основі знань про його початковий стан. Це завдання зводиться до знаходження деякого закону, який дозволяє за наявною інформацією про об'єкт в початковий момент часу в точці простору визначити його майбутнє в будь-який момент часу. Залежно від ступеня складності самого об'єкта цей закон може бути детермінованим або імовірнісним, може описувати еволюцію об'єкту тільки в часі, тільки в просторі, а може описувати просторово-часову еволюцію. Предметом нашого дослідження будуть не об'єкти взагалі, а динамічні системи в математичному розумінні цього терміну. Під динамічною системою розуміють будь-який об'єкт або процес, для якого однозначно визначено поняття стану як сукупності деяких величин в даний момент часу і заданий закон, який описує зміну початкового стану з плином часу. Цей закон дозволяє за початковим станом прогнозувати майбутній стан динамічної системи. Його називають законом еволюції. Динамічні системи описують механічні, фізичні, хімічні, біологічні та обчислювальні процеси, процеси перетворення інформації, що здійснюються відповідно до конкретних алгоритмів. Описи динамічних систем для різноманітних задач в залежності від закону еволюції також різноманітні: за допомогою диференціальних рівнянь, дискретних відображень, теорії графів, теорії марківських ланцюгів тощо. Вибір одного із способів опису задає конкретний вигляд математичної моделі відповідної динамічної системи» [12].

В. Пічкур зазначає, що «окремої уваги заслуговує одне зі значущих подій XX століття це є детермінований хаос у динамічних системах. Суть цього відкриття полягає в тому, що повністю детермінована динамічна система, при відсутності будь-яких випадкових впливів на неї, може поводитися непередбачуваним хаотичним чином». Вчений зазначає, що «в сучасній науці цей ефект строго обґрунтований теоретично і достовірно підтверджений

експериментально, тому виникає питання щодо того, чи не є цей феномен математичною екзотикою в тому сенсі, що його реалізація теоретично можлива, але практично малоймовірна». На його думку, «після відкриття детермінованого хаосу, ясного розуміння властивостей ефекту і розробки методів його дослідження, хаос був виявлений практично у всіх областях сучасного природознавства: у фізиці, радіотехніці, хімії, біології, механіці, економіці та ін» [56].

Ще один підхід, який слід проаналізувати – це концепція морального реалізму Моральний реалізм наголошує на складній взаємодії між моральними та політичними переконаннями та припускає, що політичні та пропагандистські наративи є не лише інструментами політики, а й відображають та формують моральні переконання суспільства. Ця перспектива свідчить про те, що політичні наративи та пропаганда, які поширюють країни, передбачають, що моральні виправдання, вбудовані в ці наративи, як російські, так і українські, ймовірно, формуються глибшими політичними ідеологіями, впливаючи на те, як ці наративи конструюються та сприймаються на світовій арені. Аналогічні результати можна спостерігати і там, де політичні ідеології суттєво вплинули на формування вакцин проти COVID-19, це розуміння стає важливим у геополітичній концепції, зокрема в російсько-українському конфлікті.

Розроблена соціальними психологами, теорія моральних засад розмежовує моральні міркування людини на п'ять основних цінностей: турбота/шкода, справедливість/обман, вірність / зрада, влада / підривна діяльність, святість/деградація та свобода/гноблення. Ця теорія застосовувалася і використовувалася для розуміння моральних міркувань політичних наративів і громадської думки. Наприклад, ця теорія допомагає зрозуміти моральне обґрунтування основних політичних рухів і політичних рішень, наголошуючи на тому, як різні групи можуть надавати пріоритет певним моральним цінностям над іншими. Застосування цієї теорії у дослідженні ставлення до вакцини проти COVID-19 показує, що ліберали та консерватори висловлювали різні набори моральних цінностей у своєму дискурсі.

У контексті російсько-української війни моральний реалізм є важливим методом розуміння міжнародної політики. російський наратив часто наголошує на захисті російськомовного населення в Україні, що можна трактувати як звернення до Фонду лояльності/зради. З іншого боку, акцент України на самовизначенні та опорі агресії може більше резонувати з фондами «Турбота / Шкода» та «Справедливість / Обман». Хоча моральний реалізм безпосередньо не застосовувався до аналізу дискурсу інформаційної війни, дослідження COVID-19 показує вплив розуміння моральних міркувань на політичні наративи. Моральний реалізм у контексті інформаційної війни цього конфлікту дає змогу проаналізувати моральні виправдання та наративи, які використовують Росія та Україна. Тоді ми можемо визначити етичні наслідки та цінності, що лежать в їх основі, які вони намагаються просувати. Інтегруючи моральний реалізм, ми можемо почати розуміти ефективність цих наративів у формуванні громадської думки та впливі на міжнародну реакцію на російсько-український конфлікт. Тематичне моделювання Topic Modeling – це техніка машинного навчання, яка використовується для виявлення прихованих тематичних структур у колекції документів, які часто називають «корпусами». Це дозволяє дослідникам виділяти та аналізувати домінуючі теми з мільйонів твітів, розуміючи прогрес публічного дискурсу та поширення пропагандистських чи контрпропагандистських наративів. Техніка тематичного моделювання особливо корисна при вивченні великих наборів даних, таких як ті, що генеруються з платформ соціальних медіа, щоб зрозуміти приховані наративи та настрої, які не є очевидними відразу.

Запропоноване визначення показує мету інформаційного протистояння, його сторони, ресурси, інструменти та об'єкти впливу. Виходячи із запропонованого розуміння інформаційного протистояння, можна відокремити його від інших суміжних понять – інформаційна агресія, інформаційна окупація, інформаційна співпраця. Протистояння – це завжди взаємодія з ресурсами як мінімум двох суб'єктів, які відповідно до своїх цілей реалізують соціальні дії проти інформаційних процесів і інформаційного середовища один

одного. Конфронтація, отже, вимагає наявності діючого «іншого» з цілями, інтересами і, можливо, цінностями, які протиставляються (ми свідомо вживаємо це слово) цілям, інтересам і цінностям даного соціального суб'єкта. І для того, щоб протистояння відбулося, цю невідповідність потрібно свідомо і трансформувати в мотив. Якщо цього не відбувається, мотив не сформований і випробовувані не діють по відношенню один до одного відповідно до нього, говорити про існування протистояння не можна. Навіть якщо є об'єктивне протиріччя в цілях, інтересах або цінностях.

Таким чином, будь-яке людське протистояння, а тим більше протистояння, якщо воно опосередковане свідомістю, має інформаційно-психологічну сторону, або складову. Від мікро до макрорівня. Будь-яке зіткнення інтересів або цінностей хоча б двох соціальних суб'єктів, яке є когнітивно свідомим або відчувається на афективному рівні і яке породжує соціальну дію, ґрунтується на інформаційних процесах.

Можна сформулювати постулат: будь-яке протистояння соціальних суб'єктів, в якому відбувається мотивована соціальна дія, спрямована проти іншого суб'єкта, обов'язково є інформаційно-психологічним протистоянням. Це означає, що без обміну інформацією між протилежними суб'єктами, тобто без комунікації між ними, неможливе протистояння як таке.

Інформаційне протистояння, таким чином, являє собою суб'єктивну взаємодію, в якій відповідно до своїх цілей сторони обмінюються ударами, образно кажучи, тримаючи в одній руці меч, а в іншій – щит. Доречно поставити питання, як називається ситуація, коли одна зі сторін мобілізована, озброєна «до зубів» і всіма своїми силами і засобами атакує інформаційний простір іншої, яка, навпаки, демобілізована, роз'єднана і навіть не в змозі зафіксувати і усвідомити факт агресивного нападу? Тобто відбувається не суб'єкт-суб'єктна взаємодія, не протистояння, а суб'єкт-об'єктна взаємодія, експансія, завоювання. Ми назвемо цю ситуацію інформаційною агресією. Результатом інформаційної агресії може стати інформаційна окупація, коли інформаційні процеси та інформаційний простір системи-жертви повністю

підпорядковані цілям та інтересам системи агресора і працюють за заданими останнім алгоритмами.

У деяких випадках інформаційна окупація може бути більш ефективною для агресорської системи, ніж пряма військова окупація чи насильницьке захоплення соціальної системи жертви. Введемо ще одне поняття – інформаційна колаборація – це робота професіоналів інформаційно-комунікаційної сфери системи жертви в інтересах системи агресора. Звернемося до співвідношення понять «інформаційне протистояння» та «інформаційна війна». Автор роботи згодний з тими авторами, які не ставлять між собою знак рівності, вважаючи, що інформаційна війна – це окремий випадок інформаційного протистояння, в рамках якого використовуються найбільш жорсткі, агресивні методи впливу на інформаційні процеси та інформаційне середовище противника.

Це означає, що в певних контекстах англійське слово «information warfare» можна перекласти як інформаційна війна, а в інших контекстах як інформаційна війна. При цьому «інформаційна війна» завжди перекладається як інформаційна війна. Відповідно, «інформаційний бій», який також зустрічається в літературі, можна перекласти як «інформаційне зіткнення» або «бойова інформаційна операція».

Інформаційне протистояння може набувати форми інформаційної війни як на міждержавному/геополітичному рівні, так і на рівні протистояння між політичними угрупованнями, компаніями та іншими суб'єктами господарювання. У літературі нам так і не вдалося знайти критеріїв переходу інформаційного протистояння в «гарячу» військову фазу, тому запропонуємо власне бачення відповіді на це питання.

Протистояння в інформаційній сфері перетворюється на форму війни, коли хоча б одна зі сторін відмовляється від нормативно-етичних обмежень у виборі форм і методів впливу на інформаційні процеси та інформаційне середовище противника, коли використовуються найбільш руйнівні з усіх видів інструментів – від фізичного руйнування об'єктів інформаційної

інфраструктури та ліквідації найбільш небезпечних гравців в інформаційній системі противника, до запуску потужних комп'ютерних вірусів. провокаційні фейкові новини, агресивна дезінформація та пропагандистські кампанії, що провокують масову паніку, заворушення чи деморалізацію населення протиборчої сторони. Якщо використовувати військову термінологію, то, судячи з усього, є сенс говорити про «локальні інформаційні війни» і «повномасштабні інформаційні війни».

У першому випадку мішенями виступають окремі елементи інформаційного середовища супротивника, окремі аудиторії, причому використовується обмежена кількість таких інструментів, які можна назвати «летальною інформаційною зброєю». У другому випадку війна ведеться в повному обсязі і використовуються засоби, що завдають максимально можливої шкоди. Висновки Інформаційно-комунікаційна революція перших десятиліть XXI століття, віртуалізація соціальності та формування спільнот цифрових мережевих інформаційних просьюмерів – не могли не вплинути на характер сучасного інформаційного протистояння. Трансформувалися і урізноманітнилися суб'єкти і об'єкти впливу, багато в чому змінився характер інформаційно-психологічної діяльності, з'явилися нові можливості впливу на інформаційні цілі.

Технології кастомізації та робота з великими даними дозволили створити індивідуалізовану інформаційну та психологічну зброю, адаптовану не лише під специфіку невеликих спільнот, а й під окремих користувачів у мережі. Прийшли технології штучного інтелекту, виявилося, що можна створювати і «ставити під зброю» цілі армії ботів. Багато що змінилося, але при цьому суть і цілі інформаційного протистояння і інформаційно-психологічних операцій залишилися колишніми. І не можна погодитися з думкою, що інтернет, Web 2.0 соціальні мережі. докорінно змінили все у світі інформаційної війни.

Виходячи з зазначеного, можна запропонувати авторську гіпотетичну концептуальну модель інформаційного протиборства в цифровій реальності. Ця модель розглядає інформаційне протиборство як складну динамічну систему,

що функціонує на перетині технологічного, політичного та соціокультурного просторів цифрової реальності. Її метою є забезпечення системного розуміння детермінант, механізмів та наслідків інформаційного протистояння в сучасному світі.

Основні блоки моделі:

1. Детермінанти інформаційного протиборства в цифровій реальності:

- Технологічні детермінанти: цифрові платформи та інфраструктура (соціальні мережі, месенджери, онлайн-медіа, пошукові системи, кіберпростір як поле бою); технології створення та поширення інформації (алгоритми рекомендацій, боти, тролі, штучний інтелект для генерації та аналізу контенту, технології deepfake, інструменти масової розсилки); кібернетичні можливості (кібератаки на інформаційну інфраструктуру, шпигунство, виведення з ладу систем).
- Політичні детермінанти: національні інтереси та геополітичні амбіції (боротьба за вплив, ресурси, домінування в інформаційному просторі); внутрішньополітична конкуренція (боротьба за владу, підтримку електорату, формування громадської думки); політичні ідеології та наративи (цінності, переконання, ідеологічні протиріччя як основа для інформаційного протистояння); державна інформаційна політика (стратегії захисту інформаційного простору та здійснення інформаційного впливу);
- Соціокультурні детермінанти: цінності та норми суспільства (соціальна вразливість до певних інформаційних впливів залежно від культурних особливостей); рівень медіаграмотності та критичного мислення населення (здатність розрізняти достовірну інформацію від дезінформації); соціальна згуртованість та довіра до інститутів (стійкість суспільства до поляризації та маніпуляцій); інформаційна культура та звички споживання інформації (вплив алгоритмів та ехо-камер).

2. Механізми інформаційного протиборства в цифровій реальності: створення та поширення дезінформації та пропаганди (використання фейкових новин, маніпулювання контекстом, емоційний вплив, теорії змови);

лібернетичні операції (атаки на веб-сайти, соціальні мережі, бази даних, системи управління); операції впливу в соціальних мережах (створення фейкових акаунтів, використання ботів та тролів для поширення наративів, маніпулювання трендами); психологічні операції (спрямовані на зміну настроїв, переконань, поведінки цільових аудиторій); використання лідери думок та інфлюенсерів (залучення популярних осіб для просування певних наративів); маніпулювання алгоритмами платформ (збільшення видимості потрібного контенту та приховування небажаного).

3. Форми інформаційного протиборства в цифровій реальності: цифрова пропаганда (систематичне поширення упередженої або неправдивої інформації з метою формування певних поглядів); кіберконфлікти (зіткнення в кіберпросторі між державами, групами або окремими особами); інформаційно-психологічні операції (іпсо) (скоординовані дії, спрямовані на вплив на свідомість та поведінку цільових аудиторій); гібридні конфлікти (поєднання інформаційних, кібернетичних, економічних, політичних та військових методів); кампанії дезінформації (скоординовані зусилля з метою поширення неправдивої інформації для введення в оману);

4. Наслідки інформаційного протиборства в цифровій реальності: поляризація суспільства та підрив довіри (розділення суспільства на протилежні табори, зниження довіри до медіа та державних інститутів); маніпулювання виборами та демократичними процесами (втручання у виборчі кампанії, вплив на результати голосування); дестабілізація політичних систем (організація протестів, заворушень, підрив легітимності влади); міжнародна напруженість та конфлікти (ескалація міждержавних відносин, провокування збройних конфліктів); загрози національній безпеці (кібератаки на критичну інфраструктуру, шпигунство, підрив обороноздатності); вплив на психічне здоров'я (тривожність, депресія, почуття безпорадності внаслідок інформаційного перевантаження та маніпуляцій).

Протидія інформаційному протиборству в цифровій реальності: підвищення медіаграмотності населення (навчання навичкам критичного

мислення та розпізнавання дезінформації); розвиток інститутів інформаційної безпеки (створення державних та недержавних організацій, що займаються протидією інформаційним загрозам); регулювання цифрового простору (розробка законодавчих та етичних норм поведінки в онлайн-середовищі); міжнародне співробітництво (обмін інформацією, координація зусиль у боротьбі з транснаціональними інформаційними загрозами); технологічні рішення (розробка інструментів для виявлення та блокування дезінформації, захисту від кібератак); підтримка незалежних медіа та платформ (забезпечення плюралізму думок та доступу до достовірної інформації).

Ця гіпотетична модель є спробою реконструкції можливого авторського підходу до аналізу інформаційного протиборства в цифровій реальності.

З урахуванням опису гіпотетичної концептуальної моделі інформаційного протиборства в сучасній цифровій реальності, її можна застосовувати в широкому спектрі дослідницьких, аналітичних та практичних сфер:

1. Наукові дослідження:

- Аналіз конкретних кейсів інформаційного протиборства: Модель може слугувати аналітичним інструментом для дослідження реальних випадків політичної конфронтації в цифровому просторі, таких як виборчі кампанії, міждержавні інформаційні війни, кіберконфлікти (в тому числі згадані автором щодо європейських країн), та вплив дезінформаційних кампаній.
- Порівняльний аналіз: Модель дозволяє порівнювати різні випадки інформаційного протиборства за їхніми детермінантами, механізмами, формами та наслідками, виявляючи спільні та відмінні риси.
- Прогнозування розвитку інформаційного протиборства: Вивчаючи динаміку взаємодії елементів моделі, можна намагатися прогнозувати майбутні тенденції та нові форми інформаційного протистояння.
- Розробка теоретичних концепцій: Модель може стати основою для подальшого розвитку теоретичних концепцій у сфері політичної науки, зокрема

щодо впливу цифрової реальності на політичні процеси та міжнародні відносини.

- Оцінка ефективності контрзаходів: Модель може використовуватися для аналізу та оцінки ефективності різних стратегій і тактик протидії інформаційному протиборству.

2. Аналітична діяльність:

- Державні органи та служби безпеки: Модель може бути застосована для аналізу інформаційних загроз національній безпеці, розробки стратегій інформаційної безпеки, виявлення та протидії дезінформаційним кампаніям та кібератакам.
- Аналітичні центри та дослідницькі організації: Модель може слугувати основою для проведення експертних оцінок та підготовки аналітичних звітів щодо інформаційного протиборства та його впливу на політичні процеси.
- Міжнародні організації: Модель може використовуватися для моніторингу та аналізу глобальних тенденцій у сфері інформаційного протиборства, розробки міжнародних норм та стандартів у сфері інформаційної безпеки.
- Медіа та журналістські розслідування: Модель може допомогти журналістам у розслідуванні та висвітленні випадків дезінформації, пропаганди та інших форм інформаційного впливу.

3. Практичне застосування:

- Розробка стратегій інформаційної боротьби: Модель може допомогти політичним партіям, громадським організаціям та іншим акторам розробляти ефективні стратегії комунікації та протидії ворожим інформаційним впливам.
- Підвищення медіаграмотності: Розуміння елементів моделі може бути використано для розробки навчальних програм та матеріалів з медіаграмотності для різних цільових аудиторій.

- Кризовий менеджмент: Модель може допомогти у розробці планів реагування на інформаційні кризи та мінімізації їхніх негативних наслідків.
- Розробка інструментів та технологій інформаційної безпеки: Розуміння механізмів інформаційного протиборства може сприяти розробці більш ефективних технологічних рішень для виявлення, аналізу та нейтралізації інформаційних загроз.

Таким чином, концептуальна модель інформаційного протиборства в умовах цифрової реальності має значний потенціал для застосування як у теоретичних дослідженнях, так і в практичній діяльності, спрямованій на забезпечення інформаційної безпеки та протидію деструктивним інформаційним впливам.

Вищенавелено дозволяє сформулювати наступні висновки. Поняття «інформаційне протистояння» та «інформаційна війна» є одними з найбільш вживаних при аналізі політичних комунікацій. Саме такий формат організації інформаційних взаємодій є найбільш ефективним для досягнення політичних цілей, реалізації навіть масштабних проектів у сфері влади. В даний час повсякденна політична практика дає безліч прикладів ведення найрізноманітніших інформаційних воєн як в демократичних державах, так і в перехідних політичних системах. Загалом, слід відзначити глибокі зміни у природі світу, зумовлених розвитком інформаційних технологій, та їхнього впливу на феномен інформаційного протиборства.

По-перше, стрімкий розвиток інформаційних технологій та зростаюча здатність організацій та індивідів використовувати їхній потенціал призвели до якісних трансформацій у ключових аспектах суспільного життя. Інформаційна епоха характеризується фундаментальними змінами у способах створення багатства, перерозподілі владних ресурсів, зростанні складності соціальних систем, скороченні географічних відстаней та стисненні часових рамок, що суттєво прискорює темп суспільних процесів. Ці глобальні зміни створили принципово нове середовище для міждержавної та внутрішньодержавної взаємодії, зокрема у сфері конфліктів та протистоянь.

По-друге, поява нових технологічних можливостей зумовила виникнення нових форм збройної боротьби та, відповідно, нової термінології, такої як «інформаційне протистояння», «інформаційні війни» та «кібербезпека». Важливо відзначити, що термінологічне поле даної сфери перебуває у стані динамічного розвитку, що зумовлює відсутність єдиних підходів та універсальних формулювань ключових понять. Це створює теоретико-методологічні труднощі, пов'язані як з «традиційними» термінами, що сягають своїм корінням у XX століття (наприклад, «інформаційна війна», «психологічна війна»), так і з поняттями, що виникли внаслідок розвитку новітніх інформаційних технологій та змін у військових стратегіях («кібервійна», «гібридна війна»).

По-третє, аналіз теоретико-методологічних проблем вивчення інформаційного протиборства дозволяє виокремити кілька ключових груп. Термінологічні та семантичні проблеми, пов'язані з недостатньо чітким визначенням та перетинанням значень базових понять, ускладнюють міждисциплінарний діалог та формування єдиного наукового апарату. Онтологічні проблеми стосуються макросоціологічної інтерпретації інформаційного протистояння як соціальної норми або девіації. Деонтологічні проблеми пов'язані з нормативною або об'єктивістською інтерпретацією явищ інформаційної війни та роллю категорії «правда» в інформаційних операціях. Окрему групу становлять проблеми, зумовлені впливом мінливого технологічного порядку на характер інформаційних протистоянь. Нарешті, актуальними є проблеми побудови сучасної типології інформаційних протистоянь та адекватного відображення технологічного забезпечення інформаційного протиборства в сучасних мережевих комунікаційних структурах. Розрив між військово-прикладними та математичними дослідженнями в даній сфері є очевидним та потребує подолання.

По-четверте, історичний контекст свідчить про те, що інформаційне протистояння первинно виникало в рамках збройної боротьби як засіб підняття бойового духу власних сил та деморалізації противника. З часом інформаційне

протистояння стало невід'ємною частиною політики держав не лише у воєнний, а й у мирний час, охоплюючи дипломатичну, економічну та інші сфери. Розвиток інформаційного протистояння відбувався паралельно з появою та поширенням нових, ефективніших засобів доставки інформації. Інформаційні технології, проникаючи в усі сфери суспільного життя, суттєво вплинули на політичні процеси, відкриваючи нові можливості для маніпулювання суспільною свідомістю та створюючи нові інформаційні загрози.

По-п'яте, наприкінці XX та початку XXI століття досягнення переваги в інформаційно-психологічній сфері набуло ключового значення для досягнення політичних та військових цілей. З'явився термін «стратегічна інформаційна війна», що характеризується відносно невисокою вартістю засобів, відсутністю традиційних державних кордонів, складністю виявлення початку інформаційної операції та її виокремлення в загальному інформаційному потоці. Інформаційне протистояння розглядається як вид протистояння з використанням усього спектру інформаційних можливостей для досягнення інформаційної переваги над противником у політичних, економічних та інших цілях. Сучасний досвід свідчить про те, що інформаційне протистояння може розглядатися не лише як спосіб ураження противника, а й як самостійна форма політичної боротьби, де інформаційно-психологічні методи впливу все частіше використовуються замість традиційних військових дій.

По-шосте, наукове визначення поняття «інформаційне протиборство» є складним завданням через його тісний зв'язок з іншими видами протистояння, зокрема фізичним. Ключовим аспектом є використання різноманітних засобів і способів впливу на інформаційний ресурс опонента, захист власного інформаційного ресурсу та його ефективне використання. Інформаційне протиборство може мати наступальний або оборонний характер, а важливим чинником протидії зовнішній інформаційній та психологічній агресії є державна інформаційна політика.

По-сьоме, розрізняють два покоління інформаційного протистояння. Перше покоління розглядало інформаційне протистояння як один із

компонентів досягнення мети поряд з іншими засобами. Друге покоління, в умовах інформаційної революції, трактується як довгостроковий вплив, що потенційно дозволяє відмовитися від застосування військової сили. Інформаційна війна визначається як інформаційне протистояння з метою завдання шкоди критично важливим структурам противника та дестабілізації його політичної та соціальної системи. Психологічна війна спрямована на прихований вплив на свідомість населення з використанням методів спотворення інформації та інших технологій, що впливають на сприйняття світу. У науковій літературі існують різні підходи до розгляду феномена інформаційної війни, включаючи аналіз її впливу на масову свідомість, технічний та математичний аналіз, а також інтегровані підходи.

По-восьме, існують різні тлумачення поняття інформаційної війни, включаючи розуміння її як сукупності політичних, правових, соціально-економічних дій, спрямованих на захоплення інформаційного простору, а також як найбільш гостру форму протистояння в інформаційному просторі. Інформаційна війна може розглядатися як особливий тип відносин між державами, де для вирішення протиріч використовуються методи силового впливу на інформаційну сферу. Існують різні різновиди інформаційної війни, такі як придушення систем управління, стратегічна розвідка та радіоелектронна боротьба.

По-дев'яте, концепція інформаційної переваги є ключовою для розуміння інформаційного протиборства. Інформаційна перевага визначається як здатність системи управління держави забезпечити стійкий процес отримання достовірної інформації та доведення її до споживачів при одночасному отриманні можливості використання інформаційної системи противника у своїх інтересах або зниження її ефективності. Досягнення інформаційної переваги вимагає вирішення комплексу взаємопов'язаних завдань, включаючи створення інтегрованих автоматизованих систем управління, забезпечення циркулярного доведення інформації, налагодження співробітництва у розподілі інформації,

забезпечення спільного сприйняття оперативної ситуації та використання систем в інтересах радіоелектронної боротьби.

По-десяте, теорія мережевої війни розглядає війну як мережеве явище, а військові дії – як різновид мережевих процесів, спрямованих на встановлення та підтримання тотального контролю, зокрема і над союзниками, шляхом використання численних мереж, побудованих за певними алгоритмами. Захист мережевого коду є одним із головних завдань такої війни. Математичні підходи до вивчення інформаційного протиборства використовують моделювання складних систем для аналізу динаміки міжнародних альянсів, процесів прийняття рішень та впливу соціальних мереж. Теорії складності дозволяють досліджувати поведінку агентів, які не є повністю раціональними, враховуючи їхню взаємодію, зворотні зв'язки та нелінійні ефекти.

Підсумовуючи останні досягнення в галузі інформаційних технологій глибоко трансформували природу конфліктів та протистоянь. Інформаційне протиборство стало невід'ємною частиною сучасної політики та військової стратегії, набуваючи нових форм та методів під впливом технологічного розвитку. Розуміння теоретико-методологічних проблем, історичного контексту, ключових концепцій та принципів інформаційного протиборства є необхідною умовою для ефективної протидії сучасним інформаційним загрозам та забезпечення національної безпеки в інформаційній епосі.

Висновки до Розділу 1.

Аналіз ступеня наукового розвитку досліджуваної проблематики свідчить про значну увагу наукової спільноти до питань інформаційного протистояння, особливо протягом останнього десятиліття. Збільшення кількості монографій, дисертаційних досліджень та наукових публікацій підкреслює актуальність цієї теми, зумовлену трансформаційними процесами в інформаційному просторі та зростаючою роллю інформації у політичних і соціальних процесах.

Ґрунтуючись на аналізі сутнісних характеристик інформаційної війни в цифровому середовищі, можна констатувати її складність як соціальної

системи, що володіє рекурсивними та автопоетичними властивостями. Це означає, що інформаційна війна здатна до самовідтворення та впливу на власні складові елементи, що ускладнює її прогнозування та контроль. Головним об'єктом інформаційної війни є соціокультурні цінності протиборчих сторін, що робить джерелом конфліктів фундаментальні протиріччя між цими цінностями, які унеможливлюють їхнє мирне співіснування.

Науково обґрунтовано розрізнення інформаційної війни та інформаційного протистояння. Інформаційна війна характеризується якісно вищою інтенсивністю використовуваних засобів і методів, спрямованих на досягнення радикального результату – повного соціокультурного та політичного домінування над противником, включаючи знищення опозиційної інформації. З цієї точки зору, інформаційна війна є неоголошеним, прихованим впливом на противника через різноманітні форми повідомлень та комунікації з метою формування необхідної системи цінностей, громадської думки, імперативів поведінки та регуляторів суспільних відносин, часто на несвідомому рівні для об'єктів впливу.

Вивчення феномена інформаційної війни вимагає комплексного міждисциплінарного підходу, що об'єднує положення інформаційно-когнітивної теорії формування поведінкових патернів особистості та суспільства, кібернетичної гносеології, культурної антропології та етики. Інформаційно-когнітивна теорія дозволяє аналізувати механізми сприйняття, обробки та засвоєння інформації, що лежать в основі формування переконань та поведінки. Кібернетична гносеологія надає інструменти для розуміння процесів управління інформаційними потоками та їхнього впливу на прийняття рішень. Культурна антропологія допомагає досліджувати глибинні соціокультурні цінності, які є мішенню інформаційних атак. Етичні аспекти є критично важливими для оцінки допустимості та наслідків застосування різних методів інформаційного впливу.

Глобалізація інформаційного простору, зумовлена розвитком нових електронних засобів інформації та комунікації (ЕСЕК) та відсутністю

ефективного контролю на початковому етапі, призвела до появи міжнародного тероризму як значущого актора інформаційної війни. Терористичні організації отримали безпрецедентні можливості для поширення своєї ідеології, впливу на свідомість людей незалежно від державних кордонів, що призвело до сплеску терористичної активності не лише у віртуальному, але й у реальному світі.

Усвідомлення того, що інформаційна безпека є невід'ємною складовою національної та загальної безпеки, стало реакцією на зростання інформаційних загроз. Однак, в умовах конфлікту цінностей, міжнародне співробітництво у сфері протидії тероризму та екстремізму зіткнулося зі значними перешкодами. Більш того, спостерігається тенденція використання методології, розробленої екстремістами для ведення війни проти держав через соціальні мережі, деякими західними країнами як стратегії ведення масштабних інформаційних війн проти держав з відмінними цінностями. Це підкреслює складність та багатогранність сучасного інформаційного протиборства, де межі між захистом інформаційної безпеки та здійсненням інформаційної агресії стають розмитими.

Таким чином, наукове дослідження інформаційного протиборства є не лише актуальним, але й критично важливим для розуміння сучасних соціально-політичних процесів та забезпечення національної безпеки. Подальші дослідження повинні бути спрямовані на поглиблений аналіз сутнісних характеристик інформаційної війни, розробку міждисциплінарних методологічних підходів, вивчення впливу новітніх технологій на динаміку інформаційного протиборства, а також на розробку ефективних стратегій протидії інформаційним загрозам та сприяння міжнародному співробітництву у сфері інформаційної безпеки.

Список посилань до розділу 1.

1. Аксьонова Н. (2017) Дослідження мас-медіа в умовах інформаційної війни. *Наукові праці Національної бібліотеки України ім. В. І. Вернадського :* зб. наук. пр. Вип. 48. С. 341–350.

2. Алещенко В. (2019) Особливості пропаганди в умовах інформаційно-психологічної війни. *Збірник наукових праць*. Вип. 24. С. 29–38.

3. Антонюк В. (2021). Інформаційна війна в структурі сучасного геополітичного протиборства: нові контексти та інтерпретації. *Державне управління та розвиток.* №35. URL: http://www.dy.nayka.com.ua/?op=1&z=2121 (дата звернення: 08.04.2025).

4. Базові аспекти цифровізації та їх правове забезпечення: монографія (2021) / [К. В. Єфремова, Д. І. Шматков, В. П. Кохан та ін.]; за ред. К. В. Єфремової. Харків: НДІ прав. забезп. інновац. розвитку НАПрН України. 180 с.

5. Бєлай С., Корнієнко Д. (2018) Інформаційна безпека сьогодення – невід'ємна складова воєнної безпеки. *Актуальні проблеми управління інформаційною безпекою держави.* Київ: Національна академія Служби безпеки України, 2018, 408 с.

6. Білобородов О., Довгополий А. (2019) Технології інформаційно-психологічних війн та інформаційно-психологічна зброя. *Озброєння та військова техніка.* №4. С. 93–99.

7. Валюшко І. (2018) Інформаційна безпека України в контексті російсько-українського конфлікту. Автореферат дисертації на здобуття наукового ступеня кандидата політичних наук за спеціальністю 23.00.04 – політичні проблеми міжнародних систем та глобального розвитку. Чорноморський національний університет імені Петра Могили. Миколаїв, 19 с.

8. Верголяс О. (2020) Правове забезпечення спеціальних інформаційних операцій». Кваліфікаційна наукова праця на правах рукопису. Дисертація на здобуття наукового ступеня кандидата юридичних наук (доктора філософії) за спеціальністю 12.00.07 «Адміністративне право і процес; фінансове право; інформаційне право» (08 – право). НДІІП НАПрН України, Київ, 287 с.

9. Вітюк Н. (2019) Особливості дискурсу політичної пропаганди в умовах інформаційно-психологічної війни. *Збірник наукових праць: психологія.* Вип. 24. С. 29–38.

10. Війни інформаційної епохи: міждисциплінарний дискурс: монографія (2021) / за ред. В. А. Кротюка, Харків : ФОП Федорко М. Ю. 558 с.

11. Войціховський А. (2018) Кібербезпека як важлива складова системи захисту національної безпеки європейських країн. *Журнал східноєвропейського права*. № 53. С. 26-37.

12. Воронкова В., Андрюкайтене Р. (2020). Сучасне управління у контексті теорії складності та інновацій. *IV Всеукраїнська науково-практична конференція «Публічне управління та адміністрування у процесах економічних реформ»*, 25. Херсон. http://eprints.mdpu.org.ua/id/eprint/9034/ (дата звернення 12.05.2024)

13. Гула Р. (2020) Інформаційна війна: соціально-онтологічний та мілітарний аспекти. Київ: «Каравела», 288 с.

14. Гуржій Т. (2018) Інформаційне право: виклики гібридної війни. *Зовнішня торгівля: економіка, фінанси, право*. № 4. С. 16-26

15. Данильян О., & Дзьобань, О. (2022) Інформаційна війна у медіапросторі сучасного суспільства. *Вісник НЮУ імені Ярослава Мудрого. Серія: Філософія, філософія права, політологія, соціологія.* № 3(54).

16. Данильян О., Дзьобань О. (2013) Інформаційна картина світу в контексті перспектив сучасної науки й культури. *Інформація і право.* №1 (7). С. 21–28.

17. Данильян О., Дзьобань О. (2013) Інформаційна картина світу як соціокультурна реальність. Гілея: наук. вісник. Зб. наук. пр. Вип. 70 (№3). С. 573–578.

18. Данілов О. (2020) Кіберзахист державних інформаційних ресурсів – важлива складова у процесі цифрової трансформації країни. URL: https://www.rnbo.gov.ua/ua/Diialnist/4606.html

19. Данілян О., Дзьобань О. (2022) Сучасна війна: трансформація сенсу в епоху інформаційних технологій. *Інформація і право*. № 4 (43),. С. 9-22.

20. Дзьобань О., Романюк С. (2013) Інформаційна картина світу: філософський підхід до розуміння сутності. *Вісник Національного*

університету «Юридична академія України імені Ярослава Мудрого». Серія: Філософія, філософія права, політологія, соціологія,. Вип. 2 (16). С. 116–124.

21. Долженко О. (2023). Гібридна війна як інноваційний феномен сучасної політики: український вимір: автореф. дис. ... канд. політ. наук: 23.00.02; Волинський національний університет імені Лесі Українки. Луцьк. 21 с.

22. Доренський О., Улічев О. (2024). Концептуальна модель системи інформаційного протиборства координаційного центру з питань національної безпеки і оборони. *Центральноукраїнський науковий вісник. Технічні науки*. Вип. 10 (41). Ч. ІІ. С. 23-31.

23. Завгородня Ю. (2021) Кіберконфлікти як елемент політичних технологій в інформаційному просторі. *Актуальні проблеми філософії та соціології*. № 32, С .144-149.

24. Застосування засобів масової інформації у інформаційно-психологічній війні. Інформатика та математичні методи в моделюванні (2021) / Браїловський М. М., Пірцхалава Т. П., Хорошко В. О., Хохлачова Ю. Є. Т. 11. № 3. С. 162–172.

25. Застосування Сухопутних військ Збройних Сил України у конфліктах сучасності (за досвідом забезпечення національної безпеки складовими сектору безпеки і оборони у ході російсько-української війни): *Збірник тез доповідей науково-практичної конференції* (Львів, 29-30 листопада 2023 р.). Львів: НАСВ, 2023. 381 с.

26. Захарченко К. (2021) Інституційний вимір інформаційної безпеки України: трансформаційні виклики, глобальні контексти, стратегічні орієнтири. – Кваліфікаційна наукова праця на правах рукопису. Дисертація на здобуття наукового ступеня доктора політичних наук за спеціальністю 23.00.02 – політичні інститути та процеси. Національний педагогічний університет імені М.П. Драгоманова, Львівський національний університет імені Івана Франка, Львів, 423 с.

27. Інформаційна безпека (2021) / В.В. Остроухов, М.М. Присяжнюк, О.І. Фармагей, М.М. Чеховська та ін.; під ред. В.В. Остроухова. Київ: Видавництво Ліра-К. 412 с.

28. Інформаційна безпека та кібербезпека держави: навчальний посібник (2025) / Н. М. Титова, Н. М. Рідей, В. П. Настрадін, М. М. Присяжнюк, С. М. Мамченко, С. В. Артюх, Р. О. Яворська. Київ, Видавнитво Ліра-К. 224 с.

29. Інформаційна безпека. Підручник (2024) /М. Присяжнюк. Київ: Видавництво Ліра-К. 224 с.

30. Інформаційне суспільство в світі та Україні: проблеми становлення та закономірності розвитку: колективна монографія (2017) / За ред. д. проф. В. Г.Воронкової; Запоріз. держ. інж. акад. Запоріжжя: ЗДІА, 282 с.

31. Інформаційно-психологічне протиборство: підручник (2018) / [В. М. Петрик, В. В. Бедь, М. М. Присяжнюк та ін.]; за заг. ред. В. В. Бедь, В. М. Петрика. Київ: ПАТ «ВІПОЛ», 386 с.

32. Калініченко Б. (2019) Роль засобів масової інформації в інформаційній війні: політичні детермінанти впливу та протидії. Дисертація на здобуття наукового ступеня доктора політичних наук за спеціальністю 23.00.02 – політичні інститути та процеси. Київ. 434 с.

33. Кириченко М. (2017) Зарубіжний досвід високорозвинених країн з сталим розвитком інформаційно-інноваційного суспільства в умовах трансформації сучасної цивілізації. *Актуальні проблеми філософії та соціології.* Одеса: Редакційно-видавничий відділ НДЧ Національного університету «Одеська юридична академія». № 17. С. 51-54.

34. Кириченко М. (2017) Інформаційно-семіотичні виміри інформації як головного тренду інформаційного суспільства. *Гуманітарний вісник Запорізької державної інженерної академії : зб. наук. пр*. Запоріжжя, Вид-во ЗДІА. Вип. 68. С. 57-67.

35. Кириченко М. (2017) Формування цінностей мережево-онлайнової культури в дискурсивному просторі віртуальної реальності. *Гілея. Історичні науки. Філософські науки. Політичні науки : наук. вісник : зб. наук. пр*. / М-во

освіти і науки України, Нац. пед. ун-т ім. М. П. Драгоманова. Вип. 121 (6). С. 123-127.

36. Кириченко М. (2017) Формування ідеології інформаційного суспільства в умовах глобальної інформатизації: тенденції, парадигми, перспективи розвитку: [Монографія]; Мін-во освіти і науки України, Університет менеджменту освіти НАПН України, Харків: Вид-во ПП «Технологічний Центр». 320 с.

37. Колодка А. (2023) Механізми кризового менеджменту в умовах інформаційних загроз в гібридних середовищах. Кваліфікаційна наукова праця на правах рукопису. Дисертація на здобуття наукового ступеня доктора філософії в галузі знань Публічного управління та адміністрування за спеціальністю 281 «Публічне управління та адміністрування». Інститут державного управління та наукових досліджень з цивільного захисту. Київ. 239 с.

38. Котляров В. (2024) Стратегічне управління інформаційною безпекою України. *Київський економічний науковий журнал*. № 6. С. 66-69.

39. Крилова Ю. (2020). Інформаційне (цифрове) суспільство: політико-правовий аспект упровадження. *Науковий часопис Національного педагогічного університету імені М. П. Драгоманова. Серія 22. Політичні науки та методика викладання соціально-політичних дисциплін:* збірник наукових праць. Випуск 27. Київ : Вид-во НПУ імені М. П. Драгоманова. С. 75-83.

40. Курбан О. (2021). Бойові наративи в системі сучасних геополітичних інформаційних війн (досвід російсько-української гібридної інформаційної війни 2014–2021 рр.). *Синопсис: текст, контент, медіа*. №27 (3). С. 149–158.

41. Курбан О. (2022). Проблема критичності мислення при споживанні медіаконтенту в умовах інформаційної війни. *Синопсис: текст, контент, медіа.* №28 (1) С. 21–27.

42. Лісовський П., Лісовська Ю. (2024). Воєнна мережева криптосистема: державотворчий інноваційний контекст: монографія. Київ : Видавництво Ліра-К. 114 с.

43. Лужецький В., Дудатьєв А. (2017). Концептуальна модель системи інформаційного впливу. *Безпека інформації*. 23 (1). С. 45–49.

44. Марунченко, О. (2012) Інформаційна війна в сучасному політичному просторі: дис. ... канд. політ. наук : 23.00.02. ДУ «Південноукр. нац. пед. ун-т імені К. Д. Ушинського». Одеса. 209 с.

45. Міненко Є. (2024). Розвиток інститутів інформаційної безпеки сучасної України як чинник суспільно-політичної стабільності. Кваліфікаційна наукова праця на правах рукопису. Дисертація на здобуття наукового ступеня доктора філософії за спеціальністю 052 – Політологія. Український державний університет імені Михайла Драгоманова, Київ, 2024. 257 с.

46. Младьонова А. (2021). Інформаційна війна і політика безпеки: політикоправовий вимір. Кваліфікаційна наукова праця на правах рукопису. Анотація дисертації на здобуття ступеня доктора філософії за спеціальністю 052 – Політологія (Галузь знань 05 – Соціальні та поведінкові науки). Харківський національний університет імені В. Н. Каразіна Міністерства освіти і науки України, Харків. https://old.karazin.ua/docs/work/dysertatsii/mladionova-anotatsia.pdf (дата звернення 11.09.2024)

47. Младьонова О. (2017). Маніпулювання суспільною свідомістю як технологія ведення інформаційної війни. *Вісник Харківського національного університету імені В. Н. Каразіна***.** Вип. 32. С. 79–82.

48. Наумкіна С. (2024). Ризики формування нових форм тиску як прояви цифрового тоталітаризму. *Сучасні виклики соціально-політичного розвитку: політико-правові та соціально-економічні виміри: матеріали всеукраїнської науково-практичної конференції*, м. Одеса, 24 травня 2024 року. Державний заклад «Південноукраїнський національний педагогічний університет імені К. Д. Ушинського», Центр соціально-політичних досліджень «Politicus». С. 150-152.

49. Невельська-Гордєєва О., Нечитайло В. (2021) Маніпуляції як засіб інформаційно-психологічного впливу в інформаційній війні. *Вісник*

Національного юридичного університету імені Ярослава Мудрого. Серія: Філософія, філософія права, політологія, соціологія. № 3. С. 71–83.

50. Носов В., Манжай О. (2015). Окремі аспекти протидії інформаційній війні в україні. *Правове, нормативне та метрологічне забезпечення системи захисту інформації в Україні*. Вип. 1 (29). С. 26-32.

51. Осьодло В., Денисенко І., Побочий І., Віннікова Н. (2021). Війни інформаційної епохи: міждисциплінарний дискурс: монографія/за ред. В.А. Кротюка. Харків: ФОП Федорко М. Ю.. 558 с.

52. Пасісниченко В., Пасісниченко І. (2019). Теорії складності та їх застосування в соціальних науках. *Сучасне суспільство*. Випуск 2 (19). С. 120-131.

53. Петрик В., Назаренко А. (2025). Інформаційна безпека у контексті сучасних технологій інформаційно-психологічного протиборства. Київ: Центр навчальної літератури. 258 с.

54. Пехник А., Завгородня Ю. (2021). Сучасні загрози кібертехнологій у політичному процесі. *Актуальні проблеми політики*. №68. С. 76-82.

55. Пилипчук В. (2014). Глобальне інформаційне протиборство: сучасні тенденції, виклики і загрози. *Вісник Національної академії правових наук України*. № 3. С. 43-52.

56. Пічкур В. (2020). Теорія динамічних систем. Луцьк : Вежа-Друк. 348 с.

57. Проноза І. (2018) Інформаційна війна: сутність та особливості прояву. *Актуальні проблеми політики*. №61. С. 76-84.

58. Проноза І. (2016). Гібридна російсько-українська війна як загроза європейській безпеці. *Політикус.* Вип. 1. С. 126-130.

59. Проценко, Д., Тупчієнко, Д. (2012). Огляд підходів до регулювання нових конвергентних аудіовізуальних засобів масової інформації: міжнародний досвід. *Національна рада України з питань телебачення і радіомовлення*. http://nrada.gov.ua/userfiles/file/2012/PDF/Brochure_ReviewOfRegulatory Approaches.pdf

60. Руднєва А. (2014). Інформаційні війни як фактор впливу на політичну культуру в сучасній Україні. Автореферат дисертації на здобуття наукового ступеня кандидата політичних наук за спеціальністю 23.00.03 – політична культура та ідеологія. Національний педагогічний університет імені М. П. Драгоманова. Київ. 22 с.

61. Руцький С. (2023). Загрози в сучасному політичному процесі: інформаційний аспект. *The 3rd International Scientific and Practical Internet conference «Modern Political Processes: Global and National Dimensions»*, Odesa, 2023.

62. Руцький *С.* (2023). Конфронтація взаємодії суб'єктів політики в інформаційному просторі. *Науковий журнал «Політикус».* № 5. С. 82-86.

63. Савченко О. (2014). Новітні війни з використанням інформаційно-психологічної зброї. *Вісник книжкової палати*. №8. С. 1-6.

64. Семен Н. (2018). Російські інтернет-ресурси як чинник інформаційної війни проти України (на прикладі сайтів «Правда.Ру» та «Российский диалог»). Автореферат дисертації на здобуття наукового ступеня кандидата наук із соціальних комунікацій за спеціальністю 27.00.01 – теорія та історія соціальних комунікацій. Дніпровський національний університет імені Олеся Гончара, Міністерство освіти і науки України. Дніпро, 2018. URL: https://www.dnu.dp.ua/docs/ndc/dissertations/K08.051.19/autoreferat_5bb2b747a54ef.pdf (дата звернення12.08.2024)

65. Соловйов С. (2016). Основні характеристики стратегічних комунікацій. *Вісник Нац. ун-ту цивільного захисту України*. № 1 (4). С. 165–170.

66. Стадник А. (2016). Інформаційна війна як комунікативна технологія впливу на масову свідомість та громадську думку. *Грані*. №1. С. 111–115.

67. Сунгурова С. (2023). Інформаційна війна як засіб політичного насилля. Анотація дисертація на здобуття наукового ступеня доктора філософії у галузі знань 05 «Соціальні та поведінкові науки» за спеціальністю 052 «Політологія». Київський національний університет імені Тараса Шевченка. Київ. URL: https://uacademic.info/ua/document/0823U100451#! (дата звернення 04.02.2024)

68. Тарасова В. (2020). Вербальні засоби інформаційно-психологічної війни. Вісник Маріупольського державного університету. Серія: Філологія. Вип. 22. С. 251–258.

69. Таркін В. (2023). Інформаційні війни у сучасному політичному просторі як феномен XX-XXI століття: дис…доктора філос. Національний університет «Одеська юридична академія». Одеса. 220 с.

70. Теоретичні основи створення технологій протидії прихованим інформаційним атакам в сучасній гібридній війні. / Алімпієв А. М., Бараннік В. В., Белікова Т. В., Сідченко С. О. *Системи обробки інформації*. 2017. Вип. 4. С. 113–121.

71. Торічний В. О. (2020). Інформаційне забезпечення державної безпеки України в умовах трансформаційних викликів і загроз. Кваліфікаційна наукова праця на правах рукопису. Дисертація на здобуття наукового ступеня доктора наук з державного управління за спеціальністю 25.00.05 – державне управління у сфері державної безпеки та охорони громадського порядку. Національний університет цивільного захисту України, Харків. 375 с.

72. Федотова-Півень І. М. (2017). Шляхи задоволення потреб сучасної кібербезпеки в рамках протидії методам комп'ютерної лінгвістичної стеганографії. / І. М. Федотова-Півень, Я. В. Тарасенко та ін. *Безпека інформації.* № 3 «3). С. 190-196.

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

74. Харченко І., Сапогов О., Шамраєва В, Новіков А. (2017) Основні засоби інформаційного протиборства та інформаційної війни як явища сучасного міжнародного політичного процесу. *Серія «Міжнародні відносини. Економіка. Країнознавство. Туризм».* Випуск 6. С.77-81.

75. Шевчук М. (2024). До питання генези поняття інформаційної безпеки як складової національної безпеки. Науковий вісник Ужгородського національного університету. *Серія ПРАВО*. Випуск 78. частина 2. С. 134-139.

76. Шемаєв В. (2022). Інформаційне протиборство з використанням рефлексивного управління: теорія та практика. *Інформаційна безпека людини, суспільства, держави. №* (1-3 (31–33). С. 96–104.

77. Шемчук В. (2019) Концептуальні підходи до розуміння інформаційної війни в сучасному світі. *Вчені записки ТНУ імені В.І. Вернадського. Серія: юридичні науки*. № 3. С. 29-35.

78. Шемчук В. В. (2020). Загрози інформаційній безпеці: проблеми визначення та подолання. *Експерт: парадигми юридичних наук і державного управління.* № 1 (7). С. 285-296.

79. Шпига П. С., Рудник Р. М. (2014). Основні технології та закономірності інформаційної війни. *Проблеми міжнародних відносин*. Вип. 8. С. 326–339.

80. Юдін О. К., Матвійчук-Юдіна О. В., Супрун О. М. (2021). Інформаційно-психологічна ійна та технології соціального інжинірингу. *Наукоємні технології.* №2. С. 130–139.

81. Юзова І. Ю., Пацек П. (2020). Інформаційно-психологічний вплив противника та протидія йому в умовах ведення гібридних війн. *Наука і техніка Повітряних Сил Збройних Сил України*. №3. С. 61–68.

82. Molander Roger C. Strategic information warfare: a new face of war / Roger C. Molander, Andrew S. Riddile, Peter A. Wilson. URL: http://www. rand. org/pubs/monograph_reposts/MR661.html (дата звернення: 05.02.2025)

Форми та прояви інформаційного протиборства на рівні цифрової реальності

2.1. Концепція інформаційної переваги як основа мережевої війни.

Сучасне інформаційне середовище, інформаційний простір відрізняється від попередніх новими – цифровими засобами виробництва, зберігання і передачі (передачі) інформації. Вже на етапі формування такого електронного інформаційного простору за допомогою аналогового обладнання та технологій була розроблена кібернетична гносеологія. В її основу було покладено передумову про схожість інформаційних процесів у кожного людського індивіда і суспільства в цілому з інформаційними процесами в інших живих організмах і навколишньому середовищі в цілому. Зокрема, подібно до того, як кожен живий організм має потребу протистояти ворожим атакам багатьох шкідливих бактерій та інших організмів, у соціально-інформаційному середовищі людині також доводиться боротися із зовнішніми загрозами (насильством, війною, тероризмом, екстремізмом тощо), розробляти способи взаємодії з ними, виживання та забезпечення безпеки.

До другої половини XX століття весь цей комплекс проблем поступово узагальнився в один з феноменів інформаційної цивілізації – «інформаційну війну», яку почали визначати фізики, філософи, політологи, соціологи, філологи та інші дослідники, використовуючи методологію все більшого числа соціально-гуманітарних і природничих наук. Зокрема, було розпочато розробку нової, специфічної методики цієї теми – кібернетичної гносеології. Незважаючи на те, що, на наш погляд, він здатний найбільш повно розкрити онтологічні характеристики і передати природу явища «інформаційної війни», такий підхід все ж не часто використовується в науковій літературі, а тому представляється необхідним розглянути його засади для використання в даній роботі.

Інформаційна війна стоїть на політичному порядку денному. Класичні засоби масової інформації, з одного боку, активно критикують засоби ведення інформаційної війни з боку геополітичних опонентів тієї чи іншої держави, з іншого боку, вони самі активно ведуть інформаційну війну через власну діяльність. Тим не менш, поява та активне використання терміна «інформаційна війна» досі не призвело до його загальновизнаного визначення, що ускладнює розуміння сутності та методів ведення такої війни. У 1976 р американський фізик Т. Рона вперше вжив словосполучення «Інформаційна війна» в публічній доповіді «Системи озброєнь та інформаційна війна», в якій інформація також вперше була розглянута не тільки як мета військових операцій, але і як метод. У зв'язку з тим, що значення введеного Т.Роном англомовного словосполучення відповідало кільком схожим за значенням російськомовним аналогам, виникла проблема варіантної відповідності, і, як наслідок, використання вченими різної термінології для позначення синонімних, як їм здавалося, понять. Протистояння в інформаційній сфері, на нашу думку, передбачає сукупність дій і протидій сковує в кайдани, захисного і атакуючого характеру, спрямованих на контроль над інформаційним простором, на стратегічне позиціонування інтерпретації цієї інформації. Інформаційна війна – це сукупність дій, спрямованих на безумовне домінування, аж до знищення цифрового сліду опозиційного контенту чи інтерпретації. Тобто війна відрізняється від протистояння якісно більшою інтенсивністю засобів і методів, що використовуються для досягнення радикального результату. Питання інтерпретації інформації є важливим і в контексті визначення інформаційної війни, оскільки обидві конфліктуючі сторони можуть використовувати одну й ту саму інформацію, але трактувати її по-різному.

Протистояння в інформаційній сфері не є синонімом інформаційної війни. Інформаційне протистояння може передувати війні та агресивним діям, неявно деструктивно впливаючи на інформаційне поле противника. Одним із наслідків глобалізації космосу шляхом інформатизації є виникнення і розвиток постмодерних держав, для яких поняття суверенних кордонів втрачає сенс, що

відрізняє їх від національних держав з яскраво вираженою політичною та соціальною єдністю. Нездатність національних держав забезпечити ефективне управління в умовах глобалізації та прагнення до самовизначення через вираження чіткого територіального суверенітету роблять їх можливими суб'єктами геополітичної форми інформаційної війни. Така форма війни характерна для прикордонного простору, в першу чергу для тих ділянок, де територіальні суперечки залишаються невирішеними. У цих випадках інформаційна війна набуває форми «картографічної війни», різновидами якої є витіснення топонімів, внесення спотворених відомостей про територіальну приналежність до шкільних підручників з історії та географії тощо.

Інформаційна війна ведеться за допомогою спрямованого впливу на противника за допомогою своєрідних інформаційних «квантів», тієї чи іншої форми повідомлень, актів комунікації, з метою формування необхідної громадської думки і системи цінностей кожної людини. При стратегічному позиціонуванні певним чином заряджених в суспільстві інформаційних квантів формуються імперативи і регулятори суспільних відносин, які не піддаються ні юридичному, ні транскордонному регулюванню, ні навіть регулюванню моральними нормами. Визначення інформаційної війни як складної соціальної системи зумовлює необхідність вирішення етичних проблем інформаційного середовища суспільства та його медіапростору.

Сучасні військові операції відбуваються під впливом експоненціального зростання інформаційних технологій, які прискорюють та розширюють здатність об’єднаних сил збирати, обробляти, аналізувати, зберігати та передавати дані та інформацію в масштабі, який раніше неможливо було собі уявити. Поширення супутників, передових обчислювальних і автоматизованих систем, мобільних мереж і соціальних медіа є одними з технологій, які впливають на те, як сили використовують інформацію для досягнення цілей. Слід зазначити, що наш ворог має такі ж можливості, які має і наша держава.

Для того, щоб зрозуміти сучасну війну, слід звертати увагу на її «латентний характер, постійну зміну засобів її ведення, поєднанням класичних і

некласичних аспектів її реалізації, перманентне посилення науково-технічної складової бойових дій» [44]. На це звертають увагу вчені Осьодло В., Денисенко І., Побочий І., Віннікова Н.

Мережецентрична війна (NCW) — це військова доктрина, вперше запроваджена Сполученими Штатами (США) у 1990-х роках. Прагнучи перетворити інформаційну перевагу на посилення бойових можливостей, NCW широко говорить про використання комбінації технологій інформаційної епохи для підвищення бойової потужності.

Визначено в Network-Centric Warfare: Developing and Leveraging Information Superiority, NCW – це «концепція операцій, що підтримує інформаційну перевагу, яка генерує підвищену бойову міць за допомогою мережевих датчиків, осіб, які приймають рішення, і стрільців для досягнення спільної обізнаності, збільшення швидкості командування, більш високого темпу операції, більша летальність, підвищена живучість і ступінь самосинхронізації. По суті, NCW перетворює інформаційну перевагу в бойову міць, ефективно зв’язуючи обізнані суб’єкти в бойовому просторі»

Сучасна мережецентрична війна та пов'язані з нею кардинальні зміни у військовій справі є прямим наслідком глибоких трансформацій у суспільстві. Ці зміни живляться спільною еволюцією економіки, інформаційних технологій, бізнес-підходів та організаційних структур. Їх можна об'єднати навколо трьох ключових ідей: по-перше, зміщення фокусу з окремої платформи на взаємопов'язану мережу; по-друге, перехід від розгляду учасників як ізольованих суб'єктів до їхнього розуміння як елементів гнучкої екосистеми; і, по-третє, критична важливість стратегічних рішень для адаптації або навіть виживання в цих швидко мінливих умовах.

П.Лісовський та Ю.Лісовська говорять про сучасний світ та характеризують розвиток людства «як прогресивний рух по еволюційній осі, то кіберсучасність потребує саме нових людських якостей щодо виживання в планетарно-цифровому просторі. Адже ми увійшли в період глобальних потрясінь, катаклізмів, знаходячись у біогенному середовищі» [33].

Г. Ситник досліджує питання війни та миру з позиції філософського розуміння та визначає, що війну слід розуміти як «збройного зіткнення двох або більше сторін, представлених різними державами або їхніми коаліціями» [60]. Вчений говорить про те, що «попри історичні відмінності та характер різні типи війни мають усталену структуру – комплекс ознак, що відрізняють стан війни від стану не-війни (миру), війну від конфлікту. Війна – збройна фаза конфліктного протистояння, що виникає тоді, коли вичерпані політичні засоби влагодження суперечностей або беруть гору владні амбіції однієї із сторін, яка зорієнтована на безумовне знищення або підкорення противника. У ширшому сенсі війна і мир є ознаками стану взаємодії людських спільнот або соціальних груп та державних організмів, що уособлюють соціально-історичну реальність, кожне зі свого боку» [60]. Автор зазначає, що «стан війни означає комплекс дій, спрямованих на руйнування усталеного порядку з його правилами комунікації та кодами поведінки. Війна призводить до знищення чужого, незрозумілого і неприйнятного, якщо його буде визначено як загрозу власному існуванню. Стан миру означає ствердження порядку, розбудову або відновлення свого впорядкованого світу, зрозумілого, осмисленого й звичного, що, однак, не виключає і деяку еволюцію правил взаємодії у межах прийнятої моделі» [60].

О.Савченко визначає мережу як інструмент «яким прямує інформація будь-якого штибу, від побутової, фінансової, економічної, суспільно-політичної, енергетичної до військово-стратегічної, поступово з суто технічного засобу перетворюється на головну життєву артерію сучасного суспільства. Різні мережеві структури, до яких входять засоби зв'язку, мас-медіа, транснаціональні корпорації, релігійні організації, неурядові організації, політичні осередки, спецслужби різних держав тощо, поступово інтегруються до загальної надзвичайно гнучкої й різнорідної структури» [59]. На думку науковця, головний зміст теорії мережевих війн полягає в «обміні інформацією, максимальне розширення форм виробництва в цій сфері, доступу до неї, до її розподілу і зворотного зв’язку. Мережа представляє собою новий інформаційний простір, у якому здійснюються основні стратегічні операції

розвідувального і військового характеру, а також їх медійнє, дипломатичне, економічне і технічне забезпечення. Мережа в широкому розумінні включає в себе складові, які до цього розглядались роздільно бойові одиниці, система зв'язку, інформаційне забезпечення операцій, формування громадської думки, дипломатичні кроки, розвідка та контррозвідка, етнопсихологія, релігійна та колективна психологія, економічне забезпечення, академічна наука, технічні інновації тощо, що в теперішній час розглядаються як взаємопов'язані частини єдиної системи, між якими здійснюється постійний інформаційний обмін» [59].

В.Антонюк визначає наступні цілі інформаційної війни: «попередження можливого військового конфлікту, ослаблення морального духу особового складу збройних сил і цивільного населення супротивника, внесення в суспільну свідомість й індивідуальну свідомість ворожих, шкідливих ідей і поглядів, дезорієнтація та дезорганізація мас, внесення безладу в інформаційну мережу супротивника, ослаблення патріотичних переконань і національних традицій, провокування і спонукання до відмови від участі в бойових діях, залякування свого народу образом ворога, залякування супротивника своєю могутністю, створення передумов для досягнення намічених воєнно-політичних цілей з мінімальними людськими втратами та матеріальними витратами» [1].

Вчений також виділяє основні принципи ведення такого типу війни. На його думку це: «відповідність її цілей і завдань політичним цілям війни, необхідність зосередження сил у вирішальному місці та вирішальний момент; всебічна і завчасна підготовка сил і засобів ведення інформаційної війни; принцип високої активності і рішучості в ході ведення інформаційної війни, принцип узгодженого спільного застосування різних видів і типів сил і засобів ведення інформаційної війни, принцип раптовості інформаційних ударів, постійна готовність сил і засобів інформаційної війни до захисту власної інформації і руйнівного впливу на інформаційне середовище супротивника, безперервність інформаційної війни; ведення інформаційної війни з напругою, необхідною для виконання поставлених завдань, своєчасний маневр сил і засобів ведення інформаційної війни, врахування духовного фактору в

інтересах виконання поставлених завдань, всебічне забезпечення, підтримка боєздатності та своєчасність відновлення сил і засобів ведення інформаційної війни, твердість і безперервність управління силами і засобами ведення інформаційної війни, непохитність у досягненні поставлених цілей, виконанні прийнятих рішень і поставлених завдань» [1].

Ще можна представити досить перспективний підхід до розуміння інформаційної війни, яка відбується на локальному рівні. Мова про так звані гібридні моделі, які базуються на «моделі визначеного інформаційного простору та моделі соціальної мережі. Дана гібридна модель включає в себе організаційні та когнітивні моделі». Така модель інформації «зменшується і перетворюється у вузлах та із затримкою через обмеження зв'язку між вузлами. Вона може об'єднати аналіз соціальних мереж для оцінки аспектів комунікації та ієрархії, із переконанням мереж, для оцінки аспектів індивідуальної обробки інформації. Тобто в них використовують соціальні мережі, для того, щоб зробити переконання мережі динамічними. Соціальна обробка інформації передбачає введення у дію моделей структурних процесів, які впливають на переконання». Такі моделі «зазвичай стимулюють процес, за допомогою якого люди взаємодіють з невеликою групою інших. Одне з ключових понять у даній моделі є транзактивна пам'ять, що полягає у здатності груп мати систему пам'яті. Ідея заключається у тому, що знання зберігаються стільки, скільки перебувають у динамічному використанні. Модель Вегнера транзактивної пам'яті заснована на представлені людської пам'яті у вигляді комп'ютерної системи» [76].

На думку О.Савченка. «мережецентричні війни засновані на фундаментальному поділі циклів людської історії на три фази. Це аграрні, промислові й інформаційні епохи, кожній з яких відповідають особливі моделі стратегії, що випливають з соціологічних понять передмодерн, модерн і постмодерн. Інформаційна епоха є періодо постмодерну, коли розвинені суспільства Заходу, передусім США, переходять до якісно нової фази. Теорія мережевих воєн є моделлю військової стратегії в умовах постмодерну. Як

стандарти нової економіки, засновані на інформації і високих технологіях, сьогодні доводять перевагу над традиційними капіталістичними і соціалістичними моделями промислової епохи, так і мережеві війни претендують на якісну перевагу над колишніми стратегічними концепціями індустріальної епохи. Сенс військової реформи у рамках нової теорії війни інформаційної епохи полягає у створенні потужної і всеосяжної мережі, яка концептуально замінює собою попередні моделі та поняття військової стратегії, інтегрує їх в єдину систему. Війна стає мережевим явищем, а військові дії є різновидом мережевих процесів» [59].

Інформаційну перевагу можна визначити, як створення та використання інформаційних переваг, яке сприяє досягненню цілей. Тут слід наголосити на таких моментах. По-перше, це важливість розуміння інформаційних аспектів операційного середовища як передумови розробки ефективних способів створення та використання переваг. Інформаційні міркування – це ті аспекти людського, інформаційного та фізичного вимірів, які впливають на те, як люди й автоматизовані системи отримують знання з інформації, використовують, діють і на них впливає інформація.

Другий момент – це визнання того, що існує багато форм інформаційних переваг, а не лише одна головна умова, що стосується всієї інформації. Наприклад, сторона, яка збирає, обробляє, аналізує та використовує інформацію, щоб розуміти, приймати рішення та діяти ефективніше, ніж опонент, - має перевагу. Однак ця сама сторона може бути в інформаційно невигідному становищі, оскільки протиборча сила ефективно використовує інформацію, щоб впливати на відповідну поведінку актора в протистоянні цілям.

Третій момент, на який слід звернути увагу, – це тимчасовий і відносний характер інформаційної переваги. Як фізичні та людські переваги, інформаційні переваги часто є тимчасовими та змінюються з часом залежно від адаптивного супротивника та змін у робочому середовищі. Тоді як одна сторона шукає інформаційної переваги, сили загрози роблять те саме. Інформаційна перевага –

це те, що можна здобути, захистити та використати під час конфлікту та поза ним.

Процес створення інформаційних переваг використовує всі можливості за допомогою п’яти інформаційних заходів – це забезпечення, захист, інформування, вплив та атака. Кожна інформаційна діяльність включає кілька завдань та підзавдань для досягнення різних цілей, які засновані на актуальних загрозах. Керуючись принципами інформаційної переваги слід планувати, готувати, виконувати та оцінювати інформаційну діяльність як частину загального операційного процесу.

Активна інформаційна діяльність включає завдання для покращення розуміння ситуації та прийняття рішень. Діяльність із захисту інформації включає завдання, які забороняють доступ загроз до інформації, зберігаючи при цьому можливості підтримки зв’язку. Інформаційна діяльність включає завдання , які сприяють формуванню інформованого сприйняття військових операцій і діяльності в різних аудиторіях. Ця діяльність зосереджена на збереженні довіри та впевненості внутрішньої та зовнішньої аудиторії.

Інформаційна діяльність *впливу* включає завдання, які впливають на мислення і, в кінцевому підсумку, на поведінку іншої сторони. Ця діяльність зосереджена на зміцненні або зміні того, як люди чи групи думають, відчувають і діють щодо підтримки цілей. Інформаційна діяльність щодо атаки включає завдання, які впливають на здатність загрози здійснювати С2. Ця діяльність зосереджена на впливі на дані про загрози та їхні фізичні можливості, які використовуються для зв’язку та ведення інформаційної війни. Це включає дані та зв’язок між автоматизованими системами, як-от зв’язок між радарами, системами керування вогнем і системами стрільби.

Інформаційна діяльність взаємозалежна. Наприклад, інформаційна діяльність із захисту та інформування допомагає захистити війська від зловмисного впливу. Інформаційна діяльність щодо впливу та атаки впливає на здатність загрози до С2, але використовує різні засоби. Синхронізація операцій військової інформаційної підтримки (засіб впливу) для посилення наслідків

атаки в кіберпросторі (засіб атаки) являє собою загальновійськовий підхід до приниження загрози С2.

Поєднання та виконання всіх інформаційних дій для досягнення цілей, спрямованих на загрозу, сприяє гнучкості та здатності розуміти, приймати рішення та діяти ефективніше, ніж загроза. Активація та захист інформації підвищують ефективність циклу прийняття рішень. Інформаційна діяльність щодо впливу та атаки знижує ефективність циклу прийняття рішень щодо загрози. Інформаційна діяльність використовується як для покращення С2, так і для погіршення циклу прийняття рішень щодо загроз. Сукупний ефект покращення циклу прийняття рішень із одночасним зменшенням загроз створює значну інформаційну перевагу для армії.

Щоб спрямувати мислення щодо використання інформації та використання можливостей для створення інформаційних переваг, слід застосовувати відповідні принципи.

Перший принцип – орієнтація на напад – орієнтований на ініціативу. Будь-яка інформаційна перевага, яку не прагнуть або активно не захищають, потенційно передається загрозі. Політичні лідери зберігають наступальний настрій і передбачають події в процесі створення інформаційних переваг.

Принцип зв’язку пов’язаний з ідеєю, що будь-яка діяльність має невід’ємний інформаційний ефект і що всі можливості слід використовувати для здобуття інформаційної переваги. Слід поєднувати наявні органічні, спільні, міжвідомчі та багатонаціональні можливості та підсилювати цей процес іншими засобами, щоб увімкнути С2, захистити інформацію та мережі, інформувати аудиторію, впливати на загрози та інших відповідних учасників, а також атакувати загрозу С2.

Третій принцип пов’язаний з ідеєю, що інформація є центральною для всіх дій, які здійснюють політичні (військові) сили. Тому командири повинні розуміти інформацію та продумано інтегрувати її за допомогою політичного управління, військових дій під час планування. Інформацію слід вважати ресурсом для досягнення розуміння ситуації, інструментом для створення

двозначності та невизначеності щодо загрози та основним засобом керування військовими силами. Інформаційну перевагу використовують для проникнення в процеси прийняття рішень щодо загроз, використання інформаційних залежностей, досягнення несподіванки та руйнування загрози зсередини.

Четвертий принцип в тому, що всі, хто приймає участь в інформаційному протиборстві, в процесі здобуття та використання інформаційних переваг - повинні захищати інформацію. Ми всі споживаємо, передаємо та покладаємося на інформацію для досягнення мети. Всі суб'єкти цього процесу повинні зберігати свою цифрову грамотність і готовність, оскільки користуються різними інформаційними системами, необхідними для зв'язку. Вони повинні розуміти вплив, який здійснюють відповідні дії та повідомлення. Це вимагає більш глибокого розуміння мети та відпрацювання операційної безпеки за допомогою всіх форм медіа, включно з особистими обліковими записами медіа, як під час інформаційного протиборства, так і під час перебування в стані спокою.

Концепція інформаційних переваг базується на ідеї, що інформація має важливе значення для всіх функцій ведення війни, і всі функції ведення війни можуть сприяти інформаційним перевагам щодо загроз.

Інформаційна діяльність організовує різні завдання та можливості з таких військових функцій: C2, розвідка, пересування та маневр, вогонь, захист та підтримка. Функція C2 безпосередньо сприяє активній інформаційній діяльності. Уся система C2 (люди, процеси, мережі) розроблена для підтримки можливості розуміти, візуалізувати, описувати, керувати, керувати та оцінювати швидше та ефективніше, ніж їхні опоненти.

Розглядаючи інформаційну діяльність як інтегровану систему, можна стверджувати, що її ефективність та результативність глибоко взаємопов'язані з фундаментальними функціями військової діяльності, кожна з яких вносить свій специфічний та незамінний внесок у її розгортання та досягнення стратегічних цілей.

Так, розвідувальна функція виступає в ролі інтелектуального ядра інформаційної діяльності. Її першочергове завдання полягає не лише у зборі первинних даних, але й у їхній глибокій обробці, аналізі та перетворенні на релевантну інформацію та якісні розвідувальні відомості. Ці знання, що є результатом розвідувальної діяльності, формують критично важливе підґрунтя для всебічного розуміння оперативного середовища, виявлення ключових тенденцій, прогнозування можливих дій противника та оцінки власних можливостей. Саме всеосяжне розуміння ситуації, забезпечене розвідкою, стає тим інтелектуальним компасом, який уможливлює прийняття обґрунтованих та своєчасних рішень на всіх етапах та рівнях інформаційних операцій.

У свою чергу, функція руху та маневру набуває в контексті інформаційної діяльності розширеного тлумачення, охоплюючи не лише фізичне переміщення сил, але й динамічне розгортання інформаційних ресурсів та впливів. Розвіддані про диспозицію противника та характеристики оперативного простору є критично важливими для оптимізації розгортання власних інформаційних активів, забезпечення їхньої живучості та ефективного застосування. Операції безпеки, спрямовані на захист власних інформаційних систем та критичних вузлів управління (С2), є невід'ємною складовою забезпечення стійкості інформаційної діяльності. Водночас, стратегічне розташування та маневрування інформаційними силами, включаючи демонстрацію можливостей та темпу інформаційних операцій, є потужним інструментом впливу на сприйняття противника, сигналізуючи про наміри та потенціал. Активні дії, такі як інформаційні рейди та атаки, можуть бути спрямовані на нейтралізацію або руйнування інформаційних систем та інфраструктури управління противника, створюючи інформаційну перевагу.

Функція пожежогасіння, в інформаційному вимірі, трансформується у застосування кібернетичних та електромагнітних засобів впливу. Ці інструменти можуть використовуватися як для активного захисту власних інформаційних ресурсів шляхом створення перешкод та протидії ворожим

атакам, так і для здійснення безпосереднього впливу на інформаційні системи противника, порушуючи їхню функціональність та ефективність управління.

Важливим аспектом є інтеграція функції захисту та дій безпосередньо в інформаційну діяльність. Завдання, що входять до цієї функції, такі як забезпечення живучості власних інформаційних систем, протиповітряна та протиракетна оборона критично важливих інформаційних вузлів, електромагнітний захист від ворожого впливу, безпека операцій на всіх рівнях, а також кібербезпека та захист інформаційних мереж, є фундаментальними для забезпечення стійкості та безперервності власної інформаційної діяльності в умовах активного протистояння.

Нарешті, функція підтримки військових дій відіграє всеосяжну роль у забезпеченні ефективності інформаційної діяльності. Вона охоплює не лише матеріально-технічне забезпечення (укомплектування особовим складом, оснащення необхідними технічними засобами, технічне обслуговування та постачання ресурсів), але й стратегічний вплив на інформаційне середовище через підтримку лояльних учасників. Своєчасне та адекватне надання підтримки певним акторам в інформаційному просторі може суттєво зміцнити їхню позицію, вплинути на їхню поведінку та сприяти досягненню бажаних інформаційних ефектів.

Таким чином, інформаційна діяльність не є ізольованим процесом, а глибоко інтегрована в загальну систему військової діяльності. Кожна з фундаментальних військових функцій вносить свій унікальний та незамінний внесок у її розгортання, забезпечуючи необхідні умови для розуміння ситуації, активного впливу, ефективного захисту та всебічної підтримки, що є критично важливим для досягнення стратегічних цілей в сучасному динамічному та інформаційно насиченому операційному середовищі.

Вищенаведене дозволяє сформулювати ряд ключових висновків щодо трансформації інформаційного середовища та еволюції інформаційного протистояння в умовах розвитку цифрових технологій.

Перш за все, сучасне інформаційне середовище якісно відрізняється від попередніх епох завдяки появі цифрових засобів виробництва, зберігання та передачі інформації. Ця фундаментальна зміна зумовила необхідність переосмислення підходів до розуміння інформаційних процесів, що знайшло відображення у розвитку кібернетичної гносеології. Остання, базуючись на концепції подібності інформаційних процесів на різних рівнях організації матерії (від біологічного організму до суспільства), розглядає інформаційне середовище як поле постійної боротьби із зовнішніми загрозами, аналогічної боротьбі живих організмів з патогенами.

У другій половині XX століття усвідомлення комплексу проблем, пов'язаних з інформаційним протистоянням, призвело до формування концепту «інформаційної війни». Незважаючи на активне використання цього терміну в науковому та політичному дискурсі, досі не існує його загальновизначеного визначення, що ускладнює розуміння сутності та методів ведення такої війни. Тим не менш, вже перші спроби осмислення інформаційної війни, зокрема праці Т. Рона, підкреслили зміщення акценту з інформації як об'єкта військових операцій на інформацію як активний метод досягнення військово-політичних цілей.

Інформаційне протистояння розглядається як сукупність дій та протидій захисного та наступального характеру, спрямованих на встановлення контролю над інформаційним простором та стратегічне позиціонування інтерпретації інформації. Інформаційна війна, на відміну від інформаційного протистояння, характеризується якісно вищою інтенсивністю застосовуваних засобів і методів, метою яких є досягнення радикального результату, аж до повного домінування та знищення опозиційного інформаційного контенту. Важливим аспектом є проблема інтерпретації інформації, оскільки сторони конфлікту можуть використовувати одні й ті самі дані, але надавати їм протилежні значення.

Глобалізація та інформатизація призвели до появи постмодерних держав, для яких поняття суверенних кордонів стає менш значущим, що робить їх

потенційними суб'єктами геополітичної інформаційної війни, особливо в прикордонних регіонах з невирішеними територіальними суперечками, де інформаційна війна може набувати форми "картографічної війни".

Інформаційна війна ведеться шляхом цілеспрямованого впливу на противника за допомогою інформаційних «квантів» – повідомлень, актів комунікації – з метою формування необхідної громадської думки та системи цінностей. Стратегічне позиціонування певним чином «заряджених» інформаційних квантів у суспільстві призводить до формування імперативів та регуляторів суспільних відносин, які складно піддаються юридичному чи моральному регулюванню.

Сучасні військові операції відбуваються в умовах експоненціального зростання інформаційних технологій, що значно розширює можливості збору, обробки, аналізу, зберігання та передачі інформації. Розвиток супутникових систем, обчислювальної техніки, мобільних мереж та соціальних медіа кардинально змінює способи використання інформації для досягнення військових цілей. При цьому важливо усвідомлювати, що потенційні противники також володіють аналогічними технологічними можливостями.

Для розуміння сучасної війни необхідно враховувати її латентний характер, постійну зміну засобів ведення, поєднання класичних та некласичних аспектів, а також зростаючу роль науково-технічної складової. Концепція мережецентричної війни (NCW), розроблена у США в 1990-х роках, є спробою перетворити інформаційну перевагу на посилення бойових можливостей шляхом інтеграції мережевих датчиків, осіб, що приймають рішення, та вогневих засобів для досягнення спільної обізнаності та підвищення темпу операцій. В основі NCW лежить перенесення акценту з платформи на мережу, розуміння акторів як частини динамічної екосистеми та важливість стратегічної адаптації в умовах швидкозмінних середовищ.

Інформаційна перевага визначається як створення та використання інформаційних можливостей для досягнення поставлених цілей. Важливими аспектами є розуміння інформаційних аспектів операційного середовища,

визнання множинності форм інформаційних переваг та усвідомлення їх тимчасового та відносного характеру. Процес створення інформаційних переваг включає п'ять основних інформаційних заходів: забезпечення, захист, інформування, вплив та атака, які є взаємозалежними та потребують синхронізації для досягнення максимального ефекту.

Принципи досягнення інформаційної переваги включають орієнтацію на напад, усвідомлення невід'ємного інформаційного ефекту будь-якої діяльності, центральну роль інформації у всіх діях, а також необхідність захисту інформації всіма учасниками інформаційного протиборства. Концепція інформаційних переваг інтегрується з основними функціями ведення війни (C2, розвідка, пересування та маневр, вогонь, захист та підтримка), кожна з яких може сприяти створенню інформаційних переваг щодо противника.

На локальному рівні перспективним є підхід до розуміння інформаційної війни через гібридні моделі, що поєднують моделі визначеного інформаційного простору та соціальних мереж. Ці моделі враховують організаційні та когнітивні аспекти поширення інформації, а також вплив соціальних зв'язків на формування переконань. Концепція транзактивної пам'яті підкреслює важливість динамічного використання знань у групових системах пам'яті.

Теорія мережевих війн розглядає війну як мережеве явище, а військові дії – як різновид мережевих процесів, що відповідає інформаційній епосі та постмодерній парадигмі розвитку суспільства.

Цілі інформаційної війни включають попередження конфлікту, ослаблення морального духу противника, внесення ворожих ідей, дезорієнтацію мас, руйнування інформаційних мереж, ослаблення патріотизму, провокування відмови від бойових дій, залякування власного народу та противника, а також створення передумов для досягнення воєнно-політичних цілей з мінімальними втратами. Принципи ведення інформаційної війни включають відповідність політичним цілям, зосередження сил, всебічну підготовку, високу активність, узгоджене застосування сил і засобів, раптовість ударів, постійну готовність до захисту власної інформації та атаки

інформаційного середовища противника, безперервність, напруженість, своєчасний маневр, врахування духовного фактору, всебічне забезпечення, твердість управління та непохитність у досягненні цілей.

Таким чином, сучасне інформаційне середовище є складною та динамічною системою, в якій інформаційне протистояння набуло якісно нових рис завдяки розвитку цифрових технологій. Концепція інформаційної війни еволюціонувала від розуміння інформації як об'єкта впливу до її сприйняття як активного інструменту політичної та військової боротьби. Мережецентричні підходи та гібридні моделі відображають прагнення до більш глибокого розуміння механізмів інформаційного впливу та протидії в умовах глобалізованого та цифровізованого світу. Досягнення інформаційної переваги стає ключовим фактором успіху в сучасних конфліктах, що вимагає комплексного підходу до забезпечення інформаційної безпеки та розвитку відповідних стратегій і технологій.

2.2. Алгоритми, форми та ключові умови реалізації інформаційних операцій.

В умовах демократичного суспільства громадяни контролюють вибір інструментів, які використовуються в різних сферах діяльності, включаючи засоби ведення війни. Обґрунтованим цей вибір буде лише тоді, коли наміри людей мають як моральне, так і технологічне підґрунтя. Ігнорування моральних аспектів призводить до ланцюгової реакції: втрачається суспільна підтримка, не використовуються новітні технологічні досягнення, і в результаті збройні сили залишаються без необхідних засобів. У цьому контексті ми розглянемо теорію інформаційної зброї як складову загальної системи засобів збройної боротьби та способи її застосування на стратегічному й оперативному рівнях.

На сьогоднішній день існують доступні засоби для створення інформаційної зброї. Враховуючи її велику силу, виникає необхідність захисту як військових, так і цивільного населення від її впливу. Кожна людина

потенційно вразлива до інформаційної зброї. Уряд стоїть перед вибором: розробляти таку зброю чи притягувати до відповідальності тих, хто цим займається. Це рішення має базуватися на глибокому аналізі всіх аспектів та усвідомленні морально-етичних ризиків, пов'язаних з інформаційною зброєю. Окрім врахування потенційних небезпек при прийнятті рішень щодо створення інформаційної зброї, необхідно, щоб люди розуміли принципи її дії та теорію застосування ще до її фактичного використання.

Під інформацією ми розумітимемо зміст або значення повідомлення. Головна мета засобів збройної боротьби полягає у впливі на інформаційні системи противника. У широкому розумінні інформаційні системи охоплюють усі інструменти, за допомогою яких супротивник отримує знання або формує припущення (системи знань і переконань).І. Денисовець говорить, що «інформаційно-психологічні операції складаються з політичних, військових, економічних, дипломатичних і суто інформаційно-психологічних заходів, спрямованих на конкретні групи населення з метою доведення до них далекосяжних ідеологічних і соціальних настанов, формування помилкових стереотипів поводження, трансформації в потрібному напрямі їхніх настроїв, почуттів, волі. У психологічних та інформаційних операціях йдеться про визначену структуру нав’язування моделі світогляду, відчуття та сприймання навколишнього середовища, які покликані забезпечити бажані типи поведінки об’єкта впливу» [15].

Для військових інформаційні системи є ключовим інструментом отримання даних про бойову обстановку та управління військами противника. Загалом, інформаційні системи являють собою сукупність знань, гіпотез, процесів прийняття рішень і систем опонента. Результатом інформаційних атак на будь-якому рівні є надання противнику такої інформації, яка спонукає його до припинення бойових дій.

З розвитком суспільних інститутів ускладнювалися й інформаційні системи, а разом з ними – процеси прийняття рішень. Фінансово-промислові об'єднання, що формувалися на основі домінуючих політичних структур,

збільшували складність систем зі зростанням їхньої діяльності. З'явилися мережі інформаційних зв'язків між інтелектуальними працівниками – найсучасніша форма інституційної організації, чисельність яких, як і доступність інформаційних технологій, стрімко зросла. Розвиток інформаційних технологій призвів до появи знань та практичних навичок, які підвищили ефективність інших інституційних форм.

З часом удосконалювалися й методи збройної боротьби. Жахливі звуки барабанів, прапори чи гонги часів Сунь-цзи в епоху інформаційних технологій трансформувалися у витончені психологічні операції. Метою війни стало не лише руйнування, а й відновлення контролю.

Збройне протистояння являє собою низку летальних і нелетальних дій, спрямованих на придушення ворожих дій противника. У цьому контексті «збройний конфлікт» не є синонімом слова «війна». Він не обов'язково передбачає оголошення війни або існування стану, який загальноприйнято розуміється як «стан війни». Збройний конфлікт організовується групами осіб, які контролюються або фінансуються державою, або діють самостійно. Збройне зіткнення – це ворожі дії проти ворога, метою яких не обов'язково є його вбивство, а лише приборкання. В ідеалі, найвищим мистецтвом є підкорення ворога без його знищення. Супротивник вважається підкореним, коли його дії відповідають очікуванням агресора або захисника. Прагнучи зламати волю ворога, необхідно чітко розуміти, якої неворожої поведінки ми від нього очікуємо та якої ворожої поведінки прагнемо уникнути.

У випадку збройного конфлікту між державами уряд визначає бажану неворожу поведінку противника. Коли ж у збройне протистояння вступають дві недержавні групи, наприклад, клан чи партизанський загін, лідер групи вирішує, яка неворожа поведінка є прийнятною. В обох випадках керівники груп приймають рішення щодо цілей, методів та бажаного післяконфліктного стану. Найважливішим відкриттям, що започаткувало інформаційну епоху, стало усвідомлення того, що будь-який об'єкт навколишнього світу може бути представлений як комбінація нулів та одиниць. Ці комбінації можуть

передаватися в електронному вигляді як дані та збиратися на приймальній стороні, формуючи інформацію.

Інформаційна війна – це форма конфлікту, в якій прямі атаки на інформаційні системи використовуються як засіб впливу на знання або припущення противника. Інформаційна війна може бути складовою ширших воєнних дій, таких як мережева або кібервійна, або ж виступати як самостійна форма ведення війни. Більшість видів зброї, що використовуються у збройних конфліктах (як летальних, так і нелетальних), можуть бути застосовані лише проти зовнішніх ворогів. Однак засоби ведення інформаційної війни, хоча найчастіше спрямовані проти зовнішніх противників, можуть використовуватися і проти внутрішніх. Наприклад, держава рідко застосовує зброю чи бомби проти своїх громадян. Проте засоби інформаційної війни можуть і будуть використовуватися як проти зовнішніх, так і проти внутрішніх ворогів.

Внутрішнім ворогом може бути зрадник, дисидент або будь-хто, хто протистоїть лідеру, який контролює засоби інформаційної війни, або недостатньо його підтримує. Якщо члени групи не підтримують цілей лідера під час бойових дій, внутрішня інформаційна війна (включаючи пропаганду, брехню, терористичні акти та чутки) може бути використана для того, щоб змусити їх бути більш лояльними до цілей керівництва.

Незалежно від того, проти якого ворога вона заявлена, інформаційна війна має кінцевою метою використання інформаційних засобів для впливу (маніпулювання або атаки) на системи знань і припущень якогось зовнішнього ворога. Наприклад, під час війни зовнішньому ворогові корисно знати або принаймні припускати, що проти нього об'єдналася інша держава чи група. Інформаційна війна, яка ведеться як для того, щоб громадяни держави діяли узгоджено, так і для того, щоб зовнішні вороги повірили, що їх ворог бореться з ними єдиним строєм, використовується для того, щоб донести ці знання до свідомості лідерів противника.

Системи знань - це системи, які створюються і функціонують для виявлення перевірених феноменологічних показників або позначення, переведення цих показників в сприйняту реальність і використання цих первинних відчуттів для прийняття рішень і дій. Системи знань організовуються відповідно до наукових принципів і підтримуються науковим методом. Тобто системи знань призначені для збору емпіричних даних за допомогою спостереження для висунення гіпотез, для проведення тестів, які підтверджують або відкидають ці гіпотези, і для використання цих висновків як основи для подальших дій. Системи припущень - це ті, які прямо чи опосередковано орієнтовані на використання як емпіричних даних у вигляді перевірених спостережень, так і інших видів даних або недостовірних даних (кошмари, фобії, психози, неврози та всі інші творіння підсвідомого та колективного несвідомого), які не підтверджуються або, принаймні, не легко підтверджуються.

За словами Дж.Бойда, процес або акт орієнтації – те, що Бойд називає великим О в циклі спостереження-орієнтація-рішення – також може бути під впливом генетичної спадщини або культурних традицій. Тому орієнтація американських лідерів відрізняється від, скажімо, орієнтації японських або китайських лідерів. Орієнтація капіталістів і їх вождів відрізняється від орієнтації соціалістів і їх вождів.

На відміну від систем знання, системи припущень дуже індивідуальні. Вони включають в себе елементи несвідомого і підсвідомого, про які їх носій може навіть не здогадуватися. Хоча мішенню інформаційної зброї є уми лідерів противника, помилково думати про ворога як про єдиний розум. Насправді ворог – це багато окремих ворогів, і у кожного свій розум. Але це лише трохи ускладнює проблему. Наприклад, якщо противник розігнаний, то окремі уми можуть бути атаковані окремо, використовуючи факт ізоляції на свою користь з боку нападників. Якщо ворог сконцентрований, то атаки мають здійснюватися проти великої групи людей.

Незважаючи на це, метою збройної боротьби є придушення ворожих намірів лідерів і осіб, які приймають рішення. Це може бути зроблено за допомогою прямих атак, які впливають на знання або припущення лідерів або маніпулюють ними, або непрямих атак, спрямованих на знання або припущення тих, на кого лідери покладаються при прийнятті рішень. Лідерів та осіб, які приймають рішення, зазвичай легко визначити в будь-якій організації. Коли організація має в своєму розпорядженні засобами збройної боротьби, як правило, ця організація має ієрархічну характеристику. Тому знання та припущення тих, хто приймає рішення, є ахіллесовою п'ятою ієрархій.

Системи знання, оскільки вони більш наукові, менш схильні до культурних та ірраціональних факторів, ніж системи припущень, але як системи знань, так і системи припущень є частиною будь-якої системи прийняття рішень, де є люди.

Те, що відомо, включаючи методи, за допомогою яких воно стало відомим, може бути перевірено у зв'язку з чимось іншим і визначено як істинне або хибне, істинне або хибне. Припущення не піддаються всім цим перевіркам. Причому припущення не менш значущі, ніж знання, отримані емпіричним шляхом. Як знання, так і припущення впливають на прийняття рішень людиною. Оскільки метою збройної боротьби є вплив на поведінку противника шляхом впливу на прийняття ним рішень, інформаційні атаки повинні бути спрямовані як проти систем знань, так і проти систем припущень.

Якщо противником є коаліція з кількох центрів, то в цій коаліції може бути кілька систем припущень. Всіх їх можна перемогти. Коаліція не обов'язково повинна бути групою держав або об'єднанням груп людей. Коаліція може бути сформована людьми всередині держави або групи. Наприклад, теоретик військової справи та реформатор Карл Клаузевіц говорить, що «альянси та коаліції потенційно слабкі» [29]. Більше того, лідери та особи, які приймають рішення, є кращою мішенню для прямих або непрямих атак.

Інформаційна війна розглядається як стратегічне протистояння, націлене на фундаментальні основи пізнання противника – його епістемологію, що

охоплює організацію, структуру, методи та обґрунтування знань. Ключовою метою на стратегічному рівні є не просто вплив на рішення ворога, а й маніпулювання його сприйняттям реальності таким чином, щоб він не усвідомлював зовнішнього впливу. Навіть якщо повне досягнення цієї мети є складним, вона залишається орієнтиром для стратегічних інформаційних кампаній. Успіх, навіть частковий, на цьому рівні призводить до того, що ворог приймає рішення та вчиняє дії, які суперечать його власним інтересам або перешкоджають їх реалізації.

На оперативному рівні інформаційні атаки мають на меті підірвати здатність противника до швидкого та ефективного прийняття рішень, тим самим сприяючи досягненню стратегічних цілей. Іншими словами, оперативні інформаційні дії спрямовані на дезорганізацію процесу прийняття рішень ворога, унеможливлюючи його злагоджену та ефективну військову діяльність. Суть інформаційної війни полягає в гармонізації дій на обох рівнях – стратегічному та оперативному – таким чином, щоб їх сукупний ефект змушував противника приймати рішення, що ведуть до дій, які сприяють нашим цілям і водночас перешкоджають досягненню цілей ворога.

Розробляючи стратегічний план інформаційної кампанії, керівництво має чітко розуміти щонайменше три ключові аспекти:

Стратегічна інтеграція: Як інформаційна кампанія узгоджується з ширшими цілями всієї військової кампанії? Яке її місце в загальній стратегії? Бажаний когнітивний стан ворога: Які знання, переконання чи припущення ми прагнемо сформувати у ворожого керівництва на завершення кампанії? Який бажаний епістемологічний результат є критерієм успіху нашої операції?

Інструменти впливу: Які конкретні засоби інформаційної війни є найбільш ефективними для досягнення визначеного критерію успіху? Яким чином застосування цих засобів призведе до бажаного результату?

На оперативному рівні також необхідно відповісти на ряд важливих питань, що стосуються обмежень, досяжності цілей та управління: чи існують заборонені цілі для інформаційних атак або неприпустимі методи їх здійснення;

чи є бажаний гносеологічний стан універсально досяжним, чи існують лише проміжні стани, які можуть бути досягнуті в певних географічних зонах, у визначеній послідовності або в конкретних сферах інформаційної війни; які існують органи управління інформаційними операціями та які сигнали використовуються для координації дій. Крім того, оперативне керівництво повинно мати чітке розуміння того, коли інформаційні атаки будуть завершені та яким чином буде передано сигнал про їх припинення. Це критично важливо, оскільки інформаційна зброя здатна опосередковано руйнувати системи знань та переконань противника. У найгіршому сценарії, реакцією противника можуть стати симетричні відповідні удари по власних інформаційних системах, що за своїми наслідками можна порівняти зі знищенням вогневої підтримки.

Окремої уваги заслуговують цілі інформаційних атак. Чим більша залежність противника від інформаційних систем у процесі прийняття рішень, тим вища його вразливість до ворожого маніпулювання цими системами. Специфічні види інформаційної зброї мають свої обмеження: комп'ютерні віруси діють лише в системах з програмним забезпеченням, радіоелектронна боротьба ефективна проти сил, що використовують радіо та електроніку, а електромагнітні гармати не вплинуть на комунікацію через кур'єрів.

Хоча це може створювати враження, що інформаційна війна є загрозою лише для постіндустріальних держав, це не зовсім так з двох причин: вразливість епістемологічних систем доіндустріальних суспільств: Інформаційна війна може бути спрямована на всю систему знань противника, тому навіть примітивні суспільства є вразливими до її впливу; залежність індустріальних суспільств від технологій розвинених країн: Індустріальні держави можуть значною мірою залежати від телекомунікаційної інфраструктури, придбаної у більш розвинених постіндустріальних суспільств, що робить їх вразливими.

У високотехнологічних державах або угрупованнях спектр стратегічних цілей для інформаційних атак є надзвичайно широким: телекомунікаційні мережі та телефонія, супутникові системи, автоматизовані системи фінансової,

банківської та комерційної діяльності, інтернет, культурні інститути та вся сукупність технологій і програм, на яких базується отримання знань противником. Стратегічні інформаційні системи в таких державах часто дублюються на оперативному рівні, і всі вони є потенційними цілями для атак.

Інформаційну війну не слід розглядати як захід останньої інстанції, що застосовується лише після початку відкритого конфлікту. Вже на етапі підготовки до можливого конфлікту інформаційні операції можуть мати значний вплив. Вороже керівництво буде менш схильним до початку війни, якщо воно матиме певні переконання або припущення, наприклад: негативне ставлення до насильства, відсутність союзників, загроза санкцій, нездатність промислової бази підтримувати тривалу війну або неготовність збройних сил.

Чим вищий рівень технологічного розвитку держави та чим інтенсивніші її взаємодії з іншими групами (включаючи внутрішні) або державами, тим більшою є її вразливість в інформаційній війні. Ця вразливість зростатиме пропорційно до розміру мереж, кількості та обсягу транзакцій.

Демократичні держави не є менш вразливими, ніж тоталітарні режими, хоча окремі соціальні групи в демократичних суспільствах можуть проявляти дещо більшу стійкість до інформаційних збоїв. Однак їхній економічний апарат управління є вразливим. Банківська система, фінанси, торгівля, транспортні перевезення, зокрема управління повітряним рухом, все більше залежать від інформаційних технологій.

Зі зростанням залежності від інформаційних систем, збройні конфлікти, організовані терористичними групами, релігійними екстремістами або вороже налаштованими представниками бізнесу, спрямовані проти цих систем, становитимуть реальну загрозу. Інформаційна зброя в їхніх руках може бути націлена на критично важливу інфраструктуру, таку як електромережі або комунікаційні об'єкти, що безпосередньо впливає на прийняття рішень на вищому рівні. Одночасні скоординовані атаки на різні ключові вузли можуть мати стратегічний ефект, тобто впливати на знання та волю лідерів.

Выдносно сфери використання інформаційної зброї М.Харченко, Сапогов С., Шамраєва В., Новікова Л. зазначають, що вона «включає як воєнну галузь, так і інші галузі потенційного використання з метою дезорганізації діяльності управлінських структур, транспортних потоків та засобів комунікації, блокування діяльності окремих підприємств та банків, а також цільових галузей промисловості шляхом порушення технологічних зв'язків та системи взаєморозрахунків і т.ін., ініціювання техногенних катастроф на території противника через порушення управління технологічними процесами та об'єктами, масового поширення у свідомості людей певних уявлень, поведінкових стереотипів, виклик невдоволення або паніки, а також провокування деструктивних дій різноманітних груп» [74].

В.Антонюк, характеризуючи динаміку розвитку інформаційного інструментарію, зазначає, що «вимагає розмежування розуміння інформаційної, психологічної та кібернетичної війн». Вчений відзначає, що «сутність інформаційної війни полягає в управлінні інформаційним потоками, водночас сутність психологічної війни – в зміні характеристик суспільної свідомості в бажаному напрямі, сутність кібервійни, як невід'ємної (диверсійної) складової інформаційно-пропагандистської війни полягає в руйнуванні системи управління інформацією. Організація і ведення інформаційної війни мають базуватися на відповідних законах, закономірностях і принципах» [1].

В.Антонюк виводить основні закони та закономірності інформаційної війни. До них вчений відносить «закон визначальної ролі її політичних цілей; залежності її ходу і результатів від економічних, соціально-політичних, науково-технічних і військових можливостей супротивників». До закономірностей відноситься «залежність форм і способів її ведення, її ефективності від кількості та якості засобів інформаційного впливу, а також особового складу, залежність цілей інформаційної війни від наявних сил і засобів їх застосування, залежність досягнення цілей інформаційної війни від єдності інформаційних дій суб'єктів інформаційної діяльності в часі і просторі, нерівномірність розподілу сил і засобів по всій інформаційній сфері,

нерівнозначність впливу різних сил і засобів на інформаційній сферу супротивника» [1].

Слід погодитися з висновком вченого, що «інформаційна зброя – це засоби знищення, перекручення або розкрадання інформаційних масивів, добування з них необхідної інформації після подолання систем захисту, обмеження або заборони доступу до них законних користувачів, дезорганізації роботи технічних засобів, виведення з ладу телекомунікаційних мереж, комп'ютерних систем, всього високотехнологічного забезпечення життя суспільства і функціонування держави».

Інформаційна зброя від звичайних засобів ураження відрізняє: «скритність – можливість досягати мети без видимої підготовки і оголошення війни; масштабність – можливість наносити непоправної шкоди, не визнаючи національних кордонів і суверенітету, без обмеження простору у всіх сферах життєдіяльності людини; універсальність – можливість багатоваріантного використання як військових, так і цивільних структур країни нападу проти військових і цивільних об'єктів країни поразки. При цьому, за своєю результативності інформаційна зброя порівнюється зі зброєю масового ураження. Доведено, що найбільших втрат збройні сили несуть від впливу вражаючих елементів інформаційної зброї, що діють на системи управління та психіку людини».

Відповідно до концепції американських вчений «інформаційна війна реалізується на двох рівнях: державному та військовому. На державному рівні мета інформаційного протиборства полягає у послабленні позицій конкуруючих держав, порушенні системи державного управління за рахунок інформаційного впливу на політичну, дипломатичну, економічну та соціальну сфери суспільного життя, здійснення психологічних операцій, підривних та інших пропагандистських акцій. На військовому рівні інформаційна війна є складовою частиною військових кампаній й спрямовані на досягнення інформаційної переваги шляхом впливу на інформацію та інформаційні системи супротивника з одночасним зміцненням і захистом власної інформації,

інформаційних систем та інфраструктури. Поступово військове керівництво США перестало використовувати в офіційних документах термін information warfare, віддавши перевагу терміну information operation».

Згідно з Доктриною інформаційних операцій США від 2006 року, інформаційна операція розглядається як скоординоване застосування засобів радіоелектронної боротьби (впливу на ворожу техніку електромагнітним випромінюванням), комп'ютерних мережевих операцій, психологічних операцій, військових операцій з введення в оману та заходів безпеки. Їхня мета полягає у впливі на противника, зриві його процесу прийняття рішень та одночасному захисті власних рішень. Ключовим завданням інформаційних операцій є саме вплив на процес прийняття рішень та супутні йому дії.

Основна стратегічна мета інформаційних операцій полягає у стримуванні потенційних або явних противників, а також інших цільових груп від дій, що можуть завдати шкоди національним інтересам держави.

Психологічні операції – це комплекс заходів з поширення спеціально підготовленої інформації, спрямованих на вплив на емоційний стан, мотивацію, логіку дій, процес прийняття рішень і поведінку конкретних лідерів, організацій, соціальних чи національних спільнот, а також окремих громадян інших країн. Завдання цих операцій – досягти результатів, що відповідають інтересам держави-ініціатора та її союзників.

Психологічні операції є важливим інструментом реалізації інформаційних операцій. Згідно з польовим статутом армії США, психологічні операції визначаються як спланована пропагандистська та психологічна діяльність, націлена на іноземні ворожі, дружні або нейтральні аудиторії з метою зміни їхніх поглядів і поведінки у напрямку, що сприяє досягненню політичних і військових національних цілей США.

Пропаганда являє собою систематичне та цілеспрямоване поширення певних ідей для впливу на думки, почуття, ставлення або поведінку цільових аудиторій з метою отримання прямих або непрямих вигод для держави, яка її проводить.

Психологічні акції включають використання засобів масової інформації та додаткових заходів (таких як демонстрація сили, мітинги, демонстрації тощо) як у мирний, так і у воєнний час, з метою підриву авторитету та впливу противника серед ворожих сил.

Заходи з введення в оману та оперативного маскування (MILDEC) – це спеціальні дії, спрямовані на навмисне дезорієнтування військового командування противника щодо його військових можливостей, намірів та операцій. Це робиться для того, щоб спонукати противника до дій, які сприятимуть досягненню поставлених цілей.

В основі MILDEC лежить розуміння процесів мислення та планування командування противника, а також способів використання ним інформаційного менеджменту для підтримки своїх зусиль.

Американські експерти проводять розмежування між поняттями дезінформації та психологічних операцій. Психологічні операції (ПсО) спрямовані на групи людей, тоді як дезінформація – на окремих осіб.

Радіоелектронна боротьба включає радіоелектронне придушення та радіоелектронний захист. Радіоелектронне придушення (РЕП) передбачає створення перешкод або ускладнення функціонування електронних пристроїв противника шляхом випромінювання та відбиття електромагнітних, звукових та інфрачервоних сигналів. РЕП здійснюється автоматизовано за допомогою наземних, морських та повітряних систем постановки перешкод.

Радіоелектронний захист охоплює заходи, що мають на меті убезпечення власних радіоелектронних засобів (РЕЗ) від ворожих перешкод, а також моніторинг функціонування РЕЗ союзників для запобігання їхньому небажаному впливу.

«Мережеві операції» охоплюють комп'ютерні атаки в мережах, захист мереж та використання комп'ютерних мереж противника для досягнення власних цілей. Комп'ютерні мережеві атаки визначаються як дії, що здійснюються в певних мережах з метою пошкодження або знищення важливої інформації на комп'ютерах і в комп'ютерних мережах, а також виведення з ладу

самих комп'ютерів супротивника. Мережевий захист включає заходи, що передбачають моніторинг і аналіз мережевих атак на комп'ютерні об'єкти Міністерства оборони США та їх захист. Безпекові операції (OPSEC) - це процес виявлення критичної інформації та подальшого аналізу дій, спрямованих на визначення даних, які можуть бути корисними для супротивника для отримання точної інформації про сили та наміри союзників; запобігання доступу супротивника до критичної інформації про сили та наміри союзників; а також спонукання супротивника недооцінювати значення відомої йому критичної інформації.

Процес планування безпекової операції включає послідовне виконання наступних етапів:

Ідентифікація критичної інформації: на початковому етапі здійснюється визначення інформаційних активів, які становлять стратегічну цінність для противника та можуть бути використані ним на шкоду операції.

Аналіз загроз: проводиться комплексне дослідження розвідувальних даних (включаючи агентурні, технічні та відкриті джерела) з метою ідентифікації потенційних суб'єктів, здатних протидіяти запланованій операції. На даному етапі здійснюється оцінка наступних аспектів:

– Суб'єкт загрози: ідентифікація осіб або організацій, що володіють наміром та ресурсами для здійснення ворожих дій проти операції.

– Цілі загроз: визначення стратегічних та тактичних цілей, які переслідує противник у контексті запланованої операції.

– Стратегія та тактика загроз: прогнозування можливих дій та методів, які може застосувати противник для досягнення своїх цілей.

– Інформованість противника: оцінка обсягу критичної інформації про операцію, яка вже відома противнику.

– Розвідувальний потенціал противника: аналіз технічних та людських можливостей противника щодо збору інформації.

Аналіз вразливостей: здійснюється детальний розгляд усіх аспектів операції з метою виявлення потенційних індикаторів, які можуть розкрити

критичну інформацію. Проводиться порівняльний аналіз виявлених індикаторів з розвідувальними можливостями противника. Індикатори визначаються як дії або інформація з відкритих джерел, які можуть бути ідентифіковані та інтерпретовані противником для отримання критично важливих даних:

– Приховані індикатори: визначення індикаторів критичної інформації, які наразі невідомі противнику, але можуть бути виявлені в процесі реалізації операції.

– Індикатори завдання шкоди: ідентифікація індикаторів, які можуть бути використані противником для завдання шкоди особовому складу та ресурсам.

Оцінка ризику: на даному етапі визначаються потенційні контрзаходи для нейтралізації кожної виявленої вразливості. На основі оцінки ризиків здійснюється селекція конкретних заходів для їхньої подальшої імплементації. Заходи операційної безпеки (OPSEC) можуть включати запобігання виявленню індикаторів противником, забезпечення альтернативної інтерпретації індикаторів та здійснення впливу на ворожі системи збору інформації.

Імплементація контрзаходів: на етапі реалізації обраних заходів безпеки здійснюється моніторинг реакції противника та оцінка ефективності впроваджених заходів.

До ключових заходів OPSEC належать диверсійні дії, камуфляж та маскування, приховування намірів, дезінформація тощо. Воєнні заходи з введення в оману (MILDEC) та операційна безпека (OPSEC) є взаємодоповнюючими концепціями. MILDEC спрямована на спонукання противника до хибного аналізу та помилкових висновків, тоді як OPSEC має на меті приховування достовірної інформації та ускладнення об'єктивної оцінки планів і намірів ініціюючої сторони.

До допоміжних елементів інформаційних операцій належать:

– Гарантування інформаційної безпеки (Information Assurance, IA):комплекс заходів, спрямованих на захист інформації та інформаційних систем шляхом забезпечення їхньої доступності, цілісності, автентичності, конфіденційності та неспростовності. Інформаційні операції використовують

ІА для захисту інфраструктури, необхідної для розміщення інформації, призначеної для впливу на цільові аудиторії.

– Фізична безпека (Physical Security): система заходів, спрямованих на захист персоналу та запобігання несанкціонованому доступу до обладнання, об'єктів, документації, а також на протидію шпигунству, саботажу, пошкодженню та крадіжкам. На відміну від ІА, що зосереджена на захисті електронних даних та інформаційних систем, фізична безпека забезпечує охорону матеріальних об'єктів, які містять цю інформацію та системи.

– Фізичні атаки (Physical Attack): застосування фізичної сили проти критично важливих інформаційних структур противника з метою порушення їхнього функціонування та зниження здатності до управління та інформаційного впливу.

– Контррозвідка (Counterintelligence): діяльність зі збору інформації та впровадження заходів, спрямованих на протидію шпигунству, розвідувальній діяльності, саботажу та терористичним актам, що можуть бути ініційовані іноземними урядами, організаціями, окремими особами або міжнародними терористичними групами.

Загалом, допоміжні елементи інформаційних операцій мають власні військові цілі, які відрізняються від безпосередніх цілей інформаційних операцій, проте вони функціонують в інформаційному середовищі або мають значний вплив на нього.

Для вирішення таких завдань, на думку А.Дудатьєва, «протиборчим сторонам потрібно мати відповідні ресурси. При цьому потрібно зауважити, що протиборчі сторони мають свої ресурси, процеси, що відбуваються в системах, внутрішні і зовнішні об’єктно-суб’єктні відносини тощо». На думку вченого, «будь яке протиборство повинно, в тому числі інформаційне, повинно забезпечуватись відповідними ресурсами, Узагальнено можна сказати, що це стан економіки, технологічний стан протиборчої сторони, рівень інформатизації суспільства тощо» [16].

В продовження аналізу концепції інформаційної переваги, який був представлений у підрозділі 2.1, на думку дисертата, слід продовжити в рамках військових операціях. Важливими є зміни в операційному середовищі або конкурентному просторі військових організацій, а також нові можливості, які впливають на нашу здатність розуміти та впливати на цей конкурентний простір. Зокрема, слід враховувати змінений характер місії (місій) в протиборстві, які можливості наших супротивників, і як вони можуть відчувати і розуміти це протиборство. Тут мова йде про оперативні концепції домінуючого маневру, точного ураження, повнорозмірного захисту та цілеспрямованої логістики, які будуть забезпечені завдяки інформаційній перевазі. Бажаним кінцевим станом є домінування повного спектру. Інформаційна перевага стосується досягнення вищої інформаційної позиції.

Інформація має такі виміри, як актуальність, точність і своєчасність. Верхня межа в інформаційній сфері досягається тоді, коли наслідки для актуальності, точності та своєчасності інформації наближаються до 100 відсотків. Бажаний ефект від наступальних інформаційних операцій полягає в тому, щоб спрямувати одну або кілька складових інформаційного «обсягу» конкурента до місця витоку. Бажаний ефект від оборонних інформаційних операцій полягає в тому, щоб утримувати наш інформаційний «обсяг» від стиснення. Очевидно, що інформаційна перевага - поняття порівняльне або відносне. Більше того, його цінність явно випливає з військових результатів, які вона може забезпечити. Ці можливості цінуються не самі по собі, а за те, що вони роблять більш ефективними тривалі наступальні та оборонні дії. Досягнення інформаційної переваги збільшує швидкість командування, випереджаючи варіанти супротивника, створює нові варіанти та підвищує ефективність обраних варіантів. Це обіцяє прискорити успішне завершення операцій за нижчими витратами. Результатом цього є здатність збільшувати темп операцій і випереджати або притуплювати ініціативи і варіанти дій супротивника.

Інформаційна перевага створюється і використовується шляхом прийняття концепцій, орієнтованих на мережу, які дозволяють організаціям досягати спільної обізнаності та самосинхронізації. Суть створення цінності в інформаційних військових операціях полягає у виявленні, ідентифікації та знешкодженні найважливіших цілей у будь-який момент часу. Найбільша проблема полягає в швидкоплинних цілях, тих, які є мобільними і цінність яких залежить від часу.

Кожна з цих змін має важливі наслідки для типів сил і засобів, які нам потрібні, а також для обмежень і стресів, які на нас покладаються. Виконання широкого спектру завдань вимагає доступу до нових організацій та інформації. Нам потрібно буде тісно співпрацювати з неурядовими організаціями та приватними добровільними організаціями, асоціаціями.. Інформаційні операції у формі кібервійни мають потенціал для повного перевизначення характеру ведення війни, розмивання меж між цивільною та військовою відповідальністю, надання нового набору озброєнь та створення нових вразливостей. Інформаційні операції – це загальний термін, який охоплює широкий спектр наступальних і оборонних дій. Наступальні інформаційні операції – це підвид цієї діяльності, який передбачає використання цифрової зброї проти цифрових цілей у будь-якій точці поля бою. Наприклад, це може бути впровадження вірусу в систему командування та управління супротивника або аналогічна атака на системи критичної інфраструктури супротивника (наприклад, електропостачання, зв'язок, громадська безпека).

Усі ці зміни мають глибокі наслідки для показників успіху, які можна використовувати для оцінки та аналізу операцій. У деяких випадках межа між війною і миром, між другом, ворогом і нейтралітетом розмивається до невпізнання. Асиметрична війна ставить перед собою унікальний набір викликів, не останнім з яких є пошук успішних стратегій стримування, виявлення і реагування. Смертоносна зброя може стати малоцінною в багатьох ситуаціях, коли політичні витрати на її використання значно перевищують її наслідки. Асиметрична війна передбачає, що кожна сторона грає за власними

правилами, які підкреслюють її сильні сторони, намагаючись використати слабкість супротивника Це дуже ускладнює розробку вказівок і попереджень, щоб попередити нас про те, хто готується до війни. Яскравим прикладом є початок повномасштабного вторгнення в Україну в 2022 році.

Якщо проаналізувати ці зміни в цілому, то стане очевидним, що наші завдання стали набагато складнішими, а наші виклики та супротивники – менш передбачуваними. Інформація, яка нам потрібна, щоб з'ясувати стосунки, стала водночас більш різноманітною та конкретною. Наші показники успіху також стали більш різноманітними і комплексними, і наш набір інструментів повинен бути значно розширений, щоб справлятися з більш складними і різноманітними ситуаціями. Ця робота є серйозним викликом, який вимагатиме від нас дещо іншого підходу до проблем і завдань.

Простір інформаційного протиборства й надалі буде визначатися простором цілей, які формуються природою інформаційної епохи. В даному випадку пропонуємо використовувати термін «простір інформаційного протиборства» замість «інформаційного простору», який більш глибокого передає відчуття, що середовище місії або змагальний простір охоплює набагато більше, ніж суцільне фізичне місце. Ризикуючи надмірним спрощенням, інформаційна епоха змінює інформаційне поле за такими основними напрямками.

Цілі завжди варіювалися від стратегічних до тактичних і включали як психологічні, так і фізичні. Набори цілей інформаційної епохи будуть розширюватися, а відносний пріоритет різних видів цілей змінюватиметься. Розширення наборів цілей зумовлене як зростанням різноманітності завдань, так і можливостями, створеними прогресом у технологіях. Характер стратегічних інформаційних операцій, безумовно, виводить деякі традиційні цілі за рамки, в той час як більший акцент робиться на інших. Використання інформаційних операцій передбачає використання нової зброї як проти традиційних, так і проти нових цілей. Наприклад, зараз в нас є можливість різноманітних кібератак на маршрутизатор зв'язку або базу даних. Вартість,

характер наслідків, летальність, побічна шкода, здатність оцінювати збитки, прихованість, а також реакція супротивника і громадськості, ймовірно, будуть відрізнятися не тільки в залежності від нашого вибору цілей, але і від того, як вони були атаковані. Це додає абсолютно новий вимір, який збільшує складність ситуації та завдання розробки відповіді.

Більше того, в той час, як інформаційна епоха робить інформацію доступною практично скрізь, майже в будь-який час і за зниженими витратами, вона не має такого ж впливу на економіку перевезень персоналу та матеріально-технічних засобів. Таким чином, це робить рух інформації набагато менш витратним, ніж рух фізичних об'єктів. Таким чином, економічна динаміка інформаційної ери стимулюватиме рішення, які залишатимуть людей і машини там, де вони є і використовуватимуть інформацію для підвищення ефективності тих, хто перебуває на театрі бойових дій, тобто для того, щоб частіше знаходити способи поставити їх у потрібне місце, а також на масові ефекти, а не на сили. Таким чином, простір інформаційного протиборства розширюється за рахунок збільшення числа та різноманітності цілей та засобів їх розповсюдження. Наприклад, інформаційні операції можуть проводитися виключно в цивільному секторі, але залучатимуся як цивільні, так і військові організації в якості учасників. Успіх в цих місіях вимагає, щоб дії військових і цивільних організацій координувалися набагато тісніше, ніж це було раніше в традиційних бойових ситуаціях. Це ставить протиборчі військові та цивільні організації в нові умови взаємодії.

Одним з найбільших викликів, з якими ми зіткнемося, буде встановлення особи та розташування наших супротивників в просторі інформаційного протиборства майбутнього. Терористи, використовуючи реальні або інформаційні бомби, можуть завдати удару практично з будь-якого місця, і межа між зовнішньою загрозою та внутрішньою стане розмитою.

Наступна характеристика простору інформаційного протиборства полягає в тому, що він більше не буде приватним або віддаленим. Війна в Україні є прикладом цього. В житлових будинках з нею боролися стільки ж, як і в

окопах. Інформаційна епоха змінила доступ до інформації. Це пов'язано з тим, що військові та органи національної безпеки більше не мають виключного контролю над інформацією в режимі реального часу. Комерційна доступність якісних зображень, пристроїв визначення місцезнаходження, доступ до величезних сховищ інформації та канали з високою пропускною здатністю забезпечують доступ до інформації, яка до цього була доступна лише наддержавам.

ЗМІ у поєднанні з Інтернетом роблять цю інформацію доступною практично будь-якій зацікавленій особі. Комерційні супутники надають зображення в режимі реального часу, які використовуються для підтримки широкого спектру завдань, включаючи прогнозування погоди, розвідку нафти та аналіз навколишнього середовища. Ці самі зображення можуть надати доступну інформацію для потенційних супротивників. Інформаційна епоха, роблячи можливим широкий збір і розповсюдження зображень в режимі реального часу. Іронія полягає в тому, що інформаційна епоха, яка, з одного боку, дає нам значно розширені можливості для збору та обробки даних, що дозволяють приймати все кращі і кращі рішення все швидше і швидше, з іншого боку, скорочує час, доступний для прийняття рішень.

Система «Дельта» є вирішальним чинником успіху ефективної *мережевоцентричної війни* українських військ в Україні. Крім того, він слугує планом для країн-членів НАТО протистояти російській агресії. Система ситуаційної обізнаності Delta («Система Delta» або «система») — це хмарна система, призначена для надання ситуаційної обізнаності в реальному часі. Створену у 2021 році військовою частиною A2724 та вдосконалену Міністерством оборони України, вони представили світові систему у жовтні 2022 року. Система Delta збирає, обробляє та відображає інформацію про пересування ворожих військ, координує сили оборони та надає інформацію про ситуацію в реальному часі. Крім того, система надає повну картину поточного бойового простору, що відображається та підсумовується на зручній цифровій карті, збираючи дані з датчиків і відкритих і секретних джерел.

Декілька західних держав реалізують провідні стандарти безпеки та стандарти НАТО в своєму хмарному дизайні. Таким чином, його оперативне використання та можливості у війні, що триває, є чудовою можливістю для союзників по НАТО перевірити його ефективність.

Система Delta не вимагає спеціальних налаштувань і готова до використання на ноутбуках, планшетах або мобільних телефонах. Його зручний дизайн дозволяє використовувати зображення, зібрані з дронів, супутників, джерел людського інтелекту (HUMINT) і датчиків. Результат проілюстровано на інтерактивній карті, яка визначає місцезнаходження ворожих сил і дає військам на землі вирішальну перевагу. Простіше кажучи, система є командно-контрольним центром у режимі реального часу, який надає українським збройним силам найсучасніші можливості в мережевому середовищі сучасної війни.

Передбачувана мета NCW полягає в тому, щоб дозволити невеликим підрозділам досягти безпрецедентної ефективності місії. Ефективність і дієвість військових операцій покращується завдяки високошвидкісному зв’язку та мережевій ситуаційній обізнаності. Система, яка об’єднує людей, які приймають рішення, ситуаційні та цілевказівні датчики, тобто джерела даних, швидко обробляє інформацію та надає її цільовому підрозділу. Крім того, менші підрозділи можуть компенсувати свою обмежену чисельність значним ступенем мобільності та адаптивності.

Розробка адекватної мережі, здатної обмінюватися інформацією в реальному часі, дозволяє децентралізоване командування. Крім того, така структура покращує здатність координувати асиметричні операції та перемогти чисельно переважаючого противника.

У березні 2021 року Україна оголосила про свою нову військову стратегію, проголошуючи важливість розширеного потенціалу NCW. Спільне використання безпілотників, супутникового зв’язку та навігаційних систем збільшило оперативну спроможність українських військових та стримування. Через рік це стане очевидним в українській стратегії ведення війни. Коли

почалося повномасштабне вторгнення в Україну на світанку 24 лютого 2022 року, світ спостерігав за тим, що, на їх думку, буде швидкою кампанією на основі попередніх оцінок російської військової стратегії. Масовані авіаудари послідували за спробами ворога проникнути на територію України на землі. Однак у північно-східних районах наступ швидко припинився. Невеликі децентралізовані підрозділи, що працювали в децентралізований спосіб, ефективно протистояли силам вторгнення. З надзвичайною гнучкістю, застосовуючи загальновійськову зброю, націлюючись на російське матеріально-технічне забезпечення, українські війська подолали російську чисельну та матеріальну перевагу. Коли Україна відтіснила російські війська на південь, а літо наближалося, умови змінилися, коли збільшилися поставки західних систем озброєння.

Комбіноване використання артилерії, засобів зв'язку, розвідки, радіоелектронної боротьби та захоплення цілей з децентралізованих командних і контрольних центрів в єдиній мережі виявилося вкрай необхідним для невдовзі південного контрнаступу наприкінці серпня. Зараз NCW є головним фактором успіху завдяки підтримці Заходом розробленої зброї та належній підготовці західних збройних сил.

На сьогодні, Україна є світовим лідером в NWC завдяки своїй важливій інформаційній обізнаності на полі бою. Здатність українських військ визначити місцезнаходження ворога, а також його чисельність і можливості є, як вважають, головною перевагою.

Оскільки система Delta забезпечує децентралізований контроль і управління, українські електронні підписи мають обмеження. Отже, російські кіберзасоби, спрямовані на закриття українських каналів зв'язку, виявилися менш успішними, ніж передбачалося спочатку. Крім того, оскільки російська армія є дуже централізованим апаратом, якому бракує синхронізації та здатності проводити широкомасштабні спільні операції в Україні, дуже гнучкі та мобільні українські сили важко знайти.

Децентралізована українська структура командування та управління, яка діє повністю незалежно від централізованого командування, функціонує через систему Delta. Однак система не функціонує сама по собі, а залежить від прийому, як будь-яка цифрова система. Джерелом і основним фактором успіху системи Delta є Starlink.

Starlink – це широкосмуговий супутниковий Інтернет, розроблений SpaceX, який робить українські сили незалежними від оптоволоконних кабелів або мобільних мереж, уразливими для нападу Росії. Наразі в Україні налічується приблизно 20 000 терміналів Starlink, більшість із яких фінансується західною підтримкою. Термінали мають вирішальне значення для здатності вести мережецентричну війну в Україні.

Важливою характеристикою Starlink є те, що його супутникова конструкція більш стійка до перешкод, ніж звичайні радіосигнали. Крім того, завдяки швидкому часу встановлення, приблизно 15 хвилин, українські сили можуть підтримувати високий рівень зв'язку, не покладаючись на інтернет-кабелі. Таким чином, доступ до апаратного забезпечення Starlink має вирішальне значення для покращення та підтримки можливостей української NCW через систему Delta. Крім того, дрони використовують Starlink, щоб підтримувати зв'язок, коли Україні не вистачає Інтернету та електроенергії через те, що російська артилерія обстрілює її критичну інфраструктуру.

Оскільки система сильно залежить від підтримки Заходу, є підстави припускати, що країни НАТО зацікавлені в її оперативній здатності протистояти російським загрозам.

Система Delta відповідає стандартам НАТО завдяки допомозі та фінансуванню західних радників у її розробці. Повідомляється, що США витратили мільйони доларів на проект і його стійкість до російської радіоелектронної боротьби. Крім того, повідомляється, що вони випробували систему під час військових навчань Sea Breeze у Чорному морі у 2021 році, продемонструвавши її адаптивність до НАТО.

За словами міністра оборони України Олексія Резнікова, зараз Україна є полігоном для випробувань західних систем озброєння. Оскільки приховування сигналів та електронні підписи стали важливими в середовищі радіоелектронної війни, для НАТО є перспективи збирати інформацію та розробляти інструменти для ефективної протидії російській радіоелектронній боротьбі та інструментам SIGINT. Оскільки світ стежить за війною в Україні, ноу-хау щодо ведення та протидії радіоелектронній боротьбі неминуче поширюватимуться. Таким чином, країни-члени НАТО, ймовірно, продовжуватимуть розвивати та підтримувати обмін інформацією з Україною для розробки інноваційних технологій.

Ймовірно, у майбутньому розширена співпраця між НАТО та Україною у сфері технологічного розвитку. Зі світом як спостерігачами мережецентрична війна в Україні привертає увагу. Хоча НАТО має значні переваги у розвитку своєї спроможності протистояти російській агресії, така здатність є надзвичайно важливою для України.

Система «Дельта» є передовою в сучасній війні та ключовим засобом ефективного ведення NCW. Система є одним із ключових факторів успіху ефективної мережецентричної війни українських військ в Україні. Крім того, він слугує планом для НАТО та його держав-членів щодо ефективної протидії російській агресії. Таким чином, це ілюструє перспективи збільшення та збереження підтримки України.

Загалом, операції, що базуються на мережевих принципах, забезпечують значну динаміку. На стратегічному рівні важливим є глибоке розуміння конкурентного середовища — всіх елементів бойового простору та часу. В оперативному плані тісні зв’язки між учасниками проявляються через взаємодію між підрозділами та операційним середовищем. Тактична швидкість є критично важливою. На структурному рівні мережево-центрична війна вимагає операційної архітектури, що складається з трьох основних елементів: мереж датчиків, мереж взаємодії та високоякісної інформаційної системи. Ці елементи підтримуються додатковими процесами командування та управління,

багато з яких повинні бути автоматизовані для досягнення необхідної швидкості.

Мережецентрична війна дозволяє перейти від виснажливого ведення бою до більш швидкого та ефективного стилю, що характеризується новими концепціями швидкості командування та самосинхронізації. Вона відзначається високими темпами змін, які суттєво впливають на результати, «блокуючи» альтернативні стратегії противника та перешкоджаючи його успіху. Це досягається двома взаємодоповнюючими шляхами: мережево-центрична війна дозволяє нашим силам розвивати швидкість командування та організовуватися знизу вгору для виконання намірів командира. Швидкість командування складається з трьох складових:

1. Сили досягають інформаційної переваги, маючи кращу обізнаність про бойовий простір, а не просто більше необроблених даних. Це вимагає технологій відображення та складних можливостей моделювання.

2. Сили, що діють швидко, точно та доступно, досягають масованих ефектів проти масованих сил.

3. Результати включають швидке обмеження дій противника та шок від тісно пов’язаних подій, що порушує стратегію ворога і дозволяє зупиняти події до їх початку.

Однією з переваг мережево-центричної війни є її здатність компенсувати недолік у кількості, технології чи позиції. Швидкість командування сприяє блокуванню з потужними наслідками, і досягти цього можна за кілька тижнів або навіть швидше.

З переходом на сучасні цифрові технології ми можемо підвищити обізнаність про бойовий простір, що дозволяє збільшити бойову міць і знищити більше цілей. Якщо ми впровадимо нові системи, такі як ATACMS, для атаки на сайти ППО, це дозволить знищити практично всі цілі. Висока швидкість змін на початку військових дій є критично важливою, оскільки вона може зупинити війни — це суть мережево-орієнтованої війни.

Військові операції є надзвичайно складними, і теорія складності вказує на те, що такі процеси найкраще організовуються знизу вгору. Проте традиційно військові командири прагнуть досягти низхідної синхронізації для забезпечення необхідного рівня маси та вогню в точці контакту з противником. Оскільки кожен елемент сил має свій унікальний ритм, помилки можуть зменшити бойову міць, що призводить до затримок у бойових діях.

Організація «знизу вгору» забезпечує самосинхронізацію, де крокова функція стає плавною, а бій переходить у високошвидкісний континуум. Зв’язка «Спостереження-Орієнтація-Рішення-Дії» (OODA) зникає, і противник опиняється в оперативній паузі.

Відновлення цього часу та бойової потужності посилює ефект швидкості командування, прискорюючи швидкість змін і призводячи до блокування.

Слід зазначити, що в платформоцентричних військових операціях ситуаційна обізнаність постійно погіршується. Вона періодично відновлюється, але потім знову погіршується. Операції, орієнтовані на мережу створюють вищу обізнаність і дозволяють її підтримувати. Таке усвідомлення покращує здатність стримувати конфлікт або перемагати, якщо конфлікт стає неминучим. Це не просто питання впровадження нових технологій; це питання спільної еволюції цієї технології з операційними концепціями, доктриною та організацією.

Виникла нова структурна або логічна модель мережево-центричної війни. Це потужна інформаційна мережа, яка слугує основою для обчислень і комунікацій. Інформаційна мережа забезпечує робочі архітектури сенсорних і залучаючих мереж. Сенсорні мережі швидко формують високий рівень обізнаності про бойовий простір і синхронізують цю обізнаність із військовими операціями. Мережі взаємодії використовують цю інформацію для підвищення бойової потужності. Багато ключових елементів цих мереж вже реалізовані або доступні. Наприклад, на етапі планування з'являються елементи внутрішньої мережі Міністерства оборони. Для забезпечення взаємодії всі елементи мереж повинні відповідати спільному робочому середовищу Спільної технічної

архітектури та оборонної інформаційної інфраструктури. Проте їх повна інтеграція в більш потужну екосистему бойових дій залишається частково завершеною. Це не лише теоретичні міркування, а реальні події, які відбуваються сьогодні. Наприклад, нові класи загроз вимагали підвищення оборонної бойової потужності об'єднаних сил. Бойова потужність, що виникла, — це спроможність спільного залучення, яка стала можливою завдяки переходу до мережево-центричних операцій. Вона поєднує в собі високоефективну сенсорну мережу з потужною мережею залучення. Сенсорна мережа швидко генерує інформацію про якість ураження, а мережа ураження перетворює цю інформацію на підвищення бойової потужності. Ця потужність проявляється у високій ймовірності зіткнень із загрозами, здатними подолати захист, орієнтований на платформу. Сенсорна мережа CEC об'єднує дані з кількох датчиків, щоб створити комбінований трек з якістю взаємодії, забезпечуючи рівень усвідомлення бойового простору, який перевищує будь-який рівень, досягнутий за допомогою автономних датчиків.

Отже, першим кроком нового комісара стала зміна доктрини, спрямована на боротьбу з ефектом «розбитих вікон», що стверджує, що в суспільстві існує негативний зворотний зв'язок між дрібними та серйозними злочинами. Це означає, що якщо ми вирішимо діяти на мережевій, а не на платформоцентричній основі, нам потрібно змінити підходи до навчання, організації та розподілу ресурсів. Наприклад, наш військово-морський флот, як і всі інші служби, повинен приймати ці стратегічні рішення для максимізації майбутньої бойової потужності та актуальності. Оскільки мережево-центрична сила функціонує за іншим, більш сучасним набором правил, ніж платформа-центрична, нам потрібно зробити фундаментальний вибір принаймні в трьох сферах: інтелектуальний капітал, фінансовий капітал і процеси.

Концепції мережево-орієнтованих операцій, змін конкурентних просторів, змін базових наборів правил і спільної еволюції — це не просто теорія. Вони застосовуються в складних умовах з позитивними результатами. Так само ці концепції не обмежуються кількома оптимальними обставинами. Мережево-

центрична війна отримує свою силу завдяки міцній мережі добре поінформованих, але географічно розосереджених сил. Сприйнятливими елементами є високопродуктивна інформаційна сітка, доступ до всіх відповідних джерел інформації, охоплення зброєю та маневрування з точністю та швидкістю реагування, додаткові процеси командування та управління (С2), включаючи високошвидкісне автоматизоване призначення необхідні ресурси та інтегровані сенсорні сітки, тісно пов’язані в часі зі стрільцями та процесами С2. Мережецентрична війна застосовна до всіх рівнів війни та сприяє об’єднанню стратегії, операцій і тактики. Це прозоро для місії, розміру та складу сил, а також географії.

Швидкість командування – це не просто швидкість передачі наказів, а динамічний процес перетворення інформаційної переваги на вирішальну конкурентну перевагу. Його сутність полягає у здатності оперативно та ефективно використовувати краще розуміння ситуації для радикальної зміни початкових умов на свою користь. Це досягається шляхом підтримання високого темпу змін, нав'язування противнику власного ритму дій та одночасного блокування його спроб застосувати альтернативні стратегії. Швидкість командування не розглядає окремі елементи бойової обстановки ізольовано, а сприймає їх як взаємопов'язані частини складної, гнучкої екосистеми. Його вплив є глибоким та системним, оскільки він діє через резонанс між тісно пов'язаними подіями, викликаючи каскадний ефект, що руйнує плани противника.

Іншими словами, швидкість командування – це інтелектуальна та операційна перевага, що дозволяє не просто реагувати на події, а проактивно формувати їх, створюючи для противника ситуацію постійного відставання та неможливості адаптації. Це вміння бачити поле бою як живу систему, де кожен елемент впливає на інший, і використовувати цю взаємозалежність для досягнення стратегічного успіху шляхом темпорального домінування.

Самосинхронізація, на противагу традиційній вертикальній ієрархії управління, являє собою якісно новий спосіб організації та координації

складних бойових дій, що виникає "знизу вгору". Її фундаментом є високий рівень обізнаності особового складу щодо власних сил, сил противника та всіх ключових аспектів оперативного середовища. Організаційними принципами, що забезпечують її ефективність, є спільне розуміння мети (єдність зусиль), чітко доведені до кожного виконавця наміри командувача та гнучкі, але зрозумілі правила ведення бою. Самосинхронізація нівелює втрату бойової потужності, неминучу при централізованому, ієрархічному управлінні, де час витрачається на передачу наказів по вертикалі. Вона трансформує бій з послідовності етапів у високоінтенсивний, безперервний процес, де ініціатива та узгодженість дій досягаються за рахунок внутрішньої злагодженості добре поінформованих та мотивованих підрозділів.

Суть самосинхронізації полягає в тому, що кожен елемент бойової системи, володіючи повною картиною поля бою та розуміючи загальну мету, здатен самостійно приймати рішення та координувати свої дії з іншими елементами без детальних вказівок згори. Це перетворює бойову силу з жорстко структурованої машини на живу, адаптивну мережу, здатну до швидкої самоорганізації та ефективної протидії непередбачуваним обставинам, значно підвищуючи темп і непередбачуваність бойових дій.

Аналіз дозволяє сформулювати наступні науково обґрунтовані висновки щодо еволюції простору інформаційного протиборства та концептуалізації мережевоцентричної війни (NCW), верифікованої емпіричним досвідом російсько-українського конфлікту.

Щодо інформаційної зброї та інформаційної війни:

- Детермінантність суспільного контролю та етичних імперативів: В умовах демократичного політичного режиму суспільний контроль виступає ключовим детермінантом легітимності вибору засобів збройної боротьби, зокрема інформаційної зброї. Обґрунтованість застосування останньої корелюється зі збалансованістю морально-етичних та технологічних аспектів намірів суб'єкта. Ігнорування етичних норм призводить до ерозії суспільної

підтримки та зниження операційної ефективності технологічних рішень, потенційно нівелюючи бойовий потенціал збройних сил.

- Парадигмальна значущість та відносна доступність інформаційної зброї: Інформаційна зброя є значущим та відносно економічно доступним інструментом стратегічного впливу, що зумовлює необхідність розробки комплексних заходів захисту як для військового, так і для цивільного секторів. Ухвалення політичних рішень щодо її розробки та застосування потребує глибокої інтроспекції щодо морально-етичних ризиків та проведення всебічного міждисциплінарного аналізу. Пріоритетним є також гносеологічне розуміння принципів функціонування та теоретичних засад застосування інформаційної зброї перед її оперативним використанням.
- Телеологічна спрямованість інформаційних операцій: Основною метою інформаційних операцій є цілеспрямований вплив на інформаційні системи супротивника, що охоплюють його когнітивні структури (знання, гіпотези) та процеси прийняття рішень. Операціональним результатом успішних інформаційних атак є індукція у супротивника стану, що спонукає до припинення бойових дій, зумовленого втратою оперативного контролю, деморалізацією особового складу або усвідомленням стратегічної безперспективності подальшої ескалації конфлікту.
- Діалектична еволюція інформаційних систем та методів протиборства: Інформаційні системи демонструють тенденцію до ускладнення, що є наслідком прогресу суспільних інститутів та інформаційно-комунікаційних технологій. Сучасні парадигми збройної боротьби інтегрують складні психологічні операції, спрямовані не лише на деструкцію, але й на відновлення функціональності систем управління.
- Концептуальна диференціація збройного протистояння та війни: Поняття збройного протистояння є ширшим за дефініцію війни, маючи на меті примушення супротивника до певних дій, що не обов'язково передбачає його фізичне знищення. Кульмінацією майстерності в даному контексті є досягнення підкорення волі опонента.

- Операціональна сутність інформаційної війни: Інформаційна війна є специфічною формою конфлікту, що характеризується прямими атаками на інформаційну інфраструктуру супротивника з метою впливу на його когнітивні моделі та базові припущення. Вона може здійснюватися як проти зовнішніх, так і проти внутрішніх акторів. Кінцевою метою є використання інформаційних засобів для маніпулювання системами знань та аксіоматичними передумовами ворожої сторони.
- Векторність інформаційних атак: Інформаційні атаки повинні бути націлені як на верифіковані системи знань (науково обґрунтовані), так і на суб'єктивні системи припущень (індивідуальні, включаючи ірраціональні компоненти) супротивника, з особливим акцентом на його лідерському складі та особах, що приймають стратегічно важливі рішення, які є потенційно вразливим елементом ієрархічних структур управління.
- Стратегічна та операційна інтенціональність інформаційної війни: Стратегічна мета інформаційної війни полягає у здійсненні латентного впливу на процес прийняття рішень противником таким чином, щоб його подальші дії суперечили його декларованим намірам. Оперативна мета передбачає інтервенцію в когнітивні процеси супротивника, ускладнюючи координацію та ефективність його дій.
- Епістемологічні та методологічні вимоги до планування інформаційних кампаній: Ефективне планування інформаційних кампаній на стратегічному та оперативному рівнях вимагає артикуляції відповідей на низку ключових питань, що стосуються кореляції з глобальними цілями, бажаного гносеологічного статусу противника, інструментарію досягнення цього стану, встановлення лімітів щодо цілей та засобів атаки, оцінки досяжності бажаного результату та архітектури управління кампанією.
- Залежність вразливості від інформаційної інтеграції: Ступінь вразливості суб'єкта до інформаційної війни прямо пропорційно залежить від рівня його залежності від інформаційних систем у процесі прийняття рішень. Високотехнологічні держави демонструють широкий спектр потенційних цілей,

однак і доіндустріальні суспільства є вразливими через специфіку їхніх гносеологічних систем. Демократичні держави виявляють особливу вразливість щодо свого економічного апарату управління.

- Плюралізм сфер застосування інформаційної зброї: Сфера застосування інформаційної зброї є мультидисциплінарною та охоплює як мілітарний, так і цивільний домени, з метою дезорганізації систем управління, критичної інфраструктури, фінансової діяльності, ініціювання соціальних криз та здійснення масованого впливу на суспільну свідомість.
- Концептуальна дистинкція інформаційної, психологічної та кібернетичної воєн: Існує чітке розмежування між інформаційною, психологічною та кібернетичною війнами, кожна з яких характеризується власною сутністю, методологією та стратегічними цілями. Інформаційна війна фокусується на управлінні інформаційними потоками.
- Закономірності ефективного ведення інформаційної війни: Ефективне ведення інформаційної війни ґрунтується на низці детермінант, включаючи залежність від політичних цілей, економічних, соціально-політичних, науково-технічних та військових можливостей суб'єкта.
- Атрибутивні характеристики інформаційної зброї: Інформаційна зброя характеризується латентністю застосування, масштабністю потенційного впливу, універсальністю щодо цілей та за своєю деструктивною силою може бути порівняна зі зброєю масового ураження, завдаючи значних збитків через вплив на системи управління та психоемоційний стан індивідів.

Щодо еволюції простору інформаційного протиборства та мережевоцентричної війни (NCW):

- Трансформація інформаційного простору в публічну та всеосяжну арену: Простір інформаційного протиборства зазнав якісної трансформації, набувши публічного та глобального характеру, втративши ознаки приватності та географічної віддаленості. Емпіричний досвід російсько-українського конфлікту підтверджує, що бойові дії розгортаються не лише в традиційній військовій сфері, але й у цивільному інформаційному просторі.

- Демократизація доступу до інформації та ерозія монополії національної безпеки: Інформаційна епоха спричинила кардинальні зміни у парадигмі доступу до інформації, девальвуючи монополію військових та органів національної безпеки на володіння інформацією в режимі реального часу. Комерційна доступність передових технологій (високоякісна аерокосмічна зйомка, геопросторова локалізація, аналіз великих даних, високошвидкісні канали передачі даних) надає інформацію, раніше доступну лише наддержавним акторам, широкому спектру суб'єктів.
- Роль засобів масової інформації та глобальної мережі Інтернет: Засоби масової інформації та мережа Інтернет забезпечують практично миттєву дисемінацію інформації для глобальної аудиторії. Комерційні супутникові знімки в реальному часі є показовим прикладом інформації подвійного призначення, потенційно використовуваної противниками.
- Темпоральна компресія процесів прийняття рішень: Інформаційна епоха, одночасно розширюючи аналітичні можливості через збір та обробку великих обсягів даних, парадоксально скорочує часові рамки, доступні для прийняття обґрунтованих рішень.
- Система ситуаційної обізнаності "Дельта" як ключовий елемент NCW: Інтегрована система ситуаційної обізнаності "Дельта" виступає критично важливим фактором операційного успіху українських збройних сил у контексті мережевоцентричної війни проти російської агресії. Дана хмарна платформа забезпечує агрегацію, обробку та візуалізацію розвідувальних даних про противника в режимі реального часу, здійснює координацію сил та засобів, а також забезпечує формування цілісної картини бойового простору на цифровій основі.
- Операційна сумісність та інтеграційний потенціал системи "Дельта": Система «Дельта» відповідає стандартам безпеки Організації Північноатлантичного договору (НАТО) та є цінним інструментом для країн-членів Альянсу з метою вивчення її ефективності в реальних бойових умовах. Її інтуїтивно зрозумілий інтерфейс, доступність на різних типах кінцевих

пристроїв та здатність інтегрувати дані з різнорідних джерел (безпілотні літальні апарати, супутникові системи розвідки, агентурні джерела, сенсорні мережі) забезпечує українським військам значну інформаційну перевагу.

- Концептуальні засади мережевоцентричної війни (NCW): Мережевоцентрична війна (NCW) являє собою операційну концепцію, що передбачає інтеграцію особового складу, систем підтримки прийняття рішень, сенсорних платформ та вогневих засобів через високошвидкісні комунікаційні мережі з метою досягнення спільного інформаційного простору та підвищення синергії бойових операцій. NCW надає можливість невеликим, децентралізованим підрозділам досягати безпрецедентної операційної ефективності завдяки розподіленому управлінню, високій мобільності та адаптивності до динамічних змін обстановки.
- Проактивне впровадження Україною стратегії NCW: Україна розпочала імплементацію стратегічних принципів NCW ще до початку повномасштабної військової агресії, що знайшло відображення в її тактичних підходах до ведення бойових дій. Невеликі, автономні підрозділи продемонстрували високу ефективність у протистоянні чисельно переважаючим силам противника, використовуючи гнучкість маневру та зосереджуючи зусилля на порушенні логістичних ланцюгів ворога.
- Синергія вогневих засобів, розвідки та управління в рамках NCW: Комбіноване застосування артилерійських систем, засобів зв'язку, розвідувальних платформ, систем радіоелектронної боротьби та засобів цілевказівки в рамках єдиної інформаційної мережі з децентралізованих командних центрів є критично важливим фактором успіху контрнаступальних операцій українських військ.
- Україна як лідер у сфері мережевоцентричної війни: На поточний момент Україна посідає провідні позиції у світі в галузі NCW завдяки досягнутому рівню інформаційної обізнаності на полі бою. Здатність оперативно визначати географічне положення, чисельність та операційні можливості противника є ключовою конкурентною перевагою.

- Стійкість децентралізованої системи управління до кібернетичних загроз: Децентралізована архітектура системи командування та управління Збройних Сил України, що функціонує на базі платформи «Дельта», знижує її вразливість до кібератак, спрямованих на порушення критично важливих каналів зв'язку. Централізована модель управління російської армії демонструє обмежену ефективність у протидії гнучким та мобільним українським підрозділам.
- Критична залежність NCW від супутникового інтернет-зв'язку Starlink: Функціональна стійкість системи «Дельта» критично залежить від надійного супутникового інтернет-зв'язку Starlink, що забезпечує незалежність від потенційно вразливих наземних комунікаційних мереж. Значна кількість терміналів Starlink, розгорнутих на території України, значна частина яких фінансується західними партнерами, є ключовим елементом підтримки концепції NCW.
- Технічні переваги та оперативна гнучкість системи Starlink: Конструктивні особливості супутників Starlink забезпечують підвищену стійкість до радіоелектронних перешкод, а висока швидкість розгортання термінального обладнання дозволяє українським силам підтримувати стабільний та високоефективний зв'язок. Starlink також використовується для забезпечення комунікації безпілотних літальних апаратів в умовах відсутності традиційної інтернет-інфраструктури та стаціонарного електропостачання.
- Стратегічний інтерес та підтримка західних союзників: Країни Заходу, зокрема держави-члени НАТО, виявляють значний інтерес до операційної спроможності системи «Дельта» у контексті протидії російським загрозам та надають активну підтримку її подальшому розвитку. Результати випробувань системи під час спільних навчань НАТО підтверджують її адаптивність та ефективність.
- Україна як полігон для тестування західних військових технологій: Україна фактично стала полігоном для випробувань новітніх західних систем озброєння, а набутий досвід ведення та протидії радіоелектронній боротьбі має значну цінність для країн НАТО. Очікується подальша інтенсифікація співпраці

між Україною та країнами-членами НАТО у сфері технологічного розвитку військової сфери.

- Динаміка NCW на різних рівнях військової діяльності: Мережевоцентрична війна забезпечує значну операційну динаміку на всіх рівнях військової діяльності – стратегічному, оперативному та тактичному, вимагаючи відповідної операційної архітектури, що включає інтегровані мережі сенсорів, мережі взаємодії та високопродуктивну інформаційну систему, підтримувану автоматизованими процесами командування та управління.
- Трансформація характеру бойових дій під впливом NCW: NCW надає можливість переходу від виснажливих бойових зіткнень до більш динамічного та ефективного стилю ведення війни, що характеризується високою швидкістю прийняття рішень та самосинхронізацією дій підрозділів. Це дозволяє оперативно «блокувати» стратегічні ініціативи противника та швидко досягати якісних змін початкових оперативно-тактичних умов.
- Детермінанти швидкості командування в NCW: Висока швидкість командування досягається завдяки інформаційній перевазі (глибоке розуміння ситуації), здатності швидко та точно завдавати концентрованих ударів та оперативно обмежувати маневр противника.
- Механізми самосинхронізації в NCW: Самосинхронізація, що забезпечується децентралізованою організацією управління («знизу вгору») та високим рівнем ситуаційної обізнаності особового складу, дозволяє силам координувати складні бойові дії без жорсткої централізованої синхронізації, трансформуючи бойове зіткнення у високодинамічний безперервний процес.
- Організаційно-технологічні імперативи переходу до NCW: Перехід до парадигми NCW вимагає фундаментальних змін у підходах до підготовки особового складу, організаційної структури та розподілу ресурсів, а також інтеграції новітніх технологій з існуючими операційними концепціями, військовою доктриною та організаційними штатами.
- Практична реалізація концепцій NCW: Концептуальні засади мережевоцентричної війни є не лише теоретичними конструкціями, але й

практично застосовуються в складних бойових умовах, забезпечуючи відчутну перевагу завдяки розгалуженій мережі добре поінформованих та географічно розподілених сил, що підтримуються ефективною інформаційною інфраструктурою та оптимізованими процесами командування та управління (C2).

- Ключові операційні переваги NCW: Швидкість командування та самосинхронізація виступають ключовими операційними елементами NCW, що дозволяють трансформувати інформаційну перевагу в стійку конкурентну перевагу та досягати рішучих результатів у бойових діях.
- Емпіричне підтвердження ефективності NCW досвідом України: Досвід російсько-українського конфлікту є показовим прикладом практичної ефективності мережевоцентричної війни в умовах сучасного високоінтенсивного конфлікту, демонструючи її значні переваги над більш традиційними, платформоцентричними підходами до ведення бойових дій.

Підсумовуючи, даний розділ закладає теоретико-методологічне підґрунтя для розуміння інформаційних операцій як інтегрального елементу сучасної збройної боротьби, акцентуючи увагу на їхній багатовимірності, операційній складності та імперативності врахування етичних аспектів, особливо в контексті демократичного цивільно-військового контролю. Емпіричний аналіз досвіду України впровадження концепції мережевоцентричної війни підтверджує її значний потенціал у забезпеченні операційної переваги в умовах динамічного та інформаційно насиченого поля бою.

2.3. Конфронтація взаємодії суб'єктів політики в інформаційному просторі.

Політична ситуація у світі характеризується посиленням негативних процесів у сфері глобальної та регіональної безпеки, викликаних як геополітичним суперництвом між провідними світовими державами, так і

зіткненням інтересів окремих держав (коаліцій держав). На його стан і розвиток впливає сукупність негативних факторів, які впливають на умови виконання завдань безпеки і оборони. Серед них слід зазначити:

– спроби змінити цінності та моделі розвитку, дискредитувати культури, релігії та цивілізації, фальсифікування історії;

– застосування військової сили у військових конфліктах у поєднанні з політичною, фінансово-економічною, інформаційною та іншими формами боротьби.

Виявлення факторів негативного характеру свідчить про трансформацію міждержавних відносин та військового насильства, в яких інформаційна складова є обов'язковою на всіх етапах розвитку конфліктної ситуації та її вирішення. Руйнівний інформаційно-психологічний вплив на особистість, суспільство і державу постійно вдосконалюється, розробляються нові механізми маніпулювання індивідуальною і масовою свідомістю. Не випадково інформація сьогодні має властивості зброї, а результати її застосування часто можна порівняти з результатами військових Конфлікти.

В даний час фахівці активно використовують термін «інформаційна зброя», під яким я розумію сукупність інформаційних засобів, технологій і речовин, а також спеціальних методів (способів) прихованого (по можливості) насильницького впливу на інформаційно-технічні та інформаційно-психологічні об'єкти противника (протиборчої сторони) з метою досягнення поставлених цілей і вирішення завдань інформаційної війни.

Технології інформаційних війн, засновані на маніпулятивному контролі за політичною свідомістю та поведінкою громадян, є надзвичайно небезпечними і ніколи не спрямовані на створення: їхнє головне завдання – розколоти суспільство, яке буде складатися з фрагментів, ініціюючи боротьбу за руйнування, або об'єднати їх агресію в єдиний потік і направити її проти умовного ворога чи влади.

В інформаційній війні основним об'єктом впливу є суспільна та індивідуальна свідомість і підсвідомість населення і військовослужбовців.

Метою впливу є підміна справжніх національних цінностей і національних інтересів. Основним засобом впливу на свідомість людей є інформаційна зброя. Вона відрізняється від інших видів зброї своєю універсальністю, секретністю, раптовістю, економічною ефективністю, можливістю її використання для вирішення широкого кола завдань, її масштабом, ефектом ланцюгової реакції, складністю міжнародного контролю за її розробкою та використанням. Через інформаційний простір цілеспрямовано дискредитуються конституційні засади держав та їх владних структур, розмивається національна ментальність та ідентичність, залучаються люди до екстремістської та терористичної діяльності, розпалювання міжнаціональної та міжконфесійної ворожнечі, формування радикального та протестного потенціалу.

Інформаційний фактор відіграє все більш значну роль у міждержавних конфліктах і неявних діях, спрямованих на порушення суверенітету і територіальної цілісності країн і зниження темпів їх розвитку. Військове насильство та його крайня форма – війна, не змінюючи своєї суті, що міститься в політиці, постійно змінюють свій зміст, використовуючи різні інструменти впливу на ворога на основі військової сили. Серед загальних рис сучасних військових конфліктів обґрунтовано виділяють вплив цих конфліктів на всі сфери людського життя та визначальне значення інформаційної сфери у протистоянні на всіх етапах розвитку військового конфлікту і після закінчення його активної фази.

Інформаційне протиборство включає в себе дві складові: інформаційно-технічну та інформаційно-психологічну. Вона проводиться між державами не тільки у воєнний, а й у мирний час, відкрито і приховано на захист власних інтересів, за зони політичного впливу, ринки, спірну територію, зміцнення оборонної сфери. Зрозуміло, що втручаючись в регулювання інформаційних потоків, впливаючи на хід їх обробки і управління, можна впливати на ті чи інші події і процеси. Це одна з причин запеклої боротьби за контроль над засобами масової інформації, а значить і за контроль над свідомістю населення країни

В рамках інформаційно-психологічного протистояння з використанням засобів інформаційно-психологічного впливу на психіку (свідомість, підсвідомість) інформаційних об'єктів (людей, соціальних груп, осіб, що приймають рішення)) протилежної сторони вирішується завдання їх пізнавального придушення і (або) підпорядкування, а по відношенню до об'єктів їх боку - їх інформаційно-психологічного захисту від засобів інформаційно-психологічного впливу. В основу цього процесу покладено концептуальні положення філософії війни (психологія впливу, маніпулювання суспільною свідомістю, комунікації тощо.

Так, після закінчення «холодної війни», на початку 1990-х років, керівництво США почало активніше працювати над проблемами протистояння в інформаційній сфері, або так званої інформаційної війни. Після операції "Буря в пустелі" (1991) США прийшли до висновку, що зміст війни докорінно змінився, що переможе та сторона, яка перемогла в інформаційній кампанії. Таким чином, інформація є своєрідним ключем до сучасної війни в стратегічному, оперативному, тактичному і технічному плані.

Відповідно до поглядів стратегів США на війну майбутнього, головною складовою суттєвого підвищення бойових спроможностей Збройних Сил є досягнення інформаційної та технологічної переваги. Домінуючими видами військових операцій у новому військовому вимірі, поряд із традиційними, будуть інформаційні операції, що проводяться як самостійно, так і спільно з іншими видами військових операцій. Зміна ролі та значення інформаційного впливу актуалізує проблему інформаційної безпеки як найважливішої складової національної безпеки. Згідно з Концепцією, під інформаційною безпекою розуміється стан захищеності збалансованих інтересів особистості, суспільства та держави від внутрішніх і зовнішніх загроз, що виникають в інформаційній сфері.

Варто погодитись, що метою забезпечення таких операцій є досягнення і підтримання такого рівня безпеки інформаційної сфери, який забезпечує реалізацію національних інтересів України та її прогресивний розвиток. Тобто,

об'єктом інформаційного протиборства може бути будь-який об'єкт, по відношенню до якого можна проводити інформаційні операції, результатом чого буде модифікація його властивостей як інформаційної системи (інформаційних засобів)» [57].

Загальною ознакою об'єкта, який можна розглядати як об'єкт, є використання будь-якого інформаційного впливу для порушення його функціонування. Об'єктами небезпечного впливу, а отже, і об'єктами інформаційного протиборства, можуть бути:

• психіка (свідомість, підсвідомість) індивідів і їх спільнот (соціальні об'єкти ІЛ: індивідуальний, колективний, суспільство, держава, світова спільнота);

• інформаційно-технічні системи різного масштабу і призначення.

Основними об'єктами підтримки інформаційної безпеки у військовій сфері є:

• інформаційна інфраструктура органів військового командування та управління всіх рівнів Збройних Сил та наукових установ Міністерства оборони;

• інформаційний ресурс оборонних підприємств та науково-дослідних установ, які виконують державні оборонні замовлення;

• програмно-технічні засоби автоматизованих і автоматичних систем управління військами та озброєнням, озброєнням і військовою технікою;

• інформаційний ресурс інших військ і військових формувань і органів.

У відношенні до суспільства об'єктами інформаційної безпеки є:

• система соціальних відносин суспільства;

• система політичних відносин суспільства;

• система психологічних відносин суспільства.

Об'єктом інформаційної безпеки може стати будь-яка складова або сегмент інформаційної сфери, а саме:

• масова та індивідуальна свідомість громадян;

• суспільно-політичні системи і процеси;

• інформаційно-психологічні ресурси.

Під психологічним ресурсом розуміють сукупність наступних складових інформаційної сфери:

• система цінностей суспільства (стійкість системи цінностей по відношенню до зовнішніх або внутрішніх деструктивних впливів);

• індивідуальна та масова свідомість громадян (опір свідомості громадян маніпулятивному впливу та залучення їх до протиправної діяльності);

• психічне здоров'я громадян (стійкість психічного здоров'я по відношенню до зовнішніх або внутрішніх деструктивних впливів).

Суб'єктами інформаційної безпеки є: держави, їх союзи і коаліції; міжнародні та неурядові організації; недержавні незаконні (у тому числі міжнародні) збройні формування та організації терористичної, екстремістської, радикальної політичної, радикальної релігійної спрямованості; транснаціональні корпорації; медіа-корпорації (контролюють засоби масової інформації та засоби масової комунікації).

В такому процесі для держави характерні такі ознаки: має стійкі (постійні) інтереси в інформаційній сфері; формує і контролює національний (союзний) інформаційний простір, який, як правило, так чи інакше інтегрований у світовий інформаційний простір і є його сегментом; створює спеціальні сили як у силовому блоці, так і в цивільних державних установах, в обов'язки яких входить політична поведінка; при наявності необхідного науково-технічного потенціалу розробляє і апробує засоби інформаційного впливу, а також принципи і методи їх застосування; розробляє і закріплює на офіційному рівні, в тому числі у вигляді нормативних актів, концептуальних та ідеологічних положень, що обґрунтовують необхідність його участі в таких процесах, а також основні принципи і форми участі в ньому для даного предмета.

До принципів забезпечення інформаційної безпеки належать: законність, правова безпека, баланс інтересів особистості, суспільства і держави, комплексність і послідовність, науковість і об'єктивність, інтеграція з міжнародними системами безпеки, економічна ефективність.

Слід ще раз підкреслити, що «інформаційна сфера є одним з визначальних чинників суспільного розвитку і забезпечення безпеки держави, а сучасне суперництво в ній все частіше набуває форми безкомпромісної боротьби. Метою є досягнення інформаційної переваги шляхом забезпечення необхідного ступеня власної інформаційної безпеки та зниження рівня безпеки протилежної сторони до величини, що забезпечує досягнення поставлених цілей (у тому числі військових цілей)» [26].

Принцип не тільки відображає об'єктивний зв'язок, а й спрямований на те, наскільки раціонально слід діяти в конкретних умовах для досягнення тієї чи іншої мети. Основоположний принцип - відповідність (підпорядкування) цілей і завдань інформаційної боротьби політичним цілям - випливає із закону про визначальну роль політики, її вирішальний вплив. Він відображає об'єктивний закон нерівномірного розподілу сил у просторі та часі. Важливе значення має також принцип завчасної всебічної підготовки сил окремої робочої сили. Вона випливає із загальних законів війни та відображає природну залежність процесу та результату боротьби від співвідношення матеріальних, духовних і бойових можливостей протиборчих сторін.

Економіка є матеріальною основою для інформатизації суспільства і держави, а, отже, і для успішного ведення індивідуальних підприємців, як в мирний, так і у воєнний час. Таким чином, сучасний етап розвитку суспільства характеризується все зростаючою роллю інформаційної сфери у всіх сферах людської діяльності. Метою деструктивних інформаційних дій є не руйнування протилежної сторони, а рефлекторний контроль над нею в інтересах безумовного підпорядкування волі агресора. Для цього потрібне розуміння сутності, сценаріїв інформаційних війн, психологічних операцій, IP технологій, шляхів забезпечення інформаційної безпеки особистості, суспільства та держави. Такий напрям міждержавного протистояння потребує підготовки фахівців для його проведення та забезпечення інформаційної безпеки країни.

Крім того, найважливішим чинником запобігання маніпулюванню індивідуальною та суспільною свідомістю в деструктивних цілях є високий

рівень загальної, гуманітарної та інформаційної культури особистості та суспільства в цілому. Тому рівень культури та освіченості особистості стає своєрідним імунітетом від сприйняття недостовірної інформації та психологічних маніпуляцій. Управління інформаційними ресурсами є вирішальним фактором завоювання, збереження та утримання влади. Ефективність роботи всіх підсистем національної безпеки держави залежить від знання законів їх функціонування та раціонального управління інформаційними ресурсами. Це особливо важливо для військової сфери національної безпеки, оскільки в сучасному світі інформація та вміле маніпулювання нею є зброєю масового ураження навіть без ведення класичної війни.

Варто погодитись, що «в сучасному протистоянні між політичними силами зростає важливість кіберпростору, що впливає на військову справу та змінює спосіб спілкування людей в інтернеті. Через розвиток подій змінюються структура та зміст взаємодії на полі бою. Оскільки конфлікти в кіберпросторі є відносно новим явищем, повне розуміння їхніх сучасних аспектів ще формується. Експерти називають протистояння в кіберпросторі прохолодними війнами, підкреслюючи використання інформаційних технологій. Ці конфронтаційні процеси відображають нову динаміку відносин між державами після закінчення холодної війни. Держави уникають відкритого насильства, але змушені діяти більш стримано, ніж у звичайних політичних конфліктах, що робить ці протистояння не холодними і не гарячими, а прохолодними. Нові можливості інформаційного простору призвели до зміни структури, змісту та розташування взаємодій між сторонами конфлікту на полі бою» [57].

Цілком варто погодитись, що наразі «найбільш популярний один метод кіберзлочинства, а саме – відмова в обслуговуванні (DDoS), яка впливає на динаміку конфлікту та співпрацю між державами. Ефект – це погіршення відносин як інструмент зовнішньої політики. Політична конфронтація крізь призму міжнародних відносин є суттєвою складовою сучасних відносин. Політичні протиріччя між державами спрямовані на вирішення питань у сфері зовнішньої політики. Такими питаннями можуть бути аспекти щодо етносів їх

статусу, територій та ідентифікації груп населення, які активно обговорюються на розвиваються через інформаційний простір» [57].

Питання про те, як держави та недержавні організації застосовують кібероперації разом з іншими способами впливу, порушує важливі питання щодо інструментів досягнення стратегічної переваги в майбутніх конфліктах. Ці важливі питання залишаються без наукового чи політичного порозуміння. Частково це пов'язано з тим, що основні технології є новими, постійно розвиваються і часто не є публічними, що ускладнює їхнє розуміння. Через це дослідники часто використовують концепції з минулих епох, наприклад, стратегічне ядерне стримування, для аналізу кібероперацій, хоча такий підхід має суттєві обмеження. Інформаційне протистояння значно відрізняється від звичайних військових дій: воно не передбачає прямого застосування сили, не завдає руйнувань у традиційному розумінні (принаймні поки що) і часто важко приписати конкретним виконавцям.

Ще більше плутанини викликає те, що програмісти та інженери, які знають технології, як правило розуміють науку, але не політику, тоді як політики розуміють політику, але практично не звертаються до науки. Ці виклики ускладнюють пошук кваліфікованих експертів або адекватну підготовку служби безпеки фахівців в інформаційному просторі; вони також призвели до розробки поганих продуктів кібербезпеки та гальмували створення чітких політичних і військових доктрин щодо кібервійни.

У більшості випадків «питання щодо нових доктрин та технологій можна вирішити шляхом випробувань і помилок в реальному світі. Це особливо актуально у сфері кібербезпеки приватного сектора; компанії постійно інвестують і адаптуються, щоб запобігти загрозам або, якщо їх експлуатують через попередню невідому вразливість, швидко реконструювати атакуючий код і створити захист. Цей метод дозволяє доктринам і технологіям безпеки швидко й послідовно коригуватись й адаптуватись до нових викликів» [74].

Проте, у контексті протистояння між державами таке локальне вирішення проблеми є неефективним, оскільки воно не усуває першопричину, а лише

тимчасово нейтралізує загрозу. Держави можуть дозволити собі реагувати на окремі випадки кібершпигунства, але такий підхід не повністю усвідомлює потенційну роль кібероперацій у скоординованій військовій кампанії. Масштабні політичні чи військові події, такі як криза великої держави або війна, включають багато мінливих і часто непередбачуваних елементів. Через брак достатньої кількості реальних прикладів складно точно спрогнозувати, як держави та інші політичні гравці використовуватимуть свій кіберпотенціал під час криз і конфліктів.

Цілком справедливо зазначають А.Пехник та Ю.Завгородня, головна проблема, що «в кіберпросторі важко персоналізувати учасників, тому саме по цим причинам важко зрозуміти кінцевих замовників або учасників». Вчені акцентують увагу, що «сторін протиборства є мінімум двоє, особливість їх дій в тому, що інші учасники можуть залучатись самостійно до такої форми конфлікту в кіберсередовищі лише через власне ставлення та відношення до такого типу конфлікту. Якщо деталізувати кіберконфлікти для політичних процесів на територіях пострадянських країн, то учасниками політичної конфронтації є: суб'єкти політики, громадяни, підприємства, кіберфахівці. Суб'єкти політики можуть створювати публічні висловлювання щодо кіберборотьби, пересічні громадяни висловлюють власну позицію намаючись видати свою власну позицію за об'єктивну для більшості, а кіберфахівці вчиняють заходи щодо кіберзахисту, кібербезпеки та кібератак на опонента» [50]. «Політична конфронтація розпочинається ідентично звичайному конфлікту, а саме з інциденту, як першопричині зародження протидії сторін. Причинами прояву інциденту можуть бути: політичні рішення, висловлювання, дії (нормативні акти, які не підтримуються суспільством, дії політиків, які дискредитують себе, як політичних акторів). В свою чергу такі суспільні процеси як: питання мови, релігії, корупції стають тригерами етноконфліктів» [50].

Загострення політичної боротьби є небезпечним через його потенційно неконтрольовані масштаби, оскільки кіберпростір не має державних кордонів.

Точно оцінити рівень загрози для держави чи суспільства складно, адже це залежить від учасників конфлікту та об'єкта їхнього протистояння, тобто від того, за що саме ведеться боротьба як головна мета конфронтації. «За даними дослідження IBM Global Average Data Breach, у 2022 році глобальні втрати даних від кібератак становили 4,4 мільйона доларів, порівняно з 4,2 мільйона у 2021 році та 3,9 мільйона доларів у 2020 році» [49].

Безперечно, політика держав на пострадянському просторі щодо кіберспівпраці має бути однозначною та твердою, навіть якщо кібератаки ще не мають значного впливу на політичну систему. Досвід європейських країн свідчить, що реакція на кібернетичні напади найчастіше відбувається вже після виникнення проблеми або під час аналізу завданих суспільству чи органам влади збитків. Так, на думку А.Пехник та Ю.Завгородньої, «сутність політики міститься у боротьбі за владу та розподіл владних повноважень, а відповідно і бажанням кожного політичного та державного діяча є здобуття, збільшення влади, тоді як політичні партії метою своє діяльності ставлять саме збільшення підтримки серед населення для можливостей збільшення політичної сили, а відповідно і збільшення владних повноважень. Для досягнення таких цілей, і партія, і лідери застосовують ряд політичних технологій, які допомагають підтримувати і навіть збільшувати підтримку серед громадян. Категорія громадян на яких розповсюджують суб’єкти політики свій вплив для підтвердження ефективності власної політичної діяльності» [5049].

Наприклад, в Україні, як і в інших пострадянських країнах, реакція на кіберзагрози відбувалася подібним чином. Лише після анексії частини українських територій почалися серйозні кібератаки на банки, об'єкти критичної інфраструктури та державні вебсайти, що змусило державу ухвалити Закон України «Про основні засади забезпечення кібербезпеки України» у 2017 році [19], а також Указом Президента України введено в дію Рішення Ради національної безпеки і оборони України «Про стратегію кібербезпеки України» (2021) [66]. У зв’язку з цим, «під час використання політичних технологій варто враховувати усі можливі особливості розвитку подій та враховувати усі

можливі негативні наслідки та різні напрямки розвитку політичних процесів. Відповідно, до поданої інформації в різних інформаційних ресурсах, в різни регіонах сприйняття може бути інше, а відповідно і рівень підтримки може бути різним» [50].

Отже, варто погодитись с висновками, що «для всіх учасників інформаційного простору, які не мають спільної політики щодо політичних процесів у суспільстві та перебувають у політичному протистоянні, вкрай важливо приділити увагу кіберзахисту. Це включає розробку законодавчих норм, проведення публічних дискусій, інформування про ризики використання неліцензійних ресурсів, забезпечення захисту власних пристроїв для користування кіберпростором і, найголовніше, запровадження реальних видів відповідальності за кіберзлочини» [57].

Варто погодитись, і з твердженням, що «з розвитком суспільства розвивається система управління, а відповідно і розвиваються різновиди конфліктів. За останні п’ять років (через пандемію та повномастабну війну) велика частина комунікаційних процесів трансформувалась в кіберпростір, тому небезпека та загроза кіберпротиборства стала актуальною, а кіберзагрози реальністю суспільно-політичного буття» [57]. Вважаємо, що «питання кібеконфліктів у протиборстві суб’єктів політики на території пострадянських країн, є серйозною загрозою для великої кількості осіб, які особисто не приймають участь у конфлікті, проте можуть відчути її наслідки. Щодо міжнародного рівня кіберзахисту, то він знаходиться на стадії теоретичного обговорення з визначенням статегічних завдань. У теперішній час кожна країна намагається вирішувати це питання індивідуально та звичними для себе методами, як до прикладу Китай закритою внутрішньою системою кібервідносин, та США, як зразок демократичних основ та вільного користування кіберпростором орієнтованим на свідомості громадян з системним підходом щодо захисту громадян в усіх сферах» [57].

Європейський Союз має значний досвід у протидії кіберзлочинності, і Директива про мережеву та інформаційну безпеку є важливим документом,

який варто проаналізувати з метою можливого впровадження в українське законодавство. Ця директива встановлює загальноєвропейські принципи та стандарти кібербезпеки, сприяючи поглибленій співпраці між країнами-членами ЄС. Враховуючи це, сучасним інформаційним державам, зокрема Україні, необхідно чітко визначити стратегію свого розвитку та інтегруватися в міжнародну систему кібербезпеки для ефективного захисту в кіберпросторі. Важливим кроком України в цьому напрямку стало офіційне приєднання до Центру НАТО з питань співробітництва в галузі кіберзахисту, спрямоване на підвищення рівня власної кібербезпеки. Як відзначає Ю.Завгородня щодо політики НАТО відносно здійснення впливу на кіберконфлікти, що це «нова форма політичного протистояння, яка виражається у системній боротьбі членів Альянсу з кібератаками та фейками». Вчена акцентує, що «пуваги отребує причинно-наслідковий зв'язок виникнення таких форм протиборства, оскільки саме в об’єкті та суб’єктах кіберпротиборства формується розуміння необхідності впливу на ці процеси» [18].

Отже, на думку дисертанта, цілком справедливо ствердження, що «конфронтація суб’єкті політики в інформаційному середовищі несе ряд викликів, які потребують уваги для стабілізаційного розвитку національних політичних систем країн на глобальної системи взаємовідносин» [57].

Сучасна геополітична ситуація характеризується ескалацією напруженості та посиленням негативних процесів у сфері глобальної та регіональної безпеки. Це зумовлено як загостренням суперництва між провідними світовими державами, так і зіткненням національних інтересів окремих акторів. У цьому контексті відбувається фундаментальна трансформація міждержавних відносин та природи військового насильства, де інформаційний компонент набуває стратегічно важливого та імперативного значення на всіх етапах розвитку конфліктних ситуацій, від їх зародження до врегулювання.

Інформація в сучасному світі де-факто набула властивостей зброї, а потенційні наслідки її застосування можна співставити з руйнівним ефектом

традиційних військових засобів. У науковому дискурсі активно використовується термін «інформаційна зброя», що концептуалізується як інтегрована сукупність інформаційних засобів, технологічних рішень, спеціалізованих методів та речовин, спрямованих на прихований насильницький вплив на інформаційно-технічні та інформаційно-психологічні об'єкти супротивника. Стратегічною метою застосування інформаційної зброї є досягнення визначених цілей в рамках інформаційної війни.

Особливу небезпеку становлять технології ведення інформаційних війн, що ґрунтуються на маніпулятивному контролі політичної свідомості та поведінки громадян. Їх деструктивний потенціал спрямований на глибоку фрагментацію суспільства шляхом провокування внутрішніх конфліктів або на консолідацію агресії проти штучно створеного зовнішнього чи внутрішнього ворога. Домінуючим об'єктом впливу в інформаційній війні виступає суспільна та індивідуальна свідомість, а кінцевою метою є підміна автентичних національних цінностей та фундаментальних інтересів.

Інформаційна зброя характеризується низкою специфічних атрибутів, серед яких слід виокремити універсальність застосування, латентність дії, раптовість впливу, високу економічну ефективність, масштабність потенційного охоплення аудиторії, каскадність деструктивних ефектів та значну складність міжнародного регулювання її розробки та застосування. Інформаційний простір активно використовується як канал для цілеспрямованої дискредитації конституційних засад держав та їх владних інститутів, розмивання національної ментальності й культурної ідентичності, вербування індивідів до екстремістських та терористичних організацій, ескалації міжнаціональної та міжконфесійної ворожнечі, а також для формування широкого спектру радикального та протестного потенціалу.

У контексті сучасних міждержавних відносин спостерігається неухильне зростання ролі інформаційного фактору в провокуванні та ескалації конфліктів, а також у гібридних формах протистояння, спрямованих на підрив державного суверенітету, порушення територіальної цілісності та гальмування процесів

національного розвитку. Інформаційне протиборство слід розуміти як комплексну діяльність, що охоплює інформаційно-технічний та інформаційно-психологічний виміри, здійснювану державами як в умовах воєнного, так і мирного часу з метою протекції власних національних інтересів та зміцнення позицій у конкурентній боротьбі за політичний вплив на регіональному та глобальному рівнях. Контроль над ключовими засобами масової інформації розглядається як один з найважливіших інструментів впливу на когнітивні процеси та масову свідомість населення.

Після завершення епохи біполярного протистояння та особливо після військової операції "Буря в пустелі" спостерігається значна інтенсифікація наукових досліджень у сфері інформаційного протиборства, що зумовлено глибоким усвідомленням інформації як критично важливого фактору ведення сучасної війни. Досягнення інформаційної та технологічної переваги позиціонується провідними військовими стратегами як фундаментальна складова підвищення бойового потенціалу збройних сил. У новій безпековій парадигмі інформаційні операції розглядаються як ключовий вид військової діяльності, що можуть здійснюватися як автономно, так і в тісній інтеграції з традиційними військовими операціями.

Зростання значущості інформаційного впливу об'єктивно зумовлює підвищену актуальність проблематики інформаційної безпеки, яка визначається як стан захищеності збалансованих інтересів особистості, суспільства та держави від існуючих та потенційних загроз в інформаційній сфері. Головною метою забезпечення інформаційної безпеки є формування та підтримання такого рівня захищеності національного інформаційного простору, який гарантує ефективну реалізацію національних інтересів та сталий прогресивний розвиток держави в умовах глобалізації та інформатизації.

Об'єктами інформаційного протиборства можуть виступати будь-які сутності, щодо яких існує можливість здійснення інформаційних операцій, що призводять до модифікації їхніх характеристик як інформаційних систем. До таких об'єктів належать як когнітивна сфера окремих індивідів та різноманітних

соціальних груп, так і складні інформаційно-технічні комплекси, що забезпечують функціонування критичної інфраструктури. Суб'єктами інформаційної безпеки є держави, міждержавні об'єднання, міжнародні та недержавні організації, нелегітимні збройні формування, транснаціональні корпорації та медіа-холдинги, кожен з яких має власні інтереси та стратегії в інформаційному просторі.

Держава як ключовий суб'єкт інформаційної безпеки характеризується наявністю стійких національних інтересів в інформаційній сфері, формуванням та ефективним регулюванням національного інформаційного простору, створенням спеціалізованих державних структур, розробкою засобів інформаційного впливу та відповідної нормативно-правової бази. Фундаментальними принципами забезпечення інформаційної безпеки виступають законність, правова визначеність, забезпечення балансу інтересів особистості, суспільства та держави, комплексність підходу до вирішення проблем, наукова обґрунтованість прийнятих рішень, інтеграція з міжнародними системами безпеки та економічна доцільність здійснюваних заходів.

Сучасна конкуренція в інформаційній сфері набуває форми безкомпромісної боротьби, що отримала умовну назву «інформаційний підприємець». Стратегічною метою цієї боротьби є здобуття вирішальної інформаційної переваги шляхом комплексного зміцнення власної інформаційної безпеки та одночасного послаблення інформаційної безпеки потенційного опонента. Перебіг та результати інформаційного протиборства є детермінованими низкою факторів, включаючи сукупність матеріальних та духовних ресурсів протиборчих сторін, актуальну інформаційну ситуацію, якість та кількість наявних засобів інформаційного впливу, рівень професійної кваліфікації залученого персоналу, ступінь пропорційності між поставленими цілями та використовуваними засобами, рівень координації дій сил та засобів, а також загальний рівень бойової готовності залучених структур.

Підготовка та ведення інформаційного протиборства регламентуються низкою ключових принципів, серед яких особливе значення мають принцип підпорядкування цілей інформаційної боротьби політичним цілям держави, принцип концентрації основних зусиль у вирішальний час та у вирішальній точці інформаційного простору, принцип завчасної та всебічної підготовки сил та засобів, принцип постійної готовності до активних дій, принцип високої активності та рішучості, принцип скоординованого застосування всіх наявних сил та засобів, принцип спадкоємності у веденні інформаційного протиборства, принцип підтримання необхідної інтенсивності впливу, принцип своєчасного маневрування силами та засобами, принцип вмілого використання та оперативного відновлення бойового потенціалу, принцип досягнення раптовості дій, принцип врахування морально-психологічного фактора, принцип всебічного забезпечення сил та засобів, а також принцип безперервного та гнучкого управління.

Економічний базис держави виступає фундаментальною матеріальною основою для процесів інформатизації суспільства та держави, що є необхідною передумовою для успішного ведення інформаційного протиборства як в мирний, так і у воєнний час. Стратегічною метою деструктивних інформаційних впливів є досягнення такого рівня рефлекторного контролю над противником, який забезпечує його безумовне підпорядкування волі агресора. Результати ефективно проведеного інформаційного протиборства можуть мати наслідки, які за своєю значущістю є порівнянними з ефектом військового насильства, що підкреслює його провідну роль у системі забезпечення національної безпеки держави.

Для ефективного здійснення інформаційного протиборства та забезпечення належного рівня інформаційної безпеки держави існує нагальна потреба у якісній спеціалізованій підготовці висококваліфікованих фахівців, а також у системному підвищенні рівня загальної, гуманітарної та інформаційної культури суспільства в цілому. Сучасне інформаційне протиборство характеризується високим рівнем інтелектуалізації застосовуваних методів,

значною латентністю впливу, інтенсивним використанням передових технологій, безперервністю ведення та агресивним характером дій. Управління інформаційними ресурсами держави є критично важливим фактором для завоювання, збереження та ефективної реалізації державної влади.

У сучасній системі міждержавного протистояння спостерігається стрімке зростання ролі кіберпростору як нової арени конфронтації політичних суб'єктів. Кіберсфера здійснює значний вплив на реальну військову справу та суттєво трансформує способи взаємодії суспільства в глобальній мережі Інтернет. Конфронтація в кіберпросторі набуває ознак так званих «прохолодних війн», що відображає прагнення держав до стримування від відверто жорстоких дій, проте з одночасним активним використанням некінетичних методів впливу. Кіберпростір характеризується зміною структури, змісту та локалізації взаємодій між суб'єктами протиборства. Одним з найбільш поширених інструментів кіберзлочинності є DDoS-атаки, що суттєво впливають на динаміку конфлікту та міждержавні відносини. Політична конфронтація в кіберпросторі все частіше використовується як ефективний інструмент зовнішньої політики держав.

Застосування кібероперацій державними та недержавними акторами актуалізує питання щодо інструментів досягнення стратегічної переваги у майбутніх конфліктних процесах, проте на даний момент спостерігається дефіцит наукового консенсусу щодо цієї проблематики. Інформаційна конфронтація в кіберпросторі принципово відрізняється від традиційних кінетичних війн відсутністю прямого фізичного насильства, неруйнівним характером (у традиційному розумінні) та значною складністю атрибуції дій конкретним акторам. Існує також значний розрив між рівнем розуміння технологічних аспектів кібербезпеки та політичними процесами, що ускладнює формування ефективних та адекватних стратегій кіберзахисту на державному рівні. На відміну від приватного сектору, екстраполяція методу проб та помилок на міждержавну кіберконфронтацію є недоцільною та несе значні ризики. Проблема анонімності та складності атрибуції в кіберпросторі суттєво

ускладнює ідентифікацію кінцевих замовників та безпосередніх виконавців кібернетичних атак.

Основними акторами політичної конфронтації в кіберпросторі на пострадянських територіях виступають суб'єкти політичної діяльності, громадяни, представники бізнесу та безпосередньо кіберфахівці. Політична конфронтація в кіберпросторі започатковується різноманітними політичними рішеннями, публічними заявами, діями владних структур, а також актуалізацією гострих суспільно значущих питань. Відсутність чітких територіальних обмежень у кіберпросторі робить політичне загострення небезпечним та важко контрольованим, зумовлюючи ризики неконтрольованої ескалації конфлікту. Кібератаки призводять до значних фінансових втрат на глобальному рівні. У цьому контексті існує нагальна потреба у формуванні чіткої та рішучої державної політики у сфері кібербезпеки. На пострадянському просторі політика кібербезпеки часто має реактивний характер, що є недостатнім для ефективної протидії сучасним загрозам. В Україні вживаються законодавчі заходи у сфері кібербезпеки, проте важливим є врахування особливостей сприйняття інформації різними соціальними групами та регіонами. Першочерговими завданнями у сфері кіберзахисту є вдосконалення нормативно-правового регулювання, активізація публічної дискусії, підвищення рівня обізнаності громадян, створення ефективних технічних засобів захисту та встановлення невідворотної відповідальності за кіберзлочини. Масова міграція комунікаційних процесів у кіберпростір об'єктивно робить кіберзагрози реальною складовою сучасного суспільно-політичного буття. Кіберконфлікти становлять загрозу для широкого загалу користувачів кіберпростору. Міжнародна співпраця у сфері кібербезпеки перебуває на початковому етапі свого формування, і на даний момент кожна країна намагається вирішувати питання кібербезпеки індивідуально. Існують різні національні моделі кібербезпеки, що демонструють Китай, США та Європейський Союз. У цьому контексті існує нагальна необхідність посилення міжнародної співпраці у сфері кібербезпеки. Участь України в міжнародних

ініціативах, таких як приєднання до Центру НАТО з питань співробітництва в галузі кіберзахисту, є важливим кроком у цьому напрямку.

Отже, конфронтація політичних суб'єктів в інформаційному середовищі несе комплекс різноманітних викликів, що потребують системної уваги та скоординованих зусиль для забезпечення стабілізаційного розвитку як національних політичних систем, так і глобальної системи міждержавних відносин.

Висновки до Розділу 2.

Аналіз дозволяє сформулювати комплексні науково обґрунтовані висновки щодо політико-стратегічних імперативів конфронтації в інформаційному просторі, еволюції концепції інформаційної війни та її інтеграції з парадигмою мережевоцентричної війни (NCW), особливо в контексті сучасних міждержавних відносин та емпіричного досвіду російсько-українського конфлікту.

По-перше, фундаментальною констатацією є якісна трансформація інформаційного простору, який з технічної сфери еволюціонував у публічну, всеосяжну та стратегічно значущу арену політичної боротьби. Втрата ознак приватності та географічної обмеженості інформаційного обміну зумовила розмивання традиційних меж між військовою та цивільною сферами в контексті конфлікту. Емпіричний досвід російсько-української війни є показовим прикладом, де бойові дії розгортаються не лише на фізичному полі бою, але й у публічному інформаційному просторі, що актуалізує питання інформаційної безпеки як критично важливого елементу національної стійкості.

По-друге, інформаційна епоха спричинила значну демократизацію доступу до інформації, що призвело до ерозії монополії держав та їх силових структур на володіння інформацією в режимі реального часу. Комерційна доступність передових технологій, таких як супутникова зйомка, геопросторова аналітика та високошвидкісні канали передачі даних, надає широкий спектр

інформаційних можливостей недержавним акторам, що раніше були прерогативою виключно наддержавних утворень. Засоби масової інформації та глобальна мережа Інтернет забезпечують миттєву дисемінацію інформації для глобальної аудиторії, що суттєво впливає на формування суспільної думки та політичні процеси. Паралельно, темпоральна компресія процесів прийняття рішень в умовах інформаційної перевантаженості створює нові виклики для ефективного стратегічного управління.

По-третє, концепція мережевоцентричної війни (NCW) являє собою операційну парадигму, що передбачає інтеграцію особового складу, систем підтримки прийняття рішень, сенсорних платформ та вогневих засобів через високошвидкісні комунікаційні мережі для досягнення спільного інформаційного простору та синергії бойових операцій. NCW надає можливість децентралізованим підрозділам досягати високої операційної ефективності завдяки розподіленому управлінню, мобільності та адаптивності. Проактивне впровадження Україною принципів NCW ще до початку повномасштабної агресії продемонструвало ефективність невеликих автономних підрозділів у протистоянні переважаючим силам противника. Синергія вогневих засобів, розвідки та управління в рамках NCW є критично важливим фактором успіху. Україна наразі є одним із лідерів у сфері NCW завдяки досягнутому рівню інформаційної обізнаності на полі бою. Стійкість децентралізованої системи управління до кібернетичних загроз є ще однією перевагою, хоча функціонування NCW критично залежить від надійного супутникового інтернет-зв'язку, такого як Starlink. Стратегічний інтерес та підтримка західних союзників відіграють важливу роль у розвитку NCW в Україні, яка фактично стала полігоном для тестування західних військових технологій. NCW забезпечує операційну динаміку на всіх рівнях військової діяльності, трансформуючи характер бойових дій у більш швидкий та ефективний процес, що базується на високій швидкості командування та самосинхронізації дій підрозділів.

По-четверте, перехід до парадигми NCW вимагає фундаментальних змін в організаційній структурі, підготовці особового складу, розподілі ресурсів та інтеграції новітніх технологій з існуючими доктринами та концепціями. Практична реалізація NCW у бойових умовах забезпечує відчутну перевагу завдяки розгалуженій мережі поінформованих сил та ефективній інформаційній інфраструктурі. Ключовими операційними перевагами NCW є швидкість командування та самосинхронізація, що трансформують інформаційну перевагу в стійку конкурентну перевагу. Емпіричний досвід російсько-українського конфлікту є переконливим підтвердженням ефективності NCW у сучасному високоінтенсивному конфлікті.

По-п'яте, для ефективного здійснення інформаційного протиборства та забезпечення належного рівня інформаційної безпеки держави існує нагальна потреба у якісній спеціалізованій підготовці висококваліфікованих фахівців, а також у системному підвищенні рівня загальної, гуманітарної та інформаційної культури суспільства в цілому. Сучасне інформаційне протиборство характеризується високим рівнем інтелектуалізації застосовуваних методів, значною латентністю впливу, інтенсивним використанням передових технологій, безперервністю ведення та агресивним характером дій. Управління інформаційними ресурсами держави є критично важливим фактором для завоювання, збереження та ефективної реалізації державної влади.

По-шосте, у сучасній системі міждержавного протистояння спостерігається стрімке зростання ролі кіберпростору як нової арени конфронтації політичних суб'єктів. Кіберсфера здійснює значний вплив на реальну військову справу та суттєво трансформує способи взаємодії суспільства в глобальній мережі Інтернет. Конфронтація в кіберпросторі набуває ознак так званих "прохолодних війн", що відображає прагнення держав до стримування від відверто жорстоких дій, проте з одночасним активним використанням некінетичних методів впливу. Кіберпростір характеризується зміною структури, змісту та локалізації взаємодій між суб'єктами протиборства. Одним з найбільш поширених інструментів кіберзлочинності є DDoS-атаки, що

суттєво впливають на динаміку конфлікту та міждержавні відносини. Політична конфронтація в кіберпросторі все частіше використовується як ефективний інструмент зовнішньої політики держав.

Застосування кібероперацій державними та недержавними акторами актуалізує питання щодо інструментів досягнення стратегічної переваги у майбутніх конфліктних процесах, проте на даний момент спостерігається дефіцит наукового консенсусу щодо цієї проблематики. Інформаційна конфронтація в кіберпросторі принципово відрізняється від традиційних кінетичних війн відсутністю прямого фізичного насильства, неруйнівним характером (у традиційному розумінні) та значною складністю атрибуції дій конкретним акторам. Існує також значний розрив між рівнем розуміння технологічних аспектів кібербезпеки та політичними процесами, що ускладнює формування ефективних та адекватних стратегій кіберзахисту на державному рівні. На відміну від приватного сектору, екстраполяція методу проб та помилок на міждержавну кіберконфронтацію є недоцільною та несе значні ризики. Проблема анонімності та складності атрибуції в кіберпросторі суттєво ускладнює ідентифікацію кінцевих замовників та безпосередніх виконавців кібернетичних атак.

Основними акторами політичної конфронтації в кіберпросторі на пострадянських територіях виступають суб'єкти політичної діяльності, громадяни, представники бізнесу та безпосередньо кіберфахівці. Політична конфронтація в кіберпросторі започатковується різноманітними політичними рішеннями, публічними заявами, діями владних структур, а також актуалізацією гострих суспільно значущих питань. Відсутність чітких територіальних обмежень у кіберпросторі робить політичне загострення небезпечним та важко контрольованим, зумовлюючи ризики неконтрольованої ескалації конфлікту. Кібератаки призводять до значних фінансових втрат на глобальному рівні. У цьому контексті існує нагальна потреба у формуванні чіткої та рішучої державної політики у сфері кібербезпеки. На пострадянському просторі політика кібербезпеки часто має реактивний характер, що є

недостатнім для ефективної протидії сучасним загрозам. В Україні вживаються законодавчі заходи у сфері кібербезпеки, проте важливим є врахування особливостей сприйняття інформації різними соціальними групами та регіонами. Першочерговими завданнями у сфері кіберзахисту є вдосконалення нормативно-правового регулювання, активізація публічної дискусії, підвищення рівня обізнаності громадян, створення ефективних технічних засобів захисту та встановлення невідворотної відповідальності за кіберзлочини. Масова міграція комунікаційних процесів у кіберпростір об'єктивно робить кіберзагрози реальною складовою сучасного суспільно-політичного буття. Кіберконфлікти становлять загрозу для широкого загалу користувачів кіберпростору. Міжнародна співпраця у сфері кібербезпеки перебуває на початковому етапі свого формування, і на даний момент кожна країна намагається вирішувати питання кібербезпеки індивідуально. Існують різні національні моделі кібербезпеки, що демонструють Китай, США та Європейський Союз. У цьому контексті існує нагальна необхідність посилення міжнародної співпраці у сфері кібербезпеки. Участь України в міжнародних ініціативах, таких як приєднання до Центру НАТО з питань співробітництва в галузі кіберзахисту, є важливим кроком у цьому напрямку.

Таким чином, конфронтація політичних суб'єктів в інформаційному середовищі є складним та багатогранним феноменом, що несе комплекс різноманітних викликів для національної та міжнародної безпеки. Ефективна протидія цим викликам вимагає системної уваги, скоординованих зусиль на національному та міжнародному рівнях, а також глибокого розуміння політико-стратегічних імперативів інформаційної війни та її еволюції в контексті розвитку новітніх технологій.

Список посилань до Розділу 2.

1. Антонюк В. (2021) Інформаційна війна в структурі сучасного геополітичного протиборства: нові контексти та інтерпретації. *Державне*

управління та розвиток. №35. URL: http://www.dy.nayka.com.ua/pdf/7_2021/35.pdf (дата звернення 21.02.2025)

2. Арміяinform: сайт. Міністерство оборони України. URL: https://armyinform.com.ua/ (дата звернення: 10.04.2024).

3. Баровська А. (2015). Стратегічні комунікації: досвід НАТО. *Стратегічні пріоритети.* № 1 (34). С. 147–152.

4. Бєлай С., Корнієнко Д. (2018). Інформаційна безпека сьогодення – невід'ємна складова воєнної безпеки. *Актуальні проблеми управління інформаційною безпекою держави.* Київ: Національна академія Служби безпеки України. 408 с.

5. Біденко А. (2021). Центр протидії дезінформації: філософія проти менеджменту. ГО «Детектор медіа». URL: https://detector.media/infospace/article/185107/2021-02-22-tsentr-protydii-dezinformatsiifilosofiya -proty-menedzhmentu/ (дата звернення: 01.05.2024).

6. Білобородов О., Довгополий А. (2019). Технології інформаційно-психологічних війн та інформаційно-психологічна зброя. *Озброєння та військова техніка,* №4. С. 93–99.

7. Васильків І. (2020). Основи теорії ймовірностей і математичної статистики. URL: https://new.mmf.lnu.edu.ua/wp-content/uploads/2020/04/Vasyl-kiv-I.M.-TIMS_CHASTYNA_1.pdf9 (дата звернення 12.09.2024)

8. Войціховський А. (2018)/ Кібербезпека як важлива складова системи захисту національної безпеки європейських країн. *Журнал східноєвропейського права*. № 53 С. 26-37.

9. Гбур З. (2022). Використання штучного інтелекту в інформаційній безпеці України. *Державне управління: удосконалення та розвиток*. № 1. DOI: 10.32702/2307-2156-2022.1.2.

10. Глушков В. (2015). Основи новітньої теорії ведення сучасних війн. *Актуальні проблеми політики***.** № 56. С. 12-21.

11. Гріга В., Гізун А. (2016).. Аналіз сучасних теорій інформаційно-психологічних впливів в аспекті інформаційного протиборства. *Актуальні*

задачі та досягнення у галузі кібернетики, Матеріали конференції. URL: https://core.ac.uk/download/pdf/84825492.pdf (дата звернення 11.01.2025)

12. Гула Р. (2020) Концептуальні засади воєнної політики у кіберпросторі провідних держав світу та воєнно-політичних інституцій / Р. Гула, І. Передерій, О. Вітринська. *Вісник бібліотечної палати*. № 4. С. 22–26.

13. Гуцал С. (2016). Публічна дипломатія та стратегічні комунікації: концептуальні засади взаємозв'язку та взаємодії. *Запровадження комунікації органів державної влади: Зб. мат-лів наук.-практ. конф*. Київ : Фенікс. С. 161–169.

14. Данілов О. (2020). Кіберзахист державних інформаційних ресурсів - важлива складова у процесі цифрової трансформації країни. URL: https://www.rnbo.gov.ua/ua/Diialnist/4606.html

15. Денисовець І. (2024) Інформаційні операції у структурі соціально-політичних комунікацій: сутність та засоби реалізації. *Інформація та соціум.* (Жотень). С. 12-14.

16. Дудатьєв А. (2022). Методологія інформаційного протиборства. Доповідь. URL: R.lib.vntu.edu.ua/bitstream/handle/123456789/39919/16133.pdf? (дата звернення 25.09.2024)

17. Дудатьєв А., Войтович, О. (2017). Інформаційна безпека соціотехнічних систем: Модель інформаційного впливу. *Інформаційні технології та комп'ютерна інженерія.* №38(1). С. 16–21.

18. Завгородня Ю. (2022) Роль нато у боротьбі з кіберконфліктами: політико-правовий аспект. *Регіональні студії*. № 30. С. 62-65.

19. Закон України «Про основні засади забезпечення кібербезпеки України» № 2163-VIII. *Відомості Верховної Ради України*. № 45. 2017. URL: https:// zakon.rada.gov.ua/laws/show/2163-19#Text (дата звернення 11.01.2025)

20. Запорожець, О. (2021). Операції впливу: концептуальний вимір. *Медіафорум: аналітика, прогнози, інформаційний менеджмент* №9, с.232-244.

21. Заруба О. (2017) Планування спеціальних інформаційних операцій. *Інформаційна безпека людини, суспільства, держави*. № 1 (21). С. 140–154.

22. Застосування Сухопутних військ Збройних Сил України у конфліктах сучасності (за досвідом забезпечення національної безпеки складовими сектору безпеки і оборони у ході російсько-української війни): *Збірник тез доповідей науково-практичної конференції* (Львів, 29-30 листопада 2023 р.). Львів: НАСВ, 2023. 381 с.

23. Золотухін Д. (2014) Біла Книга спеціальних інформаційних операцій проти України 2014–2018. Київ, 384 с.

24. Золотухін Д. Центр протидії дезінформації: практика імплементації. ГО «Детектор медіа». URL: https://detector.media/infospace/article/185586/2021-03-08-tsentr-protydii-dezinformatsiipraktyka-implementatsii/ (дата звернення: 01.05.2024).

25. Золотухін Д. (2018) Біла Книга спеціальних інформаційних операцій проти України. Київ, 368 с.

26. Інформаційна безпека. Підручник (2021) / В.В. Остроухов, М.М. Присяжнюк, О.І. Фармагей, М.М. Чеховська та ін.; під ред. В.В. Остроухова. Київ : Видавництво Ліра-К. 412 с.

27. Інформаційна зброя – теорія і практика застосування в інформаційному протиборстві, 2012. URL: https://mil.in.ua/uk/informatsijna-zbroya-teoriya-i-praktyka-zastosuvannya-v-informatsijnomu-protyborstvi/ (дата звернення 12.01.2025)

28. Інформаційні виклики гібридної війни: контент, канали, механізми протидії: аналіт. Доп. (2016). / За заг. ред. А. Баровської. Київ : НІСД. С. 69–80.

29. Клаузевіц К. (2023). Найважливіші принципи ведення війни. Арій, 384 с.

30. Комаров М., Гончар С., Дімітрєва Д. (2021). Дослідження проблеми кіберживучості об’єктів критичної інформаційної інфраструктури. Ядерна та радіаційна безпека. № 1(89). С. 59-66

31. Коцофане О. Які соцмережі і месенджери найпопулярніші серед українців. Webpromo. URL: https://web-promo.ua/ua/blog/kakie-socseti-i-messendzhery-samye-populyarnye-sredi-ukraincev/ (дата звернення: 01.05.2024).

32. Леонов Я., Васильківський Д., Бойко В. (2024). Еволюція інформаційного маркетингу: стратегії та технології в сучасному бізнесі. *Ефективна економіка.* № 2.

33. Лісовський П., Лісовська Ю. (2024). Воєнна мережева криптосистема: державотворчий інноваційний контекст: монографія. Київ : Видавництво Ліра-К. 114 с.

34. Лужецький В., Дудатьєв А. (2017). Концептуальна модель системи інформаційного впливу. *Безпека інформації*. №23 (1). С.45–49.

35. Ланьє Д. (2020). Десять причин видалити акаунт із соцмереж просто зараз. Харків: Віват. 176 с.

36. Лазоренко О. А. (2014). Визначальні характеристики мережевої війни як нового виду боротьби. *Scientific researches and their practical application.modern state and ways of development*. URL: https://sworld.education/index.php/safety-314/national-security-314/23039-314-248 (дата звернення 02.09.2024)

37. Литвиненко О. (2003) Інформаційні впливи та операції. Теоретико-аналітичні нариси. Київ: НІСД. 240 с.

38. Магда Е. (2015). Гібридна війна: вижити і перемогти. Харків: Віват. 320 с

39. Маркузе Г. (1996) Одновимірна людина. Дослідження ідеології розвинутого індустріального суспільства. *Сучасна зарубіжна соціальна філософія: Хрестоматія*. Київ: Либідь. С. 87–134.

40. Медіа споживання на звільнених і прифронтових територіях (2023). URL: https://www.kiis.com.ua/?lang=ukr&cat=reports&id=1308&page=9 (дата звернення: 10.04.2024).

41. «Мережева війна» як спосіб досягнення світового панування США. *Військова панорама.* URL: http://wartime.org.ua/206-merezheva-vyna-yaksposb-dosyagnennya-svtovogo-panuvannya-ssha.html (дата звернення 02.09.2024)

42. Мишкало М. Нові правила війни. URL: http://zgroup.com.ua/article.php?articleid=3851 (дата звернення 12.09.2024)

43. Мережі і мережні війни: майбутнє терору, злочинності та бойових дій / за ред. Дж. Арквілла, Д. Ронфельдта; пер. з англ. А. Іщенка. (2005). Київ: Вид. дім «Києво-Могилянська академія». 350 с.

44. Осьодло В., Денисенко І., Побочий І., Віннікова Н. (2021) Війни інформаційної епохи: міждисциплінарний дискурс: монографія /за ред. В.А. Кротюка. Харків: ФОП Федорко М. Ю. 558 с.

45. Панфілов Ю., Фінін Г. (2021) Організаційні війни як різновид неконвенційних війн. Війни інформаційної епохи: міждисциплінарний дискурс. Харків: ФОП Федорко М. С. 55-58.

46. Панченко В. (2014). Інформаційні операції в асиметричній війні Росії проти України: підходи до моделювання. Інформація і право. № 3 (12). С. 13–16.

47. Панченко В. (2016). Інформаційні операції в системі стратегічних комунікацій. *Стратегічні пріоритети. Серія: Політика*. № 4. С. 72–79.

48. Парута О. (2013). Суб'єкт правової ідентичності : загальнотеоретичні аспекти Європейські перспективи. № 13. С. 12-16.

49. Пехник А. В. (2023). Допомога Україні від міжнародної спільноти в галузі освіти під час війни: регіональний та глобальний аспекти. *Європейські орієнтири розвитку України в умовах війни та глобальних викликів XXI століття: синергія наукових, освітніх та технологічних рішень: у 2 т.: матеріали Міжнар. науково-практ. конф*. (м.Одеса). Одеса: Видавництво «Юридика». Т. 1. С. 175-178.

50. Пехник А.В., Завгородня Ю. В. (2021). Сучасні загрози кібертехнологій в політичному процесі. *Актуальні проблеми політики: зб. наук. праць*. Вип. 68. С. 76-82

51. Питання Центру протидії дезінформації: Указ Президента України від 07.05.2021 №187/2021. URL: https://www.president.gov.ua/documents/1872021-38841 (дата звернення: 01.05.2024).

52. Положення «Про Міністерство цифрової трансформації». Постанова Кабінету Міністрів України. № 856 (2019) (Україна). URL: https://zakon.rada.gov.ua/laws/show/856-2019-%D0%BF#n12

53. «Про медіа». Закон України № 2849-IX (2022) (Україна). URL: https://zakon.rada.gov.ua/laws/ show/2849-20#Text

54. «Про рішення Ради національної безпеки і оборони України» від 11 березня 2021 року «Про створення Центру протидії дезінформації»: Указ Президента України від 19.03.2021 №106/2021. URL: https://zakon.rada.gov.ua/laws/show/106/2021#Text (дата звернення: 01.05.2024).

55. Разіцький В. (2008). Інформаційна політика США в XX ст.: становлення та розвиток. *Вісник Київського національного університету імені Тараса Шевченка*. Серія: Історія. 94−95, 48−51.

56. Руцький С. (2023). Загрози в сучасному політичному процесі: інформаційний аспект. *The 3rd International Scientific and Practical Internet conference «Modern Political Processes: Global and National Dimensions*». Odesa, 2023.

57. Руцький *С. (2023.)* Конфронтація взаємодії суб'єктів політики в інформаційному просторі. *Науковий журнал «Політикус*». №5. С.82-86.

58. Руцький С. (2024). Кіберконфлікти у протиборстві суб'єктів політики на території європейських країн. Сучасні виклики соціально-політичного розвитку: політико-правові та соціально-економічні виміри. Одеса: ДЗ «Південноукраїнський національний педагогічний університет імені К. Д. Ушинського», Центр соціально-політичних досліджень «Politicus». С. 60-62.

59. Савченко О. (2014). Новітні війни з використанням інформаційно-психологічної зброї. *Вісник книжкової палати*. № 8. С. 1-6.

60. Ситник Г. (2023) Філософія війни та миру. Київ: ТОВ «САК Лтд». 118 с.

61. Сіри, С., Турченко, Ю. (2012). Інформаційна політика України доби глобалізації: теоретичний аналіз. *Політичний менеджмент. №* 4−5. С. 237−245.

62. Соловйов С. (2016). Основні характеристики стратегічних комунікацій. *Вісник національного університету цивільного захисту України*. № 1 (4). С. 165–170.

63. Солодка О. (2013) Сучасні тенденції міжнародної політики забезпечення інформаційної безпеки. Інформаційна безпека людини, суспільства, держави, №3, с.25−29.

64. Терещенко В. (2023) Особливості державної інформаційної політики в умовах війни. Юридичний науковий електронний журнал, №2, с.391−395.

65. Токар О. (2009) Державна інформаційна політика: проблеми визначення концепту. Політичний менеджмент, №5, с.131−141.

66. Указ Президента України №37/2022 «Про введення в дію рішення Ради національної безпеки і оборони України» від 30 грудня 2021 року «Про План реалізації Стратегії кібербезпеки України» 2021.

67. Українські медіа, ставлення та довіра у 2023 р.: Опитування USAID-Internews щодо споживання медіа. Internews. URL: https://internews.in.ua/wp-content/uploads/2023/10/Ukrainski-media-stavlenniata-dovira-2023r.pdf (дата звернення: 01.05.2024).

68. Фурашев В. (2009). Інформаційні операції крізь призму системи моніторингу та інтеграції Інтернет-ресурсів. *Правова інформатика*. № 2. С.49−57.

69. Харченко М., Сапогов С., Шамраєва В., Новікова Л. (2017). Основні засоби інформаційного протиборства та інформаційної війни як явища сучасного міжнародного політичного процесу. *Вісник Харківського національного університету імені В Н. Каразіна. Серія «Міжнародні відносини. Економіка. Країнознавство. Туризм*. Вип. 6. С. 77-81.

70. Цимбалюк, В., Бабінська, А. (2014). Правове регулювання інформаційної безпеки в Україні: проблеми теорії та практики. *Адміністративне право і процес.* №2 (8). С.22−30.

71. Шемчук В. (2020. Загрози інформаційній безпеці: проблеми визначення та подолання. Експерт: парадигми юридичних наук і державного управління. № 1 (7). С. 285-296.

72. Шульська Н., Букіна Н., Адамчук Н. (2023). Типологічні маркери інформаційно-психологічних операцій (іпсо) в умовах війни в медіа. *Вчені записки ТНУ імені В. І. Вернадського. Серія: Філологія. Журналістика.* Т. 34. №1. ч. 2. С. 268-273.

73. Braman S. (2011). Defining information policy. Journal of Information Policy, 1, 1−5. URL: https://www.academia.edu/2310219/Defining_Information_Policy International Strategy for

74. Ertan (Eds.) (2020). Cyber Threats and NATO 2030: Horizon Scanning and Analysis: URL://https://ccdcoe. org/uploads/2020/12/Cyber-Threats-and-NATO-2030_ Horizon-Scanning-and-Analysis.pdf.

75. Locked Shields is a unique international cyber defence exercise offering the most complex technical live-fire challenge in the world: URL: https://ccdcoe.org/ exercises/locked-shields/ (дата звернення 21.10.2024)

76. Wegner D. (1992, 1994). White bears and other unwanted thoughts: Suppression, obsession, and the psychology of mental control. New York: Viking/Penguin. German translation by Ernst Kabel Verlag. Edition New York: Guilford Press.

Розділ 3
Прийоми та інструменти інформаційного протиборства в соціальних он-лайн мережах

3.1. Інформаційні атаки в інформаційних протистояннях.

У сучасних умовах глобального інформаційного міждержавного протистояння, спрямованого на зниження економічного та військового потенціалу противника, а також на руйнування духовних цінностей, що складають фундамент державного та суспільного життя, проблема інформаційного протистояння набуває одного з основних об'єктів дослідження в різних наукових галузях. Одним з таких засобів є інформаційна атака. Практика проведення інформаційних атак випереджає процес теоретичного осмислення цього явища, що і визначає актуальність даної роботи. Спробуємо розібратися в сутності інформаційної атаки шляхом виявлення онтологічних властивостей цього явища.

О. Свідерська пропонує розглядати інформаційну війну «як цілеспрямовані злочинні дії, метою яких є дезінформувати, деморалізувати, та вибудувати мовчазну покірність населення, що здійснюються державою-агресором за допомогою хакерських атак, зламів систем внутрішньо-державного забезпечення життєдіяльності та обороноздатності, дискредитації політичного керівництва й збройних сил, проведення стратегічних, кризових та бойових інформаційно-психологічних спецоперацій на території держави, яка стала об’єктом інформаційної чи гібридної агресії». Вчена визначає, що «завдяки використанню пропаганди інформаційна війна діє на чотирьох рівнях: індивідуальному, територіальному (регіональному), національному та глобальному. Виявлено, що кожен із цих рівнів містить у собі певні ризики: втрату ідентичності, відчуття відстороненості, формування образу

«внутрішньо-державного ворога», виходячи з територіальної (регіональної) ідентичності, або втрату репутаційного капіталу держави» [35].

М.Харченко, С.Сапогов, В.Шамраєва, Л.Новікова визначають, що «за метою використання така інформаційна зброя поділяється на інформаційну зброю атаки та інформаційну зброю забезпечення. Інформаційна зброя атаки – це інформаційна зброя, за допомогою якої здійснюється вплив на інформацію, що зберігається, обробляється і передається в інформаційно-обчислювальних мережах (ІОМ) і порушуються інформаційні технології, що застосовуються в ІОМ. У складі інформаційної зброї атаки виокремлюють чотири основні види засобів інформаційних впливів: засоби порушення конфіденційності інформації; засоби порушення цілісності інформації; засоби порушення доступності інформації; засоби психологічного впливу на абонентів ІОМ». Вчені зазначають, що «застосування інформаційної зброї атаки спрямоване на зрив виконання ІОМ цільових завдань. Інформаційна зброя забезпечення це інформаційна зброя, за допомогою якої здійснюється вплив на засоби захисту інформації об’єкта атаки. До складу інформаційної зброї забезпечення входять засоби комп’ютерної розвідки та засоби подолання системи захисту інформаційної системи» [39].

На думку вчених В.Наконечного, Ю.Хлевної, І.Половінкіна, М.Кузьменка, інформаційне протиборство є «складовою частиною відносин і форма боротьби сторін, кожна з яких прагне завдати противнику поразку (збитки) у вигляді інформаційних впливів в його інформаційну сферу. Об’єктом інформаційного протиборства може стати будь-який компонент чи сегмент інформаційно-психологічного простору, у тому числі такі види: масова та індивідуальна свідомість громадян; соціально-політичні системи та процеси; інформаційна інфраструктура; інформаційні та психологічні ресурси». З позиції дослідників, «головним методом інформаційного протиборства є розповсюдження неправдивої інформації». Вчені акцентують увагу, що «самі по собі технології не можуть виграти інформаційну війну. Поле бою виходить за межі алгоритмів і коду, сягаючи самої тканини наших суспільств. Аналіз

існуючих методів надійного захисту процесу формування громадської думки в мережі Інтернет, показав, що на сьогоднішній день таких методів та технологій немає і бути не може» [26].

Словосполучення «інформаційна атака» вперше було використано американськими військовими фахівцями у зв'язку з формуванням поняття інформаційної війни. Хоча ці роботи в основному пов'язані з аспектом інформаційних технологій, висловлені в них положення є основоположними.

По-перше, американські експерти зазначають, що визначення інформаційної атаки багато в чому обумовлено розумінням змісту інформаційної війни, оскільки взаємозв'язок між цими явищами класифікується за моделлю «частина-ціле».

По-друге, інформаційна атака – це складне і багатогранне явище, яке пояснюється наступним: інформаційні атаки породжуються свідомістю людини і спрямовані на неї. Зброєю інформаційних атак є цілком звичайні речі – слова, картинки, зображення, хоча в даний час їх використання і функціонування не так поширені. І, нарешті, наслідки інформаційних атак такі ж руйнівні і непередбачувані, як і фізичне знищення предметів і людей.

По-третє, інформаційні атаки поділяються на два типи: прямі та непрямі. Пряма інформаційна атака полягає в безпосередньому втручанні в інформаційний простір противника, впровадженні в його оточення неправдивої інформації. Непрямий – у створенні недостовірної інформації, яку ворог сприйме за правду. При цьому відсутнє внутрішнє втручання в інформаційне поле противника. І, нарешті, на стратегічному рівні інформаційна атака вважається успішною, якщо індивід не усвідомлює, що на нього вплинули.

Інформаційно-психологічна війна – це «протистояння сторін, яке виникає внаслідок конфлікту інтересів і здійснюється шляхом навмисного, в першу чергу вербального, впливу на свідомість противника (народу, колективного або індивідуального) з метою його пізнавального придушення і (або) підпорядкування, а також шляхом застосування заходів інформаційно-психологічного захисту від такого впливу.

Інформаційно-психологічна війна складається з комплексу заходів, що здійснюються в мирний і воєнний час, одним з яких є інформаційна атака. Здається, що вивчення метафори, що лежить в основі цього поняття, дозволить «розкрити» сутнісні властивості розглянутого явища. Сила метафори полягає в постійному балансуванні між сказаним і несказаним, між прямим і метафоричним значенням, в збереженні асоціативного потенціалу вихідної сфери при використанні метафори для характеристики предметів цільової сфери. У первинному називному значенні «напад» визначається: – як напад, найбільш рішучий етап наступу; швидке, безперервне і цілеспрямоване переміщення підрозділів, частин і з'єднань (окремих літаків, вертольотів, кораблів і їх груп) в бойовому порядку в напрямку противника в поєднанні з інтенсивним вогнем з метою його знищення; – швидке пересування в бойовому порядку підрозділів, частин, з'єднань, а також авіації, вертольотів, кораблів та їх угруповань у поєднанні з вогнем найвищої інтенсивності з метою знищення противника; – найбільш вирішальний період наступальних операцій.

Таким чином, атака – це атака, що характеризується як швидкий, безперервний, цілеспрямований, рішучий рух, спрямований на знищення противника. У метафоричному переосмисленні з урахуванням ракурсу даного дослідження є всі підстави розглядати інформаційну атаку як спланований (організований і цілеспрямований), масований (рішучий/стрімкий/нон-стоп) інформаційний вплив на адресата з метою формування громадської думки і поведінки відповідно до завдань організаторів нападу.

Для опису потенціалу впливу інформаційної атаки і детального розгляду її онтологічних властивостей використовується модель лінійної комунікації, розроблена Г. Лассуеллом і складається з «5W»: 1. Хто – відноситься до комунікатора, який формулює повідомлення; 2. Говорить що – зміст повідомлення; 3. Який канал – середовище передачі; 4. Хто – або окремий реципієнт, або аудиторія масової комунікації; 5. Який ефект – результат повідомлення + «ефект» також відноситься до зворотного зв'язку в зв'язках з

громадськістю. Відомо, що інформаційні атаки цілеспрямовано плануються та організовуються на державному рівні, у вищих ешелонах політичної влади.

Спектр інформаційних атак широкий. Вона охоплює політику, культуру, спорт, економіку, національну ідентичність та інші сфери людської діяльності. Аналіз змісту інформаційних атак представляє великий інтерес і стає предметом численних різнопланових досліджень в залежності від мети і методологічних установок того чи іншого вченого. З іншого боку, саме мова виступає в якості провідника для мисленнєвих структур. Найкращим доступом до свідомості є не тільки спостереження за об'єктно-пізнавальної діяльністю людини як такої, але це спостереження за мовою як формою відображення і вираження розумових процесів. Засоби масової інформації та Інтернет виступають каналом передачі інформаційної атаки, а також її зброєю. У сучасних умовах засоби масової інформації є потужним ресурсом впливу на свідомість людини. Засоби масової інформації, будучи невід'ємним, поширеним і дуже важливим елементом повсякденного життя у всіх економічно розвинених країнах світу, створили умови для появи принципово нових можливостей впливу на сприйняття і свідомість. Разом з тим, громадськість не розглядає ЗМІ як арену геополітичної боротьби, продовжуючи вважати його традиційним джерелом інформації, правдивою та незаангажованою.

При проведенні інформаційної атаки проявляються такі властивості, як «рішучість», «стрімкість», «нон-стоп», які полягають у масовому поширенні ворожої інформації по відношенню до ворожої країни. Масивність проявляється як на кількісному рівні, так і на якісному (змістовному) рівні. На кількісному рівні вона відображається в обсязі публікацій на одну і ту ж тему за певний проміжок часу, а на змістовному (якісному) рівні - в реалізації факту та/або оцінці події. Варто відзначити, що контент-аналіз дає важливий інструмент для дослідження інформаційної атаки, який дозволяє перевести вербальну інформацію в більш об'єктивну невербальну форму.

У деяких випадках інтенсивному періоду нападу передує так звана підготовча фаза, але за своєю руйнівною силою і глибині впливу вона не

поступається масованої. Інформаційна атака має як внутрішніх, так і зовнішніх адресатів, тому при її вивченні необхідно враховувати фактор множинності адресатів. Цей фактор передбачає спрямованість повідомлення як на внутрішнього, так і на зовнішнього адресата, що має на увазі використання різноманітних вербальних і невербальних ресурсів таким чином, що дозволяє побудувати цільову комунікацію. Внутрішнім адресатом інформаційної атаки є представники «своєї» мовної спільноти. На цьому етапі вона маскується під звичайну новинну статтю, що інформує громадськість про негативні явища та факти, що спостерігаються у ворожій державі. Цей квант інформації, виходячи за межі «свого» інформаційного простору і доходячи до зовнішнього адресата, тобто до держави-жертви, за своєю суттю стає інформаційною атакою. Як внутрішні, так і зовнішні адресати не є однорідними. Усередині кожної категорії можуть бути противники і прихильники. Спосіб розшифровки інформації адресатом багато в чому залежить від його (адресата) ідеологічних і культурних установок. Множинність адресата впливає на вибір вербальних і невербальних засобів, за допомогою яких буде здійснюватися цілеспрямований вплив. Тут ідеться про «кілька ліній поділу словесної аргументації» в межах одного повідомлення. Оскільки протиборчими сторонами є представники різних лінгвокультурних спільнот, особливий інтерес може представляти вивчення культурних кодів і знаків.

Розуміємо кібератаку, як будь-яку навмисну спробу викрасти, викрити, змінити, вивести з ладу або знищити дані, програми чи інші активи шляхом несанкціонованого доступу до мережі, комп’ютерної системи чи цифрового пристрою. Зловмисники починають кібератаки з різних причин, від дрібних крадіжок до військових дій. Вони використовують різні тактики, як-от атаки зловмисного програмного забезпечення, шахрайство соціальної інженерії та крадіжка паролів, щоб отримати несанкціонований доступ до цільових систем. А.Пехник та Ю.Завгородня розцінюють кібератаки, як «сучасну форму нападу, що досить вдало застосовується суб’єктами політики, переважно мається на увазі наддержавна форма взаємного впливу. Агресора можливо виявити, але

важко притягнути до будь-якої форми відповідальності, будь-які каральні форми впливу на міжнародній арені діють суб'єктивно, залежно від статусу на міжнародній арені такого політичного актора. Кібератаки, які використовуються під час проведення кібероперацій, можуть привести до дуже відчутних негативних наслідків». Наприклад, така атака, як вандалізм, «завдає удару по авторитету держави як у світі, так і серед населення, простими словами, завдає репутаційних втрат» [29].

Мотивація кібератак може бути різною, але існує три основні категорії: кримінальний; політичний; особистий. Для політичних процесів можуть використовуватися всі три типи мотивації.

Кримінально вмотивовані зловмисники прагнуть отримати фінансову вигоду через крадіжку грошей, крадіжку даних або зрив бізнесу. Особисто вмотивовані зловмисники прагнуть відплати за якусь образу. Політично вмотивованізловмисники асоціюються з кібервійною, кібертероризмом або «активізмом». У кібервійні суб'єкти національної держави часто атакують урядові установи чи критичну інфраструктуру своїх ворогів. Наприклад, з початку російсько-української війни обидві країни зазнали низки кібератак на життєво важливі установи Хакери-активісти, яких називають «хактивістами», можуть не завдати значної шкоди своїм цілям. Натомість вони зазвичай прагнуть привернути увагу до своїх причин, оприлюднюючи свої напади громадськості.

О.Запорожець виділяє когнітивне, соціальне та парасоціальне хакерство. Перше «проводиться з наміром таємно вплинути на аудиторію і не вимагає чіткого наративу». Прикладом є «поширення компрометуючої інформації про політика напередодні виборів, коли політик вже не має можливості відповісти на такий закид». Наступний вид направлений на «використання уразливостей, породжених племінною природою та схильністю людей до конформізму». Це може бути «схильність приймати на віру те, у що вірять інші; прагнення приєднатись до більшості». Третій вид «передбачає експлуатацію

парасоціальних, ілюзорних ідносин, які виникають, коли юди приймають односторонні відносини як двосторонні» [15].

Злочинні організації, державні суб'єкти та приватні особи можуть почати кібератаки. Один із способів класифікувати суб'єктів загрози – класифікувати їх як сторонніх або внутрішніх загроз. Зовнішні загрози не мають права використовувати мережу чи пристрій, але все одно проникають. Зовнішні суб'єкти кіберзагрози включають організовані злочинні групи, професійних хакерів, спонсорованих державою акторів, хакерів-любителів і хактивістів. Інсайдерські загрози – це користувачі, які мають авторизований і законний доступ до якись активів та зловживають своїми привілеями навмисно чи випадково. Хоча недбалі користувачі можуть наражати свої компанії на небезпеку, кібератака вважається лише тоді, коли користувач навмисно використовує свої права для здійснення зловмисної діяльності.

Кіберзлочинці використовують багато складних інструментів і методів, щоб почати кібератаки. Деякі з найпоширеніших типів кібератак включають:

–шкідливе програмне забезпечення – це зловмисне програмне забезпечення, яке може призвести до непрацездатності заражених систем. Зловмисне програмне забезпечення може знищити дані, викрасти інформацію або навіть видалити файли, критичні для роботи операційної системи. Зловмисне програмне забезпечення існує в багатьох формах, зокрема: «троянські коні» маскуються під корисні програми або ховаються в законному програмному забезпеченні, щоб обманом змусити користувачів встановити їх. Троян віддаленого доступу (RAT) створює секретний захід на пристрої жертви, тоді як троян-дропер встановлює додаткове шкідливе програмне забезпечення, коли має точку опори.

–Програми-вимагачі — це складні шкідливі програми, які використовують надійне шифрування, щоб утримувати дані або системи в заручниках. Потім кіберзлочинці вимагають оплату в обмін на звільнення системи та відновлення функціональності.

–Scareware використовує фальшиві повідомлення, щоб залякати жертв і змусити їх завантажити зловмисне програмне забезпечення або передати конфіденційну інформацію шахраям.

–Шпигунське програмне забезпечення – це тип зловмисного програмного забезпечення, яке таємно збирає конфіденційну інформацію, як-от імена користувачів, паролі та номери кредитних карток. Потім він надсилає цю інформацію назад хакеру.

– Руткіти — це пакети зловмисних програм, які дозволяють хакерам отримати доступ на рівні адміністратора до операційної системи комп'ютера чи інших ресурсів.

– Хробаки – це шкідливий код, що самовідтворюється, який може автоматично поширюватися між програмами та пристроями.

– Соціальна інженерія – ці атаки спонукають людей робити речі, які вони не повинні робити, як-от ділитися інформацією, якою вони не повинні ділитися, завантажувати програмне забезпечення, яке вони не повинні завантажувати, або надсилати гроші злочинцям.

Фішинг є однією з найпоширеніших атак соціальної інженерії. Відповідно до звіту Cost of a Data Breach, це друга за поширеністю причина порушень. Найпростіші фішингові шахрайства використовують фальшиві електронні листи або текстові повідомлення, щоб викрасти облікові дані користувачів, викрасти конфіденційні дані або розповсюдити зловмисне програмне забезпечення. Фішингові повідомлення часто створюються так, ніби вони надходять із законного джерела. Зазвичай вони спрямовують жертву натиснути гіперпосилання, яке переведе її на шкідливий веб-сайт, або відкрити вкладення електронної пошти, яке виявляється шкідливим програмним забезпеченням.

Кіберзлочинці також розробили більш витончені методи фішингу. Фішинг – це цілеспрямована атака, метою якої є маніпулювання конкретною особою, часто з використанням деталей із загальнодоступних профілів жертви в соціальних мережах, щоб зробити обман більш переконливим. Кітовий фішинг

— це тип стрімкого фішингу, спрямований спеціально на високопоставлених керівників компаній. У шахрайстві з компрометацією бізнес-електронної пошти (BEC) кіберзлочинці видають себе за керівників, продавців або інших ділових партнерів, щоб обманом змусити жертв перевести гроші або надати конфіденційні дані. Як зазначають автори дослідження інформаційних атак в соціальних мережах «якщо не брати до уваги прицільну атаку з метою завдання шкоди конкретній особі, здебільшого фішинг дуже нагадує риболовлю. Шахрай закидає цифрову вудочку і очікує, коли на неї клюне чергова жертва». Метою може бути як масштабування фішингової діяльності, так і фінансовий та розповсюдження комерційної реклами «за рахунок жертви». Як зазначають науковці, «основна причина ефективності фішингу – недостатня цифрова грамотність жертви або вразливий психоемоційний стан, викликаний різними обставинами. Основним типом фішингу, що поширювався в 2023 році, є шахрайські сповіщення» [22].

Атаки типу «відмова в обслуговуванні» - переповнюють ресурси системи шахрайським трафіком. Цей трафік перевантажує систему, перешкоджаючи відповідям на законні запити та знижуючи здатність системи працювати. Атака типу «відмова в обслуговуванні» може бути самоціллю або підготовкою до іншої атаки.

Різниця між DoS-атаками та DDoS-атаками полягає просто в тому, що DoS-атаки використовують одне джерело для створення шахрайського трафіку, тоді як DDoS-атаки використовують кілька джерел. DDoS-атаки часто здійснюються за допомогою ботнету, мережі підключених до Інтернету заражених шкідливим програмним забезпеченням пристроїв під контролем хакера. Ботнети можуть включати ноутбуки, смартфони та пристрої Інтернету речей (IoT). Жертви часто не знають, коли ботнет захопив їхні пристрої.

Компрометація облікового запису - Злом облікового запису – це будь-яка атака, під час якої хакери захоплюють обліковий запис законного користувача для зловмисної діяльності. Кіберзлочинці можуть зламати обліковий запис користувача різними способами. Вони можуть викрасти облікові дані за

допомогою фішингових атак або купити вкрадені бази даних паролів у темній мережі. Вони можуть використовувати такі інструменти для атаки паролів, як Hashcat і John the Ripper, щоб зламати шифрування паролів або влаштувати атаки грубої сили, під час яких вони запускають автоматизовані сценарії або ботів для генерації та перевірки потенційних паролів, доки один не запрацює.

Людина посередині атакує – під час атаки «людина посередині» (MiTM), яку також називають «атакою підслуховування», хакер таємно перехоплює зв'язок між двома людьми або між користувачем і сервером. Атаки MitM зазвичай здійснюються через незахищені публічні мережі Wi-Fi, де зловмисникам відносно легко шпигувати за трафіком.

Хакери можуть читати електронні листи користувача або навіть таємно змінювати електронні листи до того, як вони дійдуть до одержувача. Під час атаки з захопленням сеансу хакер перериває з’єднання між користувачем і сервером, на якому розміщені важливі активи, як-от конфіденційна база даних компанії. Хакер змінює свою IP-адресу на адресу користувача, змушуючи сервер думати, що це законний користувач, який увійшов у законний сеанс. Це дає хакеру повну свободу для крадіжки даних або іншим чином сіяти хаос

Атаки на ланцюги поставок – це кібератаки, під час яких хакери зламують компанію, націлюючись на її постачальників програмного забезпечення, постачальників матеріалів та інших постачальників послуг. Оскільки постачальники часто певним чином підключені до мереж своїх клієнтів, хакери можуть використовувати мережу постачальника як вектор атаки для доступу до кількох цілей одночасно.

Атаки міжсайтового сценарію (XSS) вставляють зловмисний код на законну веб-сторінку або веб-програму. Коли користувач відвідує сайт або програму, код автоматично запускається у веб-браузері користувача, зазвичай крадучи конфіденційну інформацію або перенаправляючи користувача на підроблений, шкідливий веб-сайт. Зловмисники часто використовують JavaScript для атак XSS.

Атаки SQL-ін’єкцій використовують мову структурованих запитів (SQL) для надсилання зловмисних команд до серверної бази даних веб-сайту чи програми. Хакери вводять команди через призначені для користувача поля, такі як рядки пошуку та вікна входу. Потім команди передаються в базу даних, спонукаючи її повертати приватні дані, такі як номери кредитних карток або дані клієнтів.

Тунелювання DNS приховує зловмисний трафік у пакетах DNS, дозволяючи йому обходити брандмауери та інші заходи безпеки. Кіберзлочинці використовують DNS-тунелювання для створення секретних каналів зв’язку, які вони можуть використовувати для тихого вилучення даних або встановлення з’єднань між зловмисним програмним забезпеченням і сервером керування (C&C).

Експлойти нульового дня використовують переваги вразливостей нульового дня, які є або невідомими спільноті безпеки, або ідентифікованими, але ще не виправленими. Ці вразливості можуть існувати протягом днів, місяців або років, перш ніж розробники дізнаються про недоліки, що робить їх основними цілями для хакерів.

Безфайлові атаки використовують уразливості в законних програмах для введення шкідливого коду безпосередньо в пам’ять комп’ютера. Кіберзлочинці часто використовують PowerShell, інструмент створення сценаріїв, вбудований в операційні системи Microsoft Windows, для запуску шкідливих сценаріїв, які змінюють конфігурації або викрадають паролі.

Атаки DNS-спуфінгу, які також називають «отруєнням DNS», приховано редагують записи DNS, щоб замінити справжню IP-адресу веб-сайту на фальшиву. Коли жертви намагаються відвідати справжній сайт, вони несвідомо потрапляють на шкідливу копію, яка викрадає їхні дані або поширює зловмисне програмне забезпечення.

Можна зменшити кількість кібератак шляхом впровадження систем і стратегій кібербезпеки. Кібербезпека – це практика захисту критично важливих систем і конфіденційної інформації від цифрових атак за допомогою комбінації

технологій, людей і процесів. Багато організацій реалізують стратегію управління загрозами, щоб визначити та захистити свої найважливіші активи та ресурси. Управління загрозами може включати такі політики та рішення безпеки, як:

- Платформи та політики керування ідентифікацією та доступом (IAM) , включаючи доступ з найменшими привілеями, багатофакторну автентифікацію та політики надійних паролів, можуть допомогти забезпечити доступ до потрібних ресурсів лише потрібним людям. Компанії також можуть вимагати від віддалених співробітників використовувати віртуальні приватні мережі (VPN) під час доступу до конфіденційних ресурсів через незахищений Wi-Fi.
- Комплексна платформа безпеки даних і інструменти запобігання втраті даних (DLP) можуть шифрувати конфіденційні дані, контролювати їх доступ і використання, а також подавати сповіщення при виявленні підозрілої активності. Організації також можуть регулярно створювати резервні копії даних, щоб мінімізувати шкоду в разі порушення.
- Брандмауери можуть допомогти заблокувати загрози від входу в мережу в першу чергу. Брандмауери також можуть блокувати зловмисний трафік, що витікає з мережі, наприклад зловмисне програмне забезпечення, яке намагається зв’язатися з сервером керування та управління.
- Навчання з питань безпеки може допомогти користувачам визначити та уникнути деяких із найпоширеніших векторів кібератак, таких як фішинг та інші атаки соціальної інженерії.
- Політики керування вразливостями , включаючи графіки керування виправленнями та регулярне рестування на проникнення, можуть допомогти виявити та закрити вразливості до того, як хакери зможуть ними скористатися.
- Інструменти керування поверхнею атак (ASM) можуть ідентифікувати, каталогізувати та виправляти потенційно вразливі активи до того, як їх знайдуть кібератакники.

- Інструменти уніфікованого керування кінцевими точками (UEM) можуть застосовувати політики безпеки та засоби контролю навколо всіх кінцевих точок у корпоративній мережі, включаючи ноутбуки, настільні комп'ютери та мобільні пристрої.

Неможливо повністю запобігти спробам кібератак, тому організації також можуть використовувати постійний моніторинг безпеки та процеси раннього виявлення, щоб ідентифікувати та позначати поточні кібератаки. Приклади:

- Системи безпеки та управління подіями (SIEM) централізують і відстежують сповіщення від різних внутрішніх інструментів кібербезпеки, включаючи системи виявлення вторгнень (IDS), системи виявлення кінцевих точок і відповіді (EDR) та інші рішення безпеки.
- Платформи аналізу загроз розширюють сповіщення безпеки, щоб допомогти командам безпеки зрозуміти типи загроз кібербезпеці, з якими вони можуть зіткнутися.
- Антивірусне програмне забезпечення може регулярно сканувати комп'ютерні системи на наявність шкідливих програм і автоматично знищувати виявлені шкідливі програми.
- Процеси проактивного пошуку загроз можуть відстежувати кіберзагрози, які таємно ховаються в мережі, наприклад, вдосконалені постійні загрози (APT).

Організації також можуть вживати заходів для забезпечення відповідної реакції на триваючі кібератаки та інші події кібербезпеки. Приклади:

- Плани реагування на інциденти можуть допомогти стримувати та викорінювати різні види кібератак, відновлювати уражені системи та аналізувати першопричини, щоб запобігти майбутнім атакам. Показано, що плани реагування на інциденти зменшують загальні витрати на кібератаки. Відповідно до звіту Cost of a Data Breach, організації з офіційними групами реагування на інциденти та планами мають у середньому на 58% нижчі витрати на порушення.

- Рішення з оркестровки безпеки, автоматизації та реагування (SOAR) можуть дозволити командам безпеки координувати різні інструменти безпеки в напів- або повністю автоматизованих посібниках для реагування на кібератаки в режимі реального часу.
- Рішення з розширеним виявленням і реагуванням (XDR) інтегрують інструменти та операції безпеки на всіх рівнях безпеки – користувачів, кінцевих точок, електронної пошти, програм, мереж, робочих навантажень у хмарі та даних. XDR можуть допомогти автоматизувати складні процеси запобігання кібератак, виявлення, розслідування та реагування, включаючи проактивний пошук загроз.

З позиції вчених А. Дудатьєва, Л. Куперштейна, О. Войтовича, «життєдіяльність сучасних великих соціотехнічних систем, які складаються з двох складових: технічної і соціальної частин, відбувається у конкурентному інформаційному просторі». Тому, на думку вчених, «інформаційна безпека таких систем загалом, зокрема держави, у великій мірі залежить від рівня захищеності соціуму. Спеціальні деструктивні інформаційно-психологічні операції, що проводяться проти соціальної складової соціотехнічної системи, переслідують головну мету інформаційного протиборства, а саме: зміну його стану, шляхом перепрограмування свідомості суспільства». Вчені визначають шляхи «реалізації спеціальної інформаційної операції» і вважають, що це «є використання спеціально підготовленої умовної одиниці інформації, наприклад мема, який поширюється в інформаційному просторі завдяки використанню різноманітних каналів впливу і виконує функцію фактично інфікування саме соціальної частини соціотехнічних систем». Дослідники визначити задачі, «які необхідно вирішити для досягнення мети деструктивного інформаційно-психологічного впливу та навели основні етапи підготовки та здійснення інформаційно-психологічної операції». Зокрема, автори розробили «структурну модель процесів при реалізації інформаційного протиборства та запропоновали модель реалізації спеціальної інформаційно-психологічної операції, яка побудована на базі формули Бернуллі і дозволяє отримати ймовірнісну оцінку

ефективної реалізації інформаційно-психологічної операції». Це дозволяє «отримати оцінку ефективності проведення спеціальної інформаційно-психологічної операції. Ефективність проведеної спеціальної інформаційно-психологічної операції оцінюється ймовірною кількістю елементів соціальної частини, яка під дією цього впливу змінила свій початковий стан, і, як наслідок, вся соціотехнічних систем вийшла зі стану рівноваги». Вчені пропонують ці моделі використовувати «при вирішенні задач прогнозування ризиків проведення спеціальних інформаційно-психологічних операцій і системи протидії деструктивним інформаційно-психологічним впливам» [14].

Соціальна кібербезпека, інтегруючи дослідження соціальних та поведінкових наук з кібербезпекою, спрямована на розуміння та протидію цим кіберопосередкованим загрозам, включаючи маніпулювання інформацією в нечесних цілях. Поява соціальної науки про кібербезпеку, орієнтованої на розробку наукових методів та оперативних інструментів для підвищення безпеки в кіберпросторі, підкреслює необхідність міждисциплінарних підходів для ефективного виявлення та пом'якшення кіберзагроз. Існує багато методів і фреймворків для аналізу стратегій і прийомів інформаційної війни. Однією з таких є SCOTCH – методологія швидкої оцінки операцій впливу. Він складається з шести елементів: джерело, канал, мета, ціль, композиція та гачок. Кожен з них відіграє вирішальну роль у загальній стратегії кампанії впливу. Джерело визначає ініціатора кампанії, Канал посилається на платформи та функції, що використовуються для поширення наративу, Мета – мета операції, Ціль визначає цільову аудиторію, Композиція – це конкретна мова, що використовується, а Хук – це тактика, яка використовується для використання технічних механізмів. У той час як SCOTCH забезпечує структурований підхід до характеристики операцій впливу, зосереджуючись на оперативних аспектах кампаній, фреймворк BEND пропонує більш тонке тлумачення соціально-кібер-маневрів. BEND класифікує маневри за типами спільноти та наративів, кожен з яких має позитивні та негативні аспекти, надаючи всебічне уявлення про те, як онлайн-актори маніпулюють соціальними мережами та наративами. Ця

структура особливо ефективна для аналізу тонкої динаміки операцій впливу в соціальних мережах, де характер комунікації є складним і багатошаровим. Таким чином, при обговоренні того, яку структуру використовувати, в той час як SCOTCH відмінно справляється з оперативною оцінкою, BEND пропонує краще розуміння соціальних і наративних аспектів операцій впливу, що робить їх більш придатними для аналізу складного характеру операцій інформаційної війни на основі соціальних медіа.

Основні тенденції та типи кібератак у 2024 році (на основі доступних даних):

- Фішинг (Phishing): Залишається найпоширенішим типом кібератак. Багато звітів вказують, що більшість атак починаються з фішингових електронних листів.
- Програмне забезпечення-вимагач (Ransomware): Продовжувало бути серйозною загрозою, особливо для критичної інфраструктури та великих організацій. Спостерігалося зростання складності таких атак, включаючи «Ransomware як послуга» (RaaS) та подвійне вимагання.
- Шкідливе програмне забезпечення (Malware): Різноманітні типи шкідливого ПЗ, включаючи трояни, віруси та шпигунське ПЗ, залишалися поширеними. Електронна пошта залишалася основним вектором розповсюдження шкідливого ПЗ.
- Атаки на веб-додатки (Web Application Attacks): Значна частина атак була спрямована на вразливості веб-додатків.
- Використання викрадених облікових даних (Stolen Credentials): Спостерігалося значне зростання атак з використанням викрадених облікових даних.
- DDoS-атаки (Distributed Denial of Service): Залишалися актуальною загрозою, особливо проти криптовалютних фірм, де спостерігалося значне зростання таких атак.

- Атаки на ланцюги постачання (Supply Chain Attacks): Хоча конкретна статистика може бути обмеженою, цей тип атак продовжував викликати занепокоєння.
- Інсайдерські загрози (Insider Threats): Залишаються важливим фактором ризику.
- Атаки, пов'язані зі штучним інтелектом (AI) та Інтернетом речей (IoT): З розвитком цих технологій зростали і пов'язані з ними загрози.

Кількісні дані з окремих звітів за 2024 рік:

- Більше 75% атак починаються з фішингового електронного листа.
- Більше 90% шкідливого ПЗ доставляється через електронну пошту.
- 17% атак спрямовані на веб-додатки.
- До 88% витоків даних спричинені людською помилкою.
- DDoS-атаки проти криптовалютних фірм зросли більш ніж на 600%.
- Атаки, що тривали понад три години, зросли на 103%.
- Використання викрадених облікових даних у атаках зросло на 71% у порівнянні з попереднім роком.
- У третьому кварталі 2024 року середньотижнева кількість кібератак на одну організацію зросла на 75% порівняно з аналогічним періодом 2023 року.
- Північна Америка була найбільш ураженим регіоном за кількістю ransomware-інцидентів (57%).
- Виробничий сектор був найбільш ураженою галуззю за кількістю ransomware-атак (30%).

Ці дані були сформовані на основі узагальнення інформації та тенденцій, які простежувалися у різних джерелах за період 2024 року та частково за попередні роки для розуміння загальної динаміки. До цих джерел належать:

- Новинні статті та публікації в галузі кібербезпеки: Протягом 2024 року з'являлися численні статті, що описували поточні загрози та інциденти, які вказували на домінування певних типів атак (наприклад, фішингу та ransomware).

- Блоги та аналітичні матеріали компаній, що займаються кібербезпекою: Багато компаній публікують проміжні звіти, аналітику та прогнози щодо кіберзагроз, які допомагають відстежувати тенденції.
- Дані з відкритих джерел про окремі інциденти: Інформація про великі кібератаки, що потрапляли в публічний простір, також давала уявлення про використовувані методи.
- Загальні знання про ландшафт кіберзагроз: Розуміння того, які типи атак історично були найбільш поширеними та ефективними, також впливає на оцінку.

Конкретні компанії та організації, чиї звіти та аналітику я враховував (хоча і не маючи повних річних даних за 2024 рік на момент запиту):

- Check Point: Їхні регулярні звіти про загрози часто дають уявлення про поточні тенденції.
- IBM (Security X-Force): Їхні звіти про вартість витоків даних та інші дослідження є цінними.
- Verizon (Data Breach Investigations Report - DBIR): Хоча DBIR зазвичай публікується пізніше, попередні дані та аналіз від Verizon часто відображають загальні тенденції.
- CrowdStrike (Global Threat Report): Їхні звіти також надають глибокий аналіз ландшафту загроз.
- Microsoft (Digital Defense Report): Містить інформацію про загрози, які спостерігаються в їхній екосистемі.
- Інші компанії та дослідницькі групи: Symantec (Broadcom), McAfee, Mandiant (Google Cloud), та інші.

Оскільки повних річних звітів за 2024 рік ще немає, представлена статистика є оціночною і відображає прогнозований розподіл на основі доступної на той момент інформації про тенденції. Після публікації повноцінних звітів від різних організацій у сфері кібербезпеки, реальний розподіл може відрізнятися.

Можна зробити висновок, що в сучасних умовах геополітичної нестабільності спостерігається тенденція до гібридизації інформаційних та кібернетичних атак. Ця конвергенція традиційних методів інформаційної війни (дезінформація, пропаганда) з новітніми кібертехнологіями (злам систем, DDoS-атаки) ускладнює атрибуцію джерела атаки та розробку ефективних стратегій протидії. Крім того, трансформація кіберпростору та соціальних мереж у ключові арени інформаційної боротьби призводить до експоненційного зростання масштабів маніпуляції громадською думкою.

Інформаційні атаки, окрім поширення недостовірної інформації, спрямовані на маніпулювання емоційно-ціннісними структурами індивідів та соціальних груп. Використання психологічних прийомів, таких як культивування страху, ненависті та недовіри, має на меті дезінтеграцію суспільства та дестабілізацію його функціонування. У цьому контексті соціальна кібербезпека набуває статусу критично важливого елементу захисту, оскільки вона забезпечує розуміння та протидію маніпулятивним практикам в онлайн-середовищі.

Інформаційно-кібернетичні атаки все частіше використовуються як інструменти геополітичної боротьби між державами. Їх метою є підрив економічної стійкості, політичної стабільності та військового потенціалу противника. Кіберпростір, таким чином, стає новим полем конфліктів, де розмиваються межі між традиційними поняттями війни та миру.

Експоненційний розвиток інформаційних технологій, включаючи штучний інтелект, Інтернет речей та хмарні обчислення, створює нові вектори кібернетичних атак. З іншого боку, зростаюча залежність суспільства від цифрової інфраструктури підвищує його вразливість до кібернетичних загроз.

Можна конкретизувати деякі новітні форми конфронтаційної поведінки суб'єктів політичного процесу в цифровому інформаційному просторі, що виходять за межі традиційних методів інформаційного впливу:

1. Використання автоматизованих систем для поширення наративів (ботоферми та мережі тролів): На відміну від традиційного ручного поширення

інформації, у цифровому просторі суб'єкти політики активно використовують ботів та скоординовані мережі тролів для штучного збільшення охоплення певних повідомлень, створення ілюзії масової підтримки або обурення, а також для придушення опозиційних думок шляхом масованих коментарів та атак на окремих користувачів.

2. Застосування технологій штучного інтелекту для генерації та аналізу контенту: ШІ може використовуватися для автоматизованого створення великих обсягів текстових та візуальних матеріалів (включаючи фейкові новини та пропагандистські меми), а також для аналізу інформаційного простору з метою виявлення вразливих аудиторій та оптимізації стратегій впливу. Це значно підвищує швидкість та масштабність інформаційних атак.

3. Маніпулювання алгоритмами соціальних мереж («algorithm hacking»): Суб'єкти політичного процесу намагаються впливати на алгоритми ранжування контенту в соціальних мережах для підвищення видимості своїх повідомлень та зниження видимості небажаного контенту. Це може включати використання специфічних ключових слів, організацію скоординованих лайків та поширень, а також інші тактики, спрямовані на обхід правил платформ.

4. Використання технологій «deepfake» для створення сфабрикованого аудіо- та відеоконтенту: Deepfake дозволяє створювати надзвичайно реалістичні підробки виступів політиків або інших публічних осіб, що може використовуватися для поширення дезінформації, компрометації опонентів та провокування суспільного резонансу.

5. Проведення скоординованих кампаній з «доксингу» та онлайн-цькування: Оприлюднення особистої інформації опонентів (доксинг) та організація скоординованих кампаній онлайн-цькування спрямовані на залякування, дискредитацію та виведення з інформаційного простору небажаних осіб.

6. Використання кібернетичних атак для порушення роботи інформаційних ресурсів та поширення дезінформації: Кібератаки на веб-сайти, соціальні мережі, бази даних та інші елементи інформаційної інфраструктури

можуть використовуватися не лише для виведення їх з ладу, але й для розміщення сфальсифікованої інформації або отримання конфіденційних даних.

7. Застосування методів соціальної інженерії для маніпулювання користувачами: Соціальна інженерія використовує психологічні маніпуляції, щоб змусити користувачів розкривати конфіденційну інформацію або здійснювати дії, вигідні атакуючій стороні (наприклад, переходити за шкідливими посиланнями, встановлювати шкідливе програмне забезпечення).

Ці новітні форми конфронтаційної поведінки в цифровому інформаційному просторі характеризуються підвищеною швидкістю поширення, масштабністю впливу, складністю виявлення та атрибуції, а також використанням передових технологій для досягнення політичних цілей. Вони становлять значну загрозу для демократичних процесів, національної безпеки та суспільної стабільності, що підкреслює актуальність дослідження цієї проблематики.

Ефективна протидія гібридним інформаційно-кібернетичним атакам вимагає інтегрованого підходу, що включає:

- розробку та впровадження технічних засобів захисту (брандмауери, антивірусне програмне забезпечення, системи виявлення вторгнень);
- розробку та імплементацію законодавчих та регуляторних актів;
- підвищення рівня інформаційної грамотності та медіа-освіти суспільства;
- активізацію міжнародної співпраці у сфері кібербезпеки.

Також необхідний постійний моніторинг кіберпростору та обмін інформацією про нові загрози.

Соціальні мережі стали потужним інструментом для поширення дезінформації та маніпуляцій. Алгоритми соціальних мереж можуть сприяти поширенню «бульбашок фільтрів», де користувачі бачать лише ту інформацію, яка підтверджує їхні переконання. Це створює сприятливе середовище для поширення фейкових новин та пропаганди.

В умовах інформаційної війни критичне мислення стає необхідною навичкою для кожного громадянина. Люди повинні вміти аналізувати інформацію, розрізняти факти та думки, виявляти маніпуляції та пропаганду. Інформаційна грамотність та медіа-освіта повинні стати пріоритетом для суспільства. Враховуючи ці розширені висновки, стає очевидним, що інформаційні та кібератаки є складними та багатогранними загрозами, які вимагають постійної уваги та розвитку нових методів протидії.

3.2. Цифрова пропаганда, як інструмент інформаційного протиборства.

Спроби маніпуляції в Інтернеті розвиваються від відносно нескладних «неорганічних» кампаній, які проштовхують боти соціальних мереж, до більш складних «напіворганічних» зусиль, що поєднують як скоординованих користувачів-людей, так і програмне забезпечення штучного інтелекту. Додаткові тенденції, які з цим повязані, включають збільшення примусового політичного використання впливових соціальних медіа та зашифрованих програм для обміну приватними повідомленнями.

А.Дудатьєв, Л.Куперштейн, О.Войтович зауважують, що саме «початок XXI сторіччя показує, що протиріччя, кількість яких збільшується, вирішується в більшості випадків нетрадиційними методами збройних протистоянь, а з використанням сучасних інформаційних технологій. Тобто переможець у протистоянні визначається за результатом проведення спеціальних операцій, що проводяться у інформаційному просторі, які, у свою чергу, розділяються на інформаційно-кібернетичні операції, що спрямовуються на технічну складову соціотехнічної системи та інформаційно-психологічні операції, що спрямовуються на соціальну складову СТС. Крім того, існує опосередкована залежність між проведеними ІПО і рівнем безпеки технічної складової СТС». Вчені говорять про те, шо «результатом проведення ефективної спеціальної інформаційної операції можуть бути «запрограмовані» дії для супротивника,

що можуть призвести до нестійкого стану всієї системи. В першу чергу, це актуально для систем управління, так званих «критичних систем»,зокрема енергетичних, транспортних, військових систем тощо. Спеціальні інформаційні операції є механізмом проведення інформаційного протиборства, головною метою якої є перепрограмування свідомості людини. Саме тому розробка аналітичної моделі розповсюдження інформаційних впливів у соціальній частині СТС є актуальною задачею» [14].

Слід погодитися з Н.Білоусовою, що «цифрові технології впливають на сутність пропаганди, стаючи каталізатором досягнення пропагандистських ефектів. Новітні цифрові технології активно використовують для ефективного поширення цифрового мистецтва як інструменту сучасної пропаганди у системі масових комунікацій» [6].

О.Свідерська розглядає пропаганду, «як інструмент впливу на громадянську свідомість, варто наголосити на двох особливостях: з одного боку вона має достатньо довгу історію, і ми сьогодні бачимо численні повідомлення про те, що російська пропаганда не ефективна або російська пропаганда є достатньо примітивною і власне ці наративи розслабляють і призупиняють українську боротьбу в інформаційному просторі, позаяк не варто недооцінювати російські методи управління масами» [35].

С.Янишевський відзначає, що «в сучасних умовах глобалізації та цифрової трансформації суспільства людина все більше і більше приділяє увагу соціальним мережам, телебаченню та інформаційним веб-сайтам. Саме ці чинники і обумовлюють інформаційний фронт, в якому розповсюджується пропаганда та дезінформація в нашому суспільстві» [44]. У більшості випадків цифрова пропаганда використовується як засіб боротьби з цифровим викривленням дискурсу, громадянського життя та політичної інформації. Замість фанатів ми бачимо фан-ботів, які залучаються до використання, створюючи хвилю думок, створюючи та підживлюючи односторонні наративи, які приховують джерело інформації, одночасно впливаючи (маніпулюючи) на тих, хто отримує цю інформацію. На думку І.Рущенка, «цифровізація соціуму

робить пересічну людину більш залежною від інформаційних інтервенцій, за якими стоять пропагандистські центри» [34].

Цифрова пропаганда – це ілюзія найвищого рівня. Для її існування не потрібні наміри чи конкретні інформаційні цілі, однак пропагандисти використовують техніку, щоб маніпулювати алгоритмами та «затопити зону» інформацією, щоб посіяти плутанину, створити недовіру та викорінити консенсус. Такі пропагандисти отримують вигоду від усіх форм неправдивої інформації, яка миттєво проникає у великі мережі людей в інформаційному просторі.

Алгоритмічні фільтри є одним із очевидних способів, як це відбувається. Більшість алгоритмів соціальних медіа було розроблено з метою комерційних стимулів, таких як залучення користувачів, підключення користувачів і зручності, не посилаючись на етичні міркування, такі як цінність інформації, заснована на правдивості. Алгоритмічно керовані обчислювальні мережі, зокрема у формі платформ соціальних медіа, мають безпрецедентну здатність посилювати, спотворювати, деконтекстуалізувати та сприяти вірі, незалежно від ефективності інформації, шляхом постійного повторюваного впливу. Крім того, ці алгоритми в просторі соціальних медіа, як правило, посилюють когнітивне упередження, пов’язане з вибірковим впливом та створюють безперервне генерування хибного консенсусу, особливо коли алгоритм починає ізолювати людину всередині її власної специфічної інформаційної ехокамери.

Постійні зусилля росії створити плутанину та хаос у соціальних мережах для досягнення своїх цілей свідчать про систематичні маніпуляції, які вони застосовують. Наприклад, під час кримської кризи 2014 року росія використовувала широку мережу ботів і тролів для заповнення соціальних медіа проросійськими настроями, поширюючи дезінформацію про ситуацію в Україні та формуючи наратив, що виправдовує анексію Криму. Ця стратегія ілюструє принципи соціальної кібербезпеки, які зосереджені на розумінні та прогнозуванні змін у поведінці людей, опосередкованих кіберпростором, а також на соціальних, культурних і політичних наслідках таких змін.

В умовах зниження міжнародного престижу росія використовує ситуативний підхід, що ґрунтується на старанності, скрупульозно використовуючи вразливі місця на свою користь. Такий підхід демонструє російське агентство інтернет-досліджень (IRA), відоме своєю роллю в операціях онлайн-впливу. IRA ретельно розробляє повідомлення, адаптовані до конкретної аудиторії, і використовує аналітику даних для максимізації впливу своїх кампаній, тактика, яка узгоджується з методологіями, що використовуються в соціальній кібербезпеці для аналізу цифрових відбитків пропагандистських кампаній, керованих державою.

Кампанії інформаційних операцій росії проти України є значною зміною в їх стратегії ведення війни, а дезінформаційні кампанії стають невід'ємною частиною їхніх військових операцій. Розвиток російської «доктрини герасимова», яка наголошує на ролі психологічної війни, кібероперацій та кампаній з дезінформації, знаменує цей новий зсув у їхній військовій стратегії. Ця доктрина наголошує на важливості невійськових тактик, таких як кампанії з дезінформації, для досягнення стратегічних військових цілей. росія постійно збільшує використання кібервійни у своїх військових цілях, використовуючи платформи соціальних мереж для поширення своїх цілей за допомогою дезінформаційних кампаній для контролю громадської думки. За допомогою стратегій, керованих ботами, росія прагне поляризувати громади та нації, дестабілізуючи політичну стабільність і водночас підриваючи демократичні цінності під виглядом дезінформаційних операцій.

Для виявлення активності ботів було використано BotHunter, інструмент, який спеціально розроблений для виявлення та аналізу мережі ботів, які відіграли ключову роль у поширенні цієї підтримки. Цей контрнаратив, що випливає з даних і формується діалогами, керованими ботами, є важливим аспектом загальної реакції на конфлікт. Інтегруючи наступне: фреймворк BEND для аналізу стратегій інформаційної війни, моделювання доменної мови TweetBER та моральний компас, наданий теорією моральних засад, з ідеями соціальної кібербезпеки – це все забезпечує можливість розуміння стратегічних

наративів та контрнаративів після конфлікту. Тому, детальний аналіз того, як ці наслідки впливають на геополітичну стабільність та окреслення методів за допомогою яких наративи – є важливими в сучасній політичній ситуації.

Наполегливі зусилля росії створити плутанину та хаос у соціальних мережах для досягнення своєї мети є свідченням систематичних маніпуляцій, які вони використовують. Наприклад, під час кримської кризи 2014 року росія використовувала розгалужену мережу ботів і тролів, щоб наповнювати платформи соціальних мереж проросійськими настроями, поширюючи дезінформацію про ситуацію в Україні та створюючи наратив, який виправдовує анексію Криму. Ця стратегія є прикладом принципів соціальної кібербезпеки, які зосереджені на розумінні та прогнозуванні кіберопосередкованих змін у поведінці людей, а також соціальних, культурних та політичних наслідків. В умовах зниження міжнародного престижу росія використовує ситуативний підхід, що ґрунтується на старанності, скрупульозно використовуючи вразливі місця на свою користь. Такий підхід демонструє російське Агентство інтернет-досліджень (IRA), відоме своєю роллю в операціях онлайн-впливу. IRA ретельно розробляє повідомлення, адаптовані до конкретної аудиторії, і використовує аналітику даних для максимізації впливу своїх кампаній, тактика, яка узгоджується з методологіями, що використовуються в соціальній кібербезпеці для аналізу цифрових відбитків пропагандистських кампаній, керованих державою.

Російська тактика дезінформації значно еволюціонувала за останні кілька років, особливо після вторгнення в Грузію в 2008 році. Тактика посилилася під час анексії Криму в 2014 році і енергійно продовжувалася протягом поточних конфліктів в Україні та Сирії. Ця тактика є не лише продовженням методів часів холодної війни, але й використовує широкі можливості сучасних технологій та засобів масової інформації. Цифровий ландшафт став благодатним ґрунтом для розгортання росією цілого ряду пропагандистських інструментів, включаючи стратегічне використання ботів, які створюють шум і поширюють дезінформацію в безпрецедентних масштабах. Спосіб дії

російської дезінформації влучно назвали «вогняним шлангом брехні», що характеризується великим обсягом і багатоканальним розповсюдженням. Цей підхід використовує величезну кількість повідомлень і використовує ботів і платних тролів для збільшення їхнього охоплення, не лише для того, щоб підірвати інформаційний простір, але й для створення значного виклику геополітичній стабільності. Наповнюючи платформи соціальних медіа шквалом наративів, росія гарантує, що деякі з її меседжів залишаться в тоні, навіть якщо вони суперечливі або не мають прихильності до об'єктивної реальності. Цей невпинний потік контенту покликаний не просто переконати, а заплутати та пересилити аудиторію, ускладнюючи відрізнення фактів від вигадки, демонструючи, як наративи можуть бути використані як зброя для створення розколу.

Більше того, ця тактика експлуатує психологічні основи переконань і сприйняття. Частота, з якою повідомлення зустрічається, підвищує його сприйняту достовірність, незалежно від фактичної точності. Російські боти сприяють цьому ефекту, постійно публікуючи, повторно публікуючи та посилюючи контент, тим самим створюючи ілюзію консенсусу чи підтримки точок зору. Ця стратегія ефективно контролює громадську думку, сприяючи поширенню кампаній з дезінформації, ілюструючи здатність того, як наративи можуть підривати демократичні цінності та геополітичну стабільність. Російські зусилля з дезінформації продемонстрували відсутність прихильності до послідовності, часто транслюючи суперечливі повідомлення, які можуть здатися неінтуїтивними для ефективної комунікації. Однак ця непослідовність може бути тактикою, оскільки вона може призвести до невизначеності та двозначності, що зрештою підірве довіру до надійних джерел інформації. Постійно змінюючи наративи, російські пропагандисти виводять опонентів з рівноваги та створюють туман війни, який маскує правду. Ця стратегія наголошує на подвійній ролі наративів у геополітичних конфліктах, які слугують щитом єдності для власного політичного порядку денного та водночас є зброєю розколу проти супротивників. Використання ботів у цій

військовій кампанії є особливо винахідливим, оскільки вони можуть працювати цілодобово, імітувати людську поведінку та взаємодіяти з реальними користувачами. Ці боти запрограмовані на наступне: пропагування російських наративів, атаки на протилежні точки зору та роздмухування видимості підтримки знизу. Вони є ключовим компонентом стратегії росії зі структурування громадської думки та впливу на політичні результати.

Просування російської тактики дезінформації являє собою складне поєднання традиційних стратегій впливу та використання сучасних технологічних інструментів. росія розробила потужний підхід для просування пропагандистських наративів, використовуючи ботів, платформи соціальних мереж і вразливі місця людської психології. Міжнародне співтовариство, прагнучи протистояти цій тактиці, має розуміти загрозу, яку вона становить, і розробляти комплексні стратегії захисту від потоку дезінформації, який підриває демократичні процеси та геополітичну стабільність.

Інформаційна війна в соціальних медіа – це стратегічне використання соціально-кіберманеврів для впливу, маніпулювання та контролю наративів і спільнот в Інтернеті. Він використовується для маніпулювання громадською думкою, поширення дезінформації та створення дискурсів, що викликають розбіжності. Ця форма ведення війни використовує складні стратегії для використання взаємопов'язаної природи соціальних мереж і схильності користувачів споживати та ділитися контентом, який відповідає їхнім існуючим переконанням. Стратегія «управління трендом» у соціальних медіа передбачає використання алгоритмів для посилення конкретних повідомлень або наративів. Це досягається шляхом використання існуючих онлайн-мереж, використання облікових записів ботів для створення тренду або повідомлень, а потім швидкого поширення цього наративу. Така позиція експлуатує природну схильність до гомофілії – схильність індивідів асоціюватися і зближуватися з іншими на схожі теми. Платформи соціальних мереж дозволяють це зробити, створюючи ехо-камери, де користувачі-однодумці діляться та підсилюють погляди один одного.

Отже, коли наратив, який є дезінформацією, узгоджується з вже існуючими переконаннями користувача, він, швидше за все, приймається та поширюється в цих мережах росія ілюструє ефективне використання соціальних медіа в інформаційній війні там, де вони використовували їх для пропаганди в соціальних мережах, створюючи дискурс і плутанину, а також маніпулюючи як прихильниками, так і супротивниками за допомогою цілеспрямованих повідомлень. Мета полягає в тому, щоб експлуатувати існуючі соціальні та політичні розбіжності, посилювати та поширювати неправдиві наративи з метою маніпулювання громадською думкою та дискредитації усталених інституцій та людей.

Наприклад, якась платформа використовується для інформаційної війни, де різні суб'єкти розгортають ботів для контролю наративів. У цьому контексті тематичне моделювання стає потужним інструментом у розумінні швидкого і часто хаотичного поширення ідей та думок по мережі. Процес моделювання включає в себе кілька етапів. Першим кроком є збір даних, що включає твіти, в яких обговорюються ключові події та заяви, пов'язані з дослідницьким питанням. Потім нам потрібно провести попередню обробку очищення даних шляхом видалення шумів, включаючи стоп-слова, URL-адреси та згадки користувачів, щоб допомогти зосередитися на контенті, який безпосередньо стосується дослідницького питання, в даному випадку російсько-української війни. Потім нам потрібно провести векторизацію – процес перетворення попередньо обробленого тексту в числову форму, яка може бути використана статистичними моделями. Наступним кроком є застосування таких алгоритмів, як латентний розподіл Діріхле (LDA) для виявлення тем. Для кожної теми характерний розподіл слів, що виділяють теми, пов'язані з нашими дослідженнями. Важливо, щоб теми були не тільки статистично обґрунтованими, але й контекстуально релевантними подіям.

А.Біденко вказує на виклики, які на сучасному етапі нас чекають: «… картинки несуть сильніші повідомлення, ніж тексти. Тож стає критично аналізувати різні форми даних, і ефективно це можуть робити винятково

складні програмні комплекси». Цитований автор вказує, що «логічність, пояснюваність – бажана ознака системи виявлення пропаганди, адже важливо, щоб подальші дії влади мали під собою чіткі цифри та роз'яснення і не наражалися на критику. І це теж дають алгоритми, а не людські оцінки. Сьогодні навіть спеціально навчена людина не завжди може відрізнити синтетично створений текст. Тож для детекції дезінформації потрібні кількісні методи збору великих даних, які оперують не тільки контентними критеріями» [4]. А. Біденко доводить, що «автоматизація дозволить вирішити проблему захисту даних та цензури, адже виключить вплив людей, політиків на фінальні звіти. З цією метою, звичайно, необхідно, щоб сам програмний продукт створювався за участі консорціуму незалежних організацій» [4].

І.Рущенко робить висновок, з яким можна погодитися, що «реінституціоналізація пропаганди й контрпропаганди відбувається в контексті гібридних війн, до сценарію яких на сьогодні втягнуто більшість провідних країн світу. Конкуренти західної цивілізації кинули виклик світовому порядку й міжнародному праву. Інформаційна війна є боротьбою за думки людини, вона ведеться тихо, без пострілів, але систематично з використанням усього наявного технічного спектру. Цифровізація соціуму робить пересічну людину більш залежною від інформаційних інтервенцій, за якими стоять пропагандистські центри. Держави більше не можуть контролювати свої кордони, аби розмежувати інформаційні й віртуальні простори на внутрішні й зовнішні. Глобалізація на тлі цифрової революції породжує ризик оголеної свідомості, яким користуються в злочинних цілях конструктори пропаганди 2.0. Захист свідомості бачиться через щеплення інфоімунітету, поширення медіа грамотності, збільшення резистентності пересічних громадян» [34]. Вчений акцентує увагу на тому, що подальші «дослідження явища пропаганди і контрпропаганди у сучасному світі мають зосереджуватися на кількох об'єктах – стані масової свідомості в умовах інформаційної війни нового покоління та ефективності пропагандистських впливів різного технологічного змісту, роль нових медіа та інтернет-комунікацій як трансляторів пропагандистських

меседжів, методологія поширення інфо-імунітету на молодь та інші соціальні групи» [34].

Україна посилила свою інформаційну та медійну стійкість, запровадивши заходи протидії російським наративам, включаючи поширення правдивої інформації та регулювання діяльності відомих афілійованих з росією ЗМІ. Щоб зрозуміти складність кампаній інформаційної війни та контрнаративи до цих кампаній, це дослідження вивчає вплив цих стратегій, керованих ботами, на платформи соціальних медіа. Важливим є використиння поєднання аналізу настроїв, моделювання тем, динаміки мережі та аналізу інформаційної війни, інтегрованого з принципами соціальної кібербезпеки, щоб зрозуміти важливі теми та вплив, який спільноти ботів мають на різні такі платформи.

Розглянуті раніше парадигми деструктивізму в цифровому світі накладають негативний відбиток на інформаційне суспільство і часто призводять не тільки до міграції в онлайн-медіа, але сприяють перетворенню найактивніших користувачів в інформаційних біженців. Вище ми розглянули інформаційний простір з цілим рядом проблем, які є більш складними, ніж живі універсальні риси сучасного суспільства, і мають свою, специфічну природу. Однією з таких особливостей і труднощів є можливість різноманітності ідентичності суспільства і особистості в інформаційному просторі. У зв'язку з цим звернемося до процесу ідентифікації за допомогою інтернет-засобів масової інформації, на основі робіт Г. В. Лейбніца, С. Хантінгтона, Д. Дьюї та ін. Так, Г. В. Лейбніц у своїх працях вводить термін «ледачий софізм» або «ледачий розум». Філософ розмірковує про помилкові судження і небажання мислити, порівнюючи таких людей з дітьми, які «ганяються за найменшою чуттєвою насолодою теперішнього моменту».

Феномен «ледачого софізму» з розмиттям людської ідентичності в інформаційному середовищі має на увазі вибір на користь свідомого омани, в якому сучасний користувач схильний до афективних імпульсів. Праця С. Хантінгтона «Зіткнення цивілізацій» може допомогти у вивченні процесів визначення ідентичності та плавної зміни сучасностей. Наприкінці XX століття

С.Хантінгтон передбачив цифровий перехід, при якому геополітичний розкол між країнами призведе до зміни ідентичності. У зазначеній роботі С. Хантінгтон розмірковує про окремі регіони, культури, нації та вплив на них світових воєн. Автор переконаний, що саме війни формують ідентичності, на прикладі «холодної війни» визначає місце культур у світовій політиці та дає чіткий поділ на друзів та ворогів. На тлі структури армії (роти, полки, дивізії) людина може ототожнювати себе зі своїм кланом, етнічною групою, національністю, релігією і цивілізацією, С. Хантінгтон також вводить три умови формування політики ідентичності [47]. Слід зазначити, що позиція С. Хантінгтона щодо тісного взаємозв'язку війни та ідентичності суспільства чітко характеризує сучасні цифрові тренди.

Сучасне цифрове суспільство перебуває в досить складному стані, вихід з якого передбачає пошук сил для звільнення від пороків і гніту (цензури, пропаганди, монополізму тощо). Але знову можна прийти до висновку, що страждає не сам інформаційний простір, а люди всередині нього. «Зрілі» користувачі всесвітньої мережі сьогодні визначилися зі своєю особистістю, вони збираються невеликими групами в соціальних мережах і обговорюють цікаві для них теми.

На думку А.Біденко. «Fake news – невдовзі стануть неактуальні, неефективні та нецікаві. Як і фейкові експерти, фейкові організації, фейкові дослідження. Це все будуть забавки для підлітків і політтехнологів-початківців. Невдовзі реальний вплив на порядки денні країн, спільнот і індивідів отримає цифрова або обчислювальна пропаганда. Поєднання обчислювальних можливостей комп’ютерів, швидкості опрацювання інформації, big data – і потреби маніпулювати сенсами» [4].

Ми перебуваємо в складний період інформаційної епохи. Радість від доступності знань поступово змінюється розгубленістю через велику кількість інформаційного сміття. Інтернет та хмарні технології, які спочатку відкривали безмежні можливості для розвитку, перетворилися на болото з псевдонауковими новинами про лікування раку за допомогою часнику, соди та

алое. З'явилися банальні цитати про саморозвиток, реклама непотрібних товарів, теорії змови, фотошоп та діпфейки. З цим викликом сьогодні стикаються всі дослідники — критичне мислення не можна сформувати лише за допомогою лекцій та онлайн-вікторин.

Як правильно вказує І.Рущенко. «за останні роки відбулися технічні революції й виникли нові можливості для пропаганди й ведення інформаційних війн у більш широкому сенсі. Нові медіа, засновані на технічних можливостях інтернету й мобільного зв’язку, остаточно скасовують державні кордони в інформаційному й кіберпросторах. В умовах цифрового суспільства теоретично кожна людина може бути охопленою повноцінним пропагандистським впливом у режимі мультимедіа: отримувати ідеологічний контент у формі текстів, фото, відео. І чим вищим є рівень діджиталізації, тим вищою є потенційна ефективність пропагандистської роботи в інтернеті, в соціальних мережах» [34].

Як і в Середньовіччі, нові технології використовуються різними групами інтересів (країнами, спільнотами, окремими особами), які прагнуть поширити хаос будь-якою ціною. Для України, зокрема, існує конкретний ворог – росія, яка витрачає величезні ресурси на те, щоб перетворити наше інформаційне середовище на смітник. Для цього застосовуються різноманітні методи — від оперативних (коли просто «зливають» блогерів) до створення мемів, в які вшиваються потрібні смисли (особливо для роботи з молоддю).

Зараз ми перебуваємо на певному технологічному зламі. На зміну креативності, індивідуальним рішенням і геніям пропаганди приходять бездушні машинні алгоритми, які працюють з величезною кількістю користувачів одночасно, розподіляючи їх на кластери, використовуючи їхню приватну інформацію та перетворюючи їх на цільові аудиторії. Одним – соду та часник, іншим – меч Людоти, а комусь – Трипілля як основу цивілізації.

Фейкові новини в традиційному розумінні – це щось на кшталт «розіп'ятого хлопчика»: вигадана інформація, що поширюється в медіа завдяки нахабству та абсурдності, а також великим фінансовим вливанням. Звісно, є

люди, які можуть повірити в такі новини і сьогодні, але їхня кількість зменшується, і вплив таких новин є короткостроковим. Покоління Інтернету швидко навчилося розпізнавати та висміювати подібний абсурд, створюючи альтернативні меми та зводячи всі зусилля на нівець.

Тим часом цифрові пропагандисти діють зовсім інакше. Вони збирають дані про свої цільові аудиторії, максимально сегментуючи їх на різні групи. Історія Cambridge Analytica — це не лише про виборчі гасла; це також про те, кому сподобається зображення Курта Кобейна, а кому – Алли Пугачової. Потім у так званий програмний «чорний ящик» закладаються потрібні слова та сенси, а алгоритми перетворюють їх на різні формати повідомлень для кожної групи. Наприклад, для молоді це можуть бути тисячі згенерованих мемів з їхніми улюбленими персонажами та фразами, які формують певне ставлення до подій. Для старшого покоління – статті про здоров'я з ненав'язливими описами бажаних емоцій (зневіра, депресія, агресія).

Звісно, існує певна термінологічна дискусія щодо визначення терміну «бот». В українських медіа ботоферма означає технологію, за якою стоїть реальна людина, що створює 15-20 різних фіктивних профілів, використовуючи телефонні картки та підроблені паспорти. Вона послідовно заходить на ці профілі, пише статуси, коментарі, ставить лайки – з метою донести певну думку. Вся активність фіксується в таблиці та передається замовнику у вигляді звіту: щомісяця кілька тисяч коментарів з необхідною інформацією.

Для західних дослідників і медіа ботоферма – це «матриця». Це машинний алгоритм, який перетворює роботу реальної людини на другорядну. Комп'ютер може зареєструвати десятки тисяч профілів, генеруючи імена, паспортні дані та використовуючи згенеровані телефонні номери. Ці профілі функціонують у визначених кластерах, генеруючи мільйони повідомлень, лайків та хештегів. Хоча якість таких дій не зрівняється з активністю живої людини, кількість у цьому випадку є перевагою, оскільки вона може обманювати алгоритми соціальних мереж, які мають свої механізми відображення коментарів, лайків тощо. Сьогодні автоматизовані системи є

найбільш ефективними для формування трендів (тобто порядку денного), тиску на опонентів, заспамлення повідомлень або створення негативу.

«Наприклад, з поверненням путіна до президентства в 2012 році російська державна пропаганда стала жорсткішою та агресивнішою, а боти виявилися значно ефективнішим інструментом. Коли мета полягає в блокуванні альтернативних думок, а не в їх залученні до дискусії, кількісні атаки ботів мають перевагу. Російські пропагандисти почали використовувати методи цифрової пропаганди для впливу на баланс думок у соціальних мережах по всьому світу, просуваючи контент або формуючи списки трендів.

Вони відіграли свою роль, зокрема під час виборів у США 2016 року, коли розгорнулася так звана теорія Піццагейту – про нібито викрадення та вбивство дітей демократами в піцеріях. Величезна кількість фальшивих профілів у Twitter поширювала графічні меми на цю тему, формуючи негативне ставлення до Хілларі Клінтон. Ці профілі були розташовані по всьому світу – на Кіпрі, в Чехії, В'єтнамі, і більшість з них діяли автоматизовано. Одним із методів, які вони використовували, було застосування позитивних хештегів у негативних повідомленнях про опонента. Таким чином, навіть прихильники Клінтон отримували в своїх стрічках лише негативну інформацію.

Звісно, боти поки що не здатні спілкуватися з реальними людьми на достатньому рівні. Проте ми повинні усвідомити, що це лише питання часу, розвитку штучного інтелекту та створення достатньої кількості сценаріїв для взаємодії з 99% співрозмовників.

Методи обчислювальної пропаганди постійно вдосконалюються і все більше імітують людську поведінку. Сьогодні світова тенденція до їх виявлення зосереджена не на аналізі контенту, а на аналізі похідних даних. Критичними для системи є не окремі гравці, які створюють маніпулятивний контент, а ситуація, коли велика кількість профілів починає діяти скоординовано, поширюючи подібну інформацію. Отже, необхідно проводити аналіз великих даних — регіональних, кластерних, фінансових тощо. Це не може бути класичний контент-аналіз, який здійснюють 30 аналітиків у науковому

інституті. Перш за все, це має бути програмний інструмент, здатний узагальнювати великі обсяги даних і виявляти відповідні тенденції. Ці тенденції вже можуть слугувати основою для ухвалення рішень керівниками.

Аналіз групової поведінки, а не контенту окремих осіб, є основною характеристикою сучасної боротьби з дезінформацією. Цей підхід ґрунтується на тому, що поведінка живих людей є більш різноманітною і менш структурованою, ніж у ботів. Саме такий підхід сьогодні вважається пріоритетним серед дослідників у багатьох країнах. Існує брак медіаграмотності, недостатня кількість аналітиків і обмежені ресурси для моніторингу інформаційного простору. Необхідні програмні рішення, які поєднують можливості штучного інтелекту, розвитку мереж і роботи з великими даними. Фактично, потрібно створити боти для протидії іншим ботам. Наприклад, вже згадувалася система Botometer, яка виявляє соціальні боти в Twitter, аналізуючи понад 1200 характеристик профілю і з високою ймовірністю визначаючи, чи є за ним жива людина.

Так, учасники європейського проекту SOMA працювали над системою Truly Media, яка може верифікувати інформацію за сотнями критеріїв, більшість з яких не пов'язана з контентом. У Тайвані в 2016 році був запущений бот 真的假的 (перекладається як «та невже?»), метою якого є виявлення фейкових новин. Користувач надсилає йому посилання, а бот повертає його з коментарями щодо змісту. Хоча бот все ще розробляється, він вже здобув популярність у місцевих медіа.

Таким чином, стають безальтернативними виклики, які свого часу окреслили дослідники Оксфордського інституту інтернету: текст давно перестав бути єдиним способом поширення пропаганди. Зображення набуває характеристики, які дають можливість сильніше впливати на аудиторію. Тому критично важливо аналізувати різні форми даних, і це можуть ефективно робити лише складні програмні системи; логічність і пояснюваність є бажаними характеристиками системи виявлення пропаганди, оскільки важливо, щоб подальші дії влади (наприклад, блокування певних сайтів) мали чіткі

цифри та пояснення, щоб уникнути критики. Це також забезпечують алгоритми, а не людські оцінки.

Сьогодні навіть спеціально навчена людина не завжди може відрізнити синтетично створений текст. Тому для виявлення дезінформації потрібні кількісні методи збору великих даних, які враховують не лише контентні критерії. Часто важливіше знати «хто, коли і в яких профілях написав», ніж «що саме було написано»

Автоматизація допоможе вирішити проблему захисту даних та цензури, оскільки усуне вплив людей і політиків на остаточні звіти. Для цього, звісно, важливо, щоб програмний продукт розроблявся за участю консорціуму незалежних організацій, включаючи міжнародні, з формуванням Наглядової ради та дотриманням чітких стандартів захисту приватної інформації.

Об'єднання зусиль різних організацій, дослідницьких груп і центрів ухвалення рішень дозволить залишити суперечки в минулому та створити інструменти, які спростять виявлення дезінформації і захистять суверенітет країн.

Розглядаючи пропаганду як інструмент впливу на громадську свідомість, варто підкреслити дві важливі особливості: по-перше, вона має досить тривалу історію, і сьогодні ми часто чуємо заяви про те, що «російська пропаганда неефективна» або «російська пропаганда є досить примітивною». Ці наративи можуть розслабляти та зупиняти українську боротьбу в інформаційному просторі, адже не слід недооцінювати російські методи «управління масами».

Як вказує О.Свідерська, більшість населення росії «не усвідомлює всього, що відбувається зараз на території України, не намагається зупинити своє політичне керівництво у спробі повністю знищити Україну. Більше того, бере активну участь у просуванні наративів про спорт поза політикою,«культура поза політикою, церква московського патріархату поза політикою і т. д.». Вчена доводить думку, що «саме російська пропаганда породила у частини населення України негативні образи бандерівців, хунти, думку про те, що за російську мову вбивають і багато інших, у ці ж вигадки вірять і громадяни рф» [35].

Дійсно, російська пропаганда стала джерелом наративів, таких як «війна з пам'ятниками», «один народ», «ми ж брати», «кровожерливий Захід», «соросята» та «порохоботи». Ситуація з пандемією Covid-19, хоч це і звучить дивно, лише сприяла закріпленню в українському та російському контенті уявлень про «натівські лабораторії» та «прахи, здатні переносити віруси». Як інструмент політичного маніпулювання, пропаганда націлена на внутрішню мотивацію та емоційно чутливі сфери особистості. Розвиток інформаційного суспільства та поява соціальних мереж, подібно до друкарства, радіо чи телебачення, сприяють швидкому поширенню пропагандистської інформації, яка є стратегічно важливим елементом спеціальних психологічних операцій. Медіа, що транслюють таку інформацію, здатні фактично конструювати нову політичну реальність.

На думку прихильників пропаганди, її основним завданням є створення певного сталого образу чи норми без спотворення, з подальшим уточненням і впровадженням у маси, не допускаючи нерозуміння на індивідуальному, локальному або груповому рівні. Схожу процедуру описував Дж. Орвелл у «Колгоспі тварин», де принцип «всі тварини рівні» одного дня перетворився на «всі тварини рівні, але деякі рівніші». Теза Путіна про те, що росія проводить превентивну «військову операцію» проти України, оскільки, за його словами, Україна готувалася до нової «каральної операції на Донбасі» та «вторгнення» на російські «історичні території», зокрема Крим, могла б бути досить успішною. Доказом цього є анексовані території Донецької та Луганської областей, а також Крим, які росія вважає споконвічно своїми, хоча насправді вони ніколи не були російськими, за винятком окупаційних періодів. Водночас, у заявах світових лідерів чуємо, що сьогоднішньої війни не було б, якби у 2014 році повірили Україні, а не путінським наративам про «громадянську війну на Донбасі», «українську хунту», «розп'ятих хлопчиків» тощо. Проте в 2014 році Україна не була готова ані до збройного протистояння, ані до інформаційного. За ці роки в українському суспільстві відбулися важливі зміни в готовності протистояти інформаційним фейкам та дезінформації. Численні проекти з

фактчекінгу, навчання з медіаграмотності, впровадження відповідних курсів у системі освіти на різних рівнях та розвиток критичного мислення підвищили здатність розрізняти фейки та споживати інформацію лише з перевірених і офіційних джерел.

Індивідуальне сприйняття пропаганди значною мірою залежить від особистісних характеристик людини. Те, що викликає страх у одних громадян і змушує їх залишати свої домівки, може мобілізувати інших. Розвиток інформаційного суспільства призводить до того, що атомізовані індивіди часто змушені боротися за свою ідентичність. Соціальні медіа, які сприяють формуванню відчуття самотності у сучасних людей, змушують їх сприймати політичну реальність через призму власного Его, трактуючи себе як релігійних або аполітичних.

Якщо вважати, що певний тип людини, будь то демократичний чи масовий, формується під впливом соціуму, можна припустити, що байдужість до політики є наслідком інформаційно перенасиченого світу, а не причиною конфліктів. В українському суспільстві це також можна розглядати як результат тривалого споживання пропагандистських наративів, таких як: «поза політикою», «політика — це брудно», «політики завжди крадуть», «бариги», «на війні заробляють олігархи» тощо. Це призводить до бажання дистанціюватися, байдужого або надто радикального ставлення до політичних реалій. Таким чином, російська пропаганда на індивідуальному рівні здатна розмивати ідентичність, формувати відчуття відстороненості, мозаїчності та самотності. На територіальному рівні інформаційна війна пропаганди рф звертається до колективних, зокрема етнічних, ідентичностей. Оскільки українське суспільство є мультикультурним і складається з багатьох етносів, російська пропаганда апелює до тих його частин, які виявляють найбільшу лояльність та довіру до росії та російської культури. Це сформувалося під впливом різних чинників: родинних зв’язків, широкого використання російськомовних практик у публічному житті, домінування символічних російських маркерів (пам’ятників, топонімів тощо), перегляду переважно

російських (російськомовних) ЗМІ, а також проживання на території, що межує з агресором, і безпосередньої комунікації з громадянами рф. Через високий рівень залученості до російської культури та повсякденних практик ця категорія населення дуже негативно реагує на будь-які зміни в нормативних актах, що стосуються заборони російської музики, мовлення, викладання в школах, перейменування вулиць, населених пунктів тощо. Це також підсилюється політизацією групових територіальних (регіональних) та етнічних ідентичностей, які формують суспільні вимоги щодо їх врахування в загальнонаціональних інституціях та адаптації інституційних і публічних практик.

Ці фактори стали основою для позитивного сприйняття наративів кремлівської пропаганди, яка завжди ґрунтувалася на історичних міфах про «один народ», «ми ж брати», «українська влада про нас не дбає», «злі бандерівці», «добрі руські». Сьогодні російська пропаганда продовжує тримати такі етнічні групи в повній дезінформації. Відомо, що коли російські війська входять до окупованих міст і сіл, вони відразу починають встановлювати свої правила. Співробітники Національного музею історії України виявили одну з методичок, яка описує, як має відбуватися формування «мовчазної покірності населення» під час експедиції в селі Димерка на Київщині. З фотографій методичок, опублікованих у соціальних мережах, маємо ті ж самі наративи: «народ сам вирішить, хто тут має правити», «влада всіх покинула на призволяще», «всю північ залишили без світла за наказом Києва», «в усьому винні маріонетки Порошенка і Зеленського та їхні ляльководи з США». Наприклад, на одному з Telegram-каналів «Барби на войнушке», що належить Христині Мельниковій, фактчекерський проект «БезБрехні» є допис за 1 травня 2022 року: «Мир, праця, травень! Фрески на заводі Ілліча, які я фотографувала кілька днів тому в практично мирному Маріуполі. Все, що залишилося від радянської спадщини, говорить мені про велич устремлінь того суспільства». Таким чином, конструюючи позитивне ставлення до російських бойовиків, пропаганда підмінює поняття, називаючи окупацію «мирним Маріуполем»:

«Війна – це мир, свобода – це рабство, незнання – сила». Пояснення механізму дії такої пропаганди можна знайти в книзі Е. Фромма «Втеча від свободи». Він зазначає, наскільки важливим для людини є відчуття самотності, і що в критичних ситуаціях їй потрібно спиратися на щось визначене, правду, яка може виявитися хибною: «в кожній живій істоті є прагнення до істини саме тому, що людина для чогось її потребує. І насамперед це стосується орієнтування у зовнішньому світі» [38, с. 57].

Внаслідок тривалого споживання російської пропаганди протягом понад 30 років, яка просувала ідеї «великої і всеосяжної любові росії» та «ненависті» до вигаданих «бандерівців», виникла неспроможність чітко визначити позицію в умовах кризової суспільно-політичної ситуації. Розуміння того, що саме «любляча росія» здійснює агресію та вбивства, руйнує міфи та довіру, які роками формувалися російською пропагандою, що, в свою чергу, «паралізує здатність до критичного мислення».

На національному рівні російська пропаганда поширює наративи про «неефективність політичного керівництва» та «неефективність ЗСУ», створює діпфейки, в яких нібито В. Зеленський оголошує про капітуляцію держави, розсилає масові повідомлення військовим про те, що «військо склало зброю», а також здійснює кібератаки на банківські системи та зламує офіційні сторінки загальнодержавного значення. Тому з перших хвилин повномасштабного вторгнення надзвичайно важливою була мобілізація українців в інформаційному просторі, що дозволяло підтримувати активність значної частини населення та зменшувати панічні настрої шляхом зниження частоти повідомлень про гіпотетичні бомбардування, загрози використання хімічної зброї тощо. Важливу роль також відіграла українська контрпропаганда, яка запустила міфи «про привида Києва», «героїв острова Зміїний», «княгиню Ольгу нашого часу» та «збитого ворожого дрона банкою консервів». Ці наративи сприяли формуванню відчуття єдності та мобілізували населення для масової волонтерської допомоги. Прикладом глобального сприйняття пропаганди є спроби Путіна, його уряду та російських державних ЗМІ

прирівняти Україну до «неонацистів». Однак це твердження не витримує навіть найпростішої перевірки фактів, оскільки в Україні не існує ані тоталітарної системи, ані представників ультраправих сил у парламенті.

Спроби дискредитувати Україну в очах Заходу росія маскує під наративами про «появу трупів у Бучі після відступу російських військ» та «живих трупів» Бучі, стверджуючи, що вбивства і зображення трупів є інсценуванням. Аналогічно, російська пропаганда називала відео з обстріляного пологового будинку в Маріуполі «постановочним відео Зеленського». Хоча на глобальному рівні пропаганда рф не є ефективною, це не означає, що її поширення не становить загрози для України. Дж.Голдензєр у своїй статті підкреслює, що, незважаючи на те, що «Захід оголосив про перемогу України в інформаційній війні, вона має не лише цей фронт. Поки Захід відкидає російські наративи, інші впливові політичні актори їх слухають і приймають. Це стосується, зокрема, Китаю, теоретиків «теорії змови» в США, а також глобального Півдня, який неохоче засуджує росію за війну і практично не протидіє її дезінформації. Сорок країн не підтримали надзвичайну резолюцію Генеральної Асамблеї ООН, що засуджує вторгнення росії в Україну. Білорусь, Еритрея, Північна Корея та Сирія вирішили підтримати росію. Серед 35 країн, які утрималися, були Китай, Іран, Індія, Ірак, Пакистан, Південна Африка, Південний Судан та В'єтнам – держави, які раніше отримували підтримку від США або мали з ними партнерські відносини, які останнім часом поглиблювалися» [48]. Отже, російська дезінформація та гібридна війна, яку росія веде проти України, матиме серйозні наслідки для міжнародних відносин ще довгий час після її завершення. Водночас важливо підкреслити, що пропагандистський вплив на глобальному рівні несе відповідні ризики, зокрема можливість втрати репутаційного капіталу держави. Розподіл функціонування інформаційної війни можна доповнити двома іншими рівнями: цивільним та військовим.

Особливо цікавими в цьому контексті є «м'які атаки» на обидва рівні. Вони не дають миттєвих результатів і практично непомітні. З одного боку, вони

виглядають як звичайні кібератаки, але з іншого – завдяки своїм особливостям впливають на когнітивні процеси. Прикладами таких атак можуть бути злами систем, проникнення, руйнування інформаційних систем, використання зовнішніх акторів і корумпованих внутрішніх структур, а також послаблення можливостей інформаційних систем противника, зокрема за допомогою шкідливих програм і систем штучного інтелекту. У контексті російсько-української війни такі м'які атаки відбуваються постійно. Йдеться не лише про стратегічні інформаційно-психологічні операції (ІПСО), які впливають на територіальному рівні, але й про залучення різноманітних корумпованих політичних акторів, заангажованих ЗМІ, «громадських активістів» та блогерів для підривної та деморалізуючої діяльності в Україні.

Відмінність сучасної російської пропаганди від радянської традиції полягає також у тому, що раніше вона спиралася на міцний підмурівок – комуністичну ідеологію, марксизм-ленінізм, які мали глобальне поширення та певну популярність. Натомість російська пропаганда для внутрішнього споживання та цілей експансії на пострадянському просторі використовує ідеологію «русского мира». Це досить агресивний концепт, під прапором якого відбулося захоплення та анексія Криму, а також триває війна на Донбасі. Для більш широкого вжитку ідея «русского мира» не є прийнятною.

Позитивного порядку денного немає, і російські спецслужби розробили тактику хаотизації свідомості та соціального життя в цивілізованих країнах. Вона включає такі тези та прийоми:

а) критику демократії як неефективної політичної системи,

б) розпалювання внутрішніх громадянських конфліктів, підтримку сепаратистських рухів;

в) втручання у внутрішні справи та електоральний процес;

г) підтримку радикальних організацій у західних країнах, які прагнуть руйнування інтеграційних структур.

Спеціальні ретельні розслідування, проведені спецслужбами США та журналістами провідних видань, підтвердили факти втручання та підривної

пропаганди з використанням інтернет-технологій. Виявилося, що щодо США курс було взято на розпалювання расових протиріч.

Гібридна війна перетворюється на глобальний конфлікт цивілізацій, що розгортається за трьома основними напрямками: західна цивілізація проти євразійської цивілізації, західна цивілізація проти сінської цивілізації та західна цивілізація проти ісламської цивілізації. Китайська пропаганда, через значні культурні відмінності, не має суттєвого впливу на західні країни і зосереджується на просуванні ролі Великого Китаю в Азії. Натомість ісламська пропаганда з боку радикальних груп є більш небезпечною, оскільки впливає на діаспори вихідців зі Сходу в західних країнах, спонукаючи молодь до джихаду та тероризму. російська пропаганда виявилася найбільш загрозливою для Заходу, оскільки росія продемонструвала її ефективність під час війни з Україною. Росія витрачає масштабні нресурси на інформаційну війну; російська пропаганда стає дедалі професійнішою, гнучкішою та підступнішою. Навіть США не можуть повністю захиститися від інформаційних атак і кібератак. Зусилля росії з відновлення пропагандистської машини викликали ланцюгову реакцію. До речі, як вказує Н.Ржевська «з 2012 року хакерські атаки в США стали кваліфікуватися як збройна агресія, що вимагає відповідного реагування, а значна частина фінансування науково-дослідних розробок у США — спрямовуватися на розробку систем захисту інформації. Черговим свідченням значущості управління» [31]

Пропаганда завжди стикається з контрпропагандою. Державна пропаганда повинна бути спростована на рівні державних інституцій або міжнародних об'єднань. Національні уряди західних країн, а також провідні міжнародні організації, такі як НАТО та ЄС, частково повертаються до практик Холодної війни в новому форматі, так званому «2.0». Вони змушені створювати нові контрпропагандистські структури. Їх основне завдання – моніторинг російської пропаганди, виявлення та спростування фейків, а також дослідження методів і прийомів російської пропаганди. У сучасній безпековій лексиці теми пропаганди та контрпропаганди позначаються як «стратегічні комунікації».

Європейський Союз «прокинувся» на початку 2015 року, коли була створена робоча група зі стратегічних комунікацій East StratCom Task Force з метою «протидії російським кампаніям дезінформації». Група виконала певну роботу в рамках проєкту «ЄС проти дезінформації», відкривши сайт, метою якого є «спростування російської пропаганди». На початку квітня 2016 року Єврокомісія ухвалила «Спільні принципи протидії гібридним загрозам — відповідь Європейського Союзу» (Joint Framework on countering hybrid threats a European Union response). У листопаді 2016 року Європейський парламент прийняв Резолюцію «Стратегічні комунікації Європейського Союзу як протидія пропаганді третіх сторін» (EU strategic communication to counteract propaganda against it by third parties), яка, зокрема, передбачала застосування цензурних заходів щодо ряду російських пропагандистських ресурсів.

У 2015 році в Ризі було засновано центр стратегічних комунікацій НАТО, який займається інформаційними та психологічними операціями, а також суспільними відносинами і пропагандою (Central Excellence). З вересня 2017 року в Хельсінкі функціонує Європейський центр боротьби з гібридними загрозами, до складу якого входять 12 західноєвропейських країн.

Основною метою цього центру є збір та поширення інформації про гібридні загрози, зокрема, щодо інформаційного впливу росії на міжнародній арені. В Чехії вже кілька років діє Центр боротьби з гібридними загрозами та тероризмом, який підпорядковується Міністерству внутрішніх справ і займається, зокрема, протидією дезінформації. Основна діяльність цього центру полягає у спростуванні міфів і дезінформації, що надходять з російської федерації. Частково центр проводить освітню роботу, маючи публічні акаунти в соціальних мережах, де висвітлюються ворожі наративи, приклади дезінформації та їх спростування. У Польщі при Міністерстві закордонних справ створено групу експертів, які займаються боротьбою з історичними дезінформаціями з боку росії. Практично всі європейські країни так чи інакше відреагували на події в Україні та нові загрози з боку росії. США також долучилися до цього процесу, виділяючи цільові кошти на боротьбу з

пропагандою ІДІЛ та російської федерації. У березні 2016 року до Сенату було подано законопроєкт «Про протидію інформаційній війні», який передбачав створення комплексної стратегії боротьби з дезінформацією та пропагандою, що поширюються росією та Китаєм. У травні 2016 року цей законопроєкт був внесений до Палати представників під назвою «Про боротьбу з іноземною дезінформацією та пропагандою». У грудні 2016 року положення цього законопроєкту були включені до проєкту Закону «Про національний оборонний бюджет» (National Defense Authorization Act 2017).

На основі прийнятих положень у Державному департаменті було створено Глобальний центр взаємодії (Global Engagement Center), метою якого є протидія державній пропаганді та дезінформації. 16 січня 2018 року сенатори США (Marco Rubio, Chris Van Hollen) представили законопроєкт, що передбачає санкції для країн, які втручаються у вибори США. Зокрема, законопроєкт забороняє іноземним урядам або агентам, що діють від їхнього імені, використовувати соціальні мережі та традиційні ЗМІ для поширення неправдивої інформації, купувати рекламу для впливу на вибори, а також блокувати чи перешкоджати доступу до виборчої інфраструктури.

У 2021 році, напередодні зустрічі лідерів держав G7, міністр закордонних справ Великої Британії Д. Рааб заявив, що його країна веде «виснажливу роботу» з путіним у боротьбі з фейковими новинами та дезінформацією. Міністр зазначив, що найближчим часом країна посилить боротьбу з російською пропагандою на тлі результатів дослідження про російську фабрику тролів, яка націлена на національні ЗМІ та працює над поширенням промосковських поглядів.

Дослідження виявило, що російські тролі під виглядом британців публікують провокаційні коментарі під статтями в The Times, Daily Mail, The Sun та Daily Express, щоб створити хибне враження про підтримку британським суспільством агресії Росії проти України. Ці коментарі потім використовуються російськими державними ЗМІ як доказ нібито підтримки москви з боку громадськості Великої Британії. Міністр повідомив, що країни G7 повинні

розробити механізм швидкого реагування на московську пропаганду. Україна розпочала боротьбу на інформаційному фронті з весни 2014 року, але інституційна реакція затримувалася.

Перші контрпропагандистські акції здійснювалися за ініціативою волонтерів, журналістів та небайдужих громадян, переважно в інтернеті. У березні 2014 року був запущений волонтерський проєкт Stoop Fake. У червні 2014 року було створено Міністерство інформаційної політики, яке в лютому 2015 року ініціювало інтернет-проєкт «Інформаційні війська України» з гаслом: «Кожен твій інформаційний посил – це куля у свідомість ворога». У проєкті брали участь від 20 до 30 тисяч волонтерів, які, зокрема, моніторили російські ЗМІ, включаючи пропагандистські медіа, такі як Lifenews, Russia Today, Lenta.ru та «РИА Новости». Телеканали також запустили контрпропагандистські проєкти, такі як «Антизомбі» на ICTV та «Вєсті Кремля» на «24 каналі». Лише навесні 2021 року в Україні почали створюватися центри, що за структурою та функціями нагадують західні інституції. Рада національної безпеки і оборони заснувала Центр протидії дезінформації, який підпорядковується секретарю РНБО. Паралельно при Міністерстві культури та інформаційної політики був презентований Центр стратегічних комунікацій та інформаційної безпеки.

Основні напрямки його роботи включають:

1) створення онлайн-ресурсу для оперативного реагування на інформаційні атаки;

2) інформування про гібридну агресію на міжнародному рівні;

3) стратегічні комунікації, включаючи розробку контрнаративів, проведення інформаційних кампаній та інтеграцію українських наративів у щоденну комунікацію уряду;

4) діяльність, спрямована на підвищення рівня критичного мислення суспільства для розуміння російських провокацій.

Сучасний етап розвитку суспільства, позначений глибокими соціокультурними та технологічними змінами, стає ареною інтенсивної

політичної боротьби, де цифрова пропаганда відіграє ключову роль. Цифрова пропаганда, використовуючи технологічні досягнення, перетворилася на потужний інструмент політичного протистояння. Її здатність формувати громадську думку та впливати на електоральні процеси робить її стратегічно важливим елементом політичної боротьби на національному та міжнародному рівнях. Активне використання цифрової пропаганди російською Федерацією у її гібридній війні проти України є яскравим прикладом політично вмотивованого застосування дезінформації для досягнення конкретних геополітичних цілей.

Технологічні аспекти цифрової пропаганди безпосередньо пов'язані з політичними цілями. Алгоритми соціальних мереж, що підсилюють поширення певного контенту, можуть бути використані для просування політичних наративів та дискредитації опонентів. Застосування штучного інтелекту для автоматизованого створення та розповсюдження політично заангажованої інформації дозволяє здійснювати масштабний вплив на громадську думку з мінімальними людськими ресурсами. Аналіз великих даних стає інструментом політичного маркетингу, дозволяючи точно сегментувати електорат та адаптувати пропагандистські повідомлення для максимізації політичного впливу.

Соціально-психологічні механізми, що лежать в основі сприйняття цифрової пропаганди, також мають чітке політичне забарвлення. Експлуатація когнітивних упереджень та ефекту повторення спрямована на формування стійких політичних переконань та поляризацію суспільства. Протидія цифровій пропаганді, таким чином, є не лише питанням медіаграмотності, але й завданням захисту демократичного процесу від зовнішнього та внутрішнього політичного втручання.

Еволюція пропагандистських методів відображає політичну конкуренцію в цифровому просторі. Відмова від примітивних фейкових новин на користь складних, персоналізованих кампаній свідчить про зростаючу політичну зрілість акторів інформаційної війни. Використання ботових мереж для

формування штучної підтримки політичних ідей або для атак на політичних опонентів є прямим втручанням у демократичний дискурс.

Протидія цифровій пропаганді набуває політичного значення, оскільки вона спрямована на захист національного суверенітету та демократичних інститутів від деструктивного впливу. Комплексний підхід до цієї проблеми включає не лише технологічні рішення, але й правове регулювання політичної реклами в цифровому просторі, а також соціальні ініціативи, спрямовані на підвищення політичної свідомості громадян. Міжнародна співпраця у цій сфері є необхідною для протидії транснаціональним політичним впливам.

Російська пропаганда є яскравим прикладом використання цифрових технологій як інструменту зовнішньої політичної інтервенції. Її наративи, спрямовані на дестабілізацію України та підрив довіри до західних демократій, мають чітко визначені політичні цілі. Тактика «м'яких атак» через залучення лояльних політичних сил та медіа є складовою ширшої стратегії політичного впливу.

Контрпропагандистські зусилля держав та міжнародних організацій також мають політичну природу, оскільки спрямовані на захист власних політичних систем та цінностей від зовнішньої інформаційної агресії. Створення спеціалізованих структур та розробка стратегій протидії дезінформації є політичним рішенням, що відображає усвідомлення загрози цифровій пропаганди для національної безпеки та демократії.

Отже, цифрова пропаганда є невід'ємною складовою сучасної політичної боротьби. Її технологічні можливості використовуються для досягнення конкретних політичних цілей, маніпулювання електоратом та підриву демократичних процесів. Ефективна протидія цій загрозі вимагає не лише технологічних інновацій, але й усвідомлення політичної природи цих процесів, а також скоординованих зусиль на національному та міжнародному рівнях для захисту політичного суверенітету та демократичних цінностей.

Висновки до Розділу 3.

У сучасних умовах геополітичної нестабільності та інформаційної насиченості, феномен інформаційної атаки набуває особливої актуальності як інструмент впливу на суспільну свідомість та поведінку. Інформаційна атака визначається як спланований, цілеспрямований та масований інформаційний вплив на визначеного адресата або множину адресатів, що має на меті формування запрограмованої громадської думки та, як наслідок, корекцію їхньої поведінки у бажаному для комунікатора напрямку. На відміну від тривалого стану інформаційної війни, інформаційна атака характеризується чітко окресленими часовими рамками, що дозволяє ідентифікувати її початок та завершення.

До онтологічних властивостей інформаційної атаки слід віднести її організованість, що передбачає наявність суб'єкта-комунікатора, чіткого плану дій та скоординованих зусиль для досягнення поставленої мети. Цілеспрямованість є ключовою характеристикою, оскільки кожна інформаційна атака має конкретну мету – зміну установок, переконань або поведінки адресата. Масивність впливу проявляється як на кількісному рівні – залучення значної кількості інформаційних повідомлень та каналів їхньої трансляції, так і на змістовному рівні – багаторазове повторення ключових наративів, використання різноманітних вербальних та невербальних засобів впливу, адаптованих до особливостей різних сегментів аудиторії.

Каналами передачі інформаційної атаки та одночасно її «зброєю» виступають засоби масової інформації (традиційні та цифрові) та мережа Інтернет у всьому її різноманітті – соціальні мережі, блогосфера, месенджери, онлайн-медіа. Важливою особливістю інформаційної атаки є множинність її адресатів, що зумовлює необхідність врахування цього фактору при її плануванні та проведенні. Одночасний вплив на різні соціальні групи, що можуть мати відмінні ціннісні орієнтації, рівень освіти та сприйняття інформації, вимагає ретельного вибору вербальних (лінгвістичних конструкцій,

стилістичних прийомів) та невербальних (візуальних образів, символів, аудіоматеріалів) засобів комунікації для забезпечення максимальної ефективності впливу на кожен сегмент аудиторії.

Інформаційну атаку можливо змоделювати, використовуючи класичну комунікаційну модель, що включає такі елементи: комунікатор (суб'єкт атаки), повідомлення (інформаційний контент), канал (засоби масової інформації та Інтернет), адресат (цільова аудиторія) та ефект (зміни у громадській думці та поведінці адресата). Ефективність проведеної інформаційної атаки стає відчутною після її завершення та в кінцевому підсумку проявляється на невербальному рівні – у зміні поведінкових патернів адресатів, їхній політичній активності, підтримці певних ідей або дій.

У контексті зростаючої ролі цифрових технологій у політичній боротьбі, перспективним напрямком наукових досліджень є поглиблене вивчення цифрової пропаганди. Особливий інтерес представляє аналіз ролі спільнот ботів у процесах поширення та ампліфікації пропагандистських наративів, що просуваються національними державами. Дослідження екосистем, керованих ботами, та оцінка їхньої ефективності у просуванні політичного порядку денного, зокрема Російської Федерації, шляхом маніпулювання суспільно значущими наративами, дозволить більш глибоко оцінити глобальний вплив цих штучно створених спільнот на досягнення їхніх стратегічних цілей.

У цьому контексті, наукова увага повинна бути зосереджена не лише на аналізі механізмів поширення проросійських наративів ботовими спільнотами, але й на дослідженні контрнаративів, спрямованих на підтримку України, які також можуть бути виявлені та проаналізовані в межах діяльності цих ботових екосистем. Вивчення взаємодії між проросійськими та проукраїнськими наративами, що циркулюють у ботових спільнотах, може надати цінну інформацію про стратегії інформаційного протиборства в цифровому просторі та виявити найбільш ефективні методи протидії дезінформації.

Таким чином, інформаційна атака є складним та багатоаспектним феноменом, що відіграє значну роль у сучасній політичній боротьбі.

Поглиблене наукове дослідження її онтологічних властивостей, механізмів реалізації та особливостей прояву в цифровому середовищі, зокрема через діяльність ботових спільнот, є важливим завданням для розуміння сучасних інформаційних війн та розробки ефективних стратегій протидії маніпулятивному впливу на суспільну свідомість. Подальші дослідження в цьому напрямку сприятимуть підвищенню рівня інформаційної безпеки та захисту демократичних цінностей в умовах зростаючої складності інформаційного ландшафту.

Застосування цифрової пропаганди як інструменту політичної боротьби є багатогранним та охоплює широкий спектр технологічних та соціально-психологічних аспектів. З технологічної точки зору, цифрова пропаганда активно використовує можливості соціальних мереж, пошукових систем, месенджерів та інших онлайн-платформ для поширення політично заангажованого контенту. Алгоритми функціонування цих платформ, оптимізовані переважно для комерційних цілей, можуть ненавмисно або навмисно сприяти поширенню дезінформації та фейкових новин, створюючи так звані «ехо-камери» або «бульбашки фільтрів, в яких користувачі опиняються в інформаційному вакуумі, що підтверджує їхні вже існуючі упередження та обмежує доступ до альтернативних точок зору.

Крім того, стрімкий розвиток штучного інтелекту (ШІ) та технологій автоматизації відкриває нові перспективи для цифрової пропаганди. Системи ШІ можуть бути використані для автоматизованого створення та розповсюдження великих обсягів пропагандистського контенту, генерування фейкових акаунтів у соціальних мережах (ботів), а також для проведення складних аналітичних операцій з метою виявлення найбільш вразливих аудиторій та адаптації пропагандистських повідомлень під їхні індивідуальні характеристики та психологічні особливості. Аналіз великих даних (Big Data) стає незамінним інструментом для політичних акторів, що прагнуть ефективно використовувати цифрову пропаганду, оскільки він дозволяє отримувати детальну інформацію про настрої та переконання різних соціальних груп,

прогнозувати їхню реакцію на певні політичні події та розробляти цілеспрямовані пропагандистські кампанії.

З соціально-психологічної точки зору, цифрова пропаганда активно експлуатує фундаментальні когнітивні механізми та психологічні упередження, властиві людській природі. Такі прийоми, як апеляція до емоцій (страху, гніву, ненависті), використання ефекту багаторазового повторення, поширення конспірологічних теорій та створення образів ворога, спрямовані на формування у цільових аудиторій певних політичних переконань та спонукання їх до конкретних дій. В умовах інформаційної перенасиченості та високої швидкості поширення інформації в цифровому середовищі, індивіди часто відчувають труднощі з критичною оцінкою отриманих даних, що робить їх більш вразливими до маніпулятивного впливу пропаганди.

Еволюція методів пропаганди в цифрову епоху свідчить про перехід від простих та часто грубих фейкових новин до більш витончених та цілеспрямованих стратегій. Сучасні цифрові пропагандисти віддають перевагу збору та ретельному аналізу даних про свої цільові аудиторії, їхню поведінку в онлайн-середовищі, інтереси та вподобання. На основі отриманих даних здійснюється глибока сегментація аудиторій та розробка персоналізованих пропагандистських повідомлень, які враховують психологічні особливості кожної окремої групи. Використання ботових мереж та тролів дозволяє створювати ілюзію широкої підтримки певних політичних ідей або, навпаки, дискредитувати опонентів шляхом поширення негативних коментарів та фейкових звинувачень.

Протидія цифровій пропаганді є складним та багатоаспектним завданням, що вимагає комплексного підходу та об'єднання зусиль на різних рівнях – від індивідуального до міжнародного. На технологічному рівні необхідно розробляти та впроваджувати ефективні інструменти для виявлення та аналізу дезінформаційного контенту, ідентифікації ботових мереж та протидії їхній діяльності. Застосування технологій штучного інтелекту для автоматизованої

фільтрації недостовірної інформації та верифікації фактів є одним з перспективних напрямків у цій сфері.

На правовому рівні необхідно розробляти та вдосконалювати законодавчу базу, спрямовану на регулювання діяльності в інформаційному просторі, протидію поширенню дезінформації та притягнення до відповідальності осіб, причетних до організації та проведення пропагандистських кампаній, що мають на меті підрив національної безпеки та демократичних інститутів.

На соціально-освітньому рівні ключову роль відіграє підвищення рівня медіаграмотності та критичного мислення громадян. Розробка та впровадження освітніх програм, спрямованих на формування у населення навичок аналізу інформації, розпізнавання фейків та пропагандистських маніпуляцій, є важливим елементом створення стійкого до інформаційних загроз суспільства. Підтримка незалежних медіа та фактчекінгових ініціатив також сприяє підвищенню якості інформаційного простору та протидії поширенню недостовірної інформації.

У контексті політичної боротьби, цифрова пропаганда набуває особливої гостроти, оскільки використовується для досягнення конкретних політичних цілей. Прикладом цього є активне застосування Російською Федерацією цифрової пропаганди як інструменту гібридної війни проти України. Російські пропагандистські кампанії спрямовані на дестабілізацію політичної ситуації в Україні, підрив довіри до державних інститутів, розпалювання соціальної напруженості та формування у населення викривленого уявлення про події, що відбуваються. Аналогічні методи можуть використовуватися для втручання у виборчі процеси в інших країнах, дискредитації політичних опонентів та просування власних геополітичних інтересів.

Протидія цифровій пропаганді в політичній сфері вимагає скоординованих зусиль з боку державних органів, політичних партій, громадських організацій та міжнародної спільноти. Необхідно розробляти та впроваджувати стратегії контрпропаганди, спрямовані на спростування дезінформаційних наративів та просування об'єктивної інформації. Важливу

роль у цьому процесі відіграє міжнародна співпраця, обмін досвідом та координація дій між різними країнами у сфері боротьби з цифровою пропагандою.

Отже, цифрова пропаганда є складним, багатогранним та динамічним явищем, що становить серйозну загрозу для демократичних цінностей, національної безпеки та стабільного розвитку суспільства. В умовах глибоких соціокультурних та технологічних трансформацій вона стає одним з ключових інструментів політичної боротьби, ефективна протидія якій вимагає комплексного, системного та скоординованого підходу на всіх рівнях – від індивідуального до глобального. Лише шляхом об'єднання зусиль, розвитку критичного мислення, підвищення медіаграмотності, впровадження технологічних інновацій та правового регулювання можливо мінімізувати негативний вплив цифрової пропаганди та забезпечити інформаційну безпеку суспільства в умовах сучасних викликів.

Список посилань до Розділу 3.

1. Алещенко В. (2019) Особливості пропаганди в умовах інформаційно-психологічної війни. *Збірник наукових праць*. Вип. 24. С. 29–38.
2. Бар-Зохар М., Мішаль Н. (2021) Моссад. Найвидатніші операції ізраїльської розвідки. Наш Формат. 384 с.
3. Бєлай С., Корнієнко Д. (2018. Інформаційна безпека сьогодення – невід'ємна складова воєнної безпеки. *Актуальні проблеми управління інформаційною безпекою держави.* Київ: Національна академія Служби безпеки України, 408 с.
4. Біденко А. (2023). Цифрова пропаганда як нова мода в інформаційних війнах. *Лабораторія цифрової дипломатії*. URL: https://intrel.lnu.edu.ua/ddlab/2021/09/27/tsyfrova-propahanda-iak-nova-moda-v-informatsiynykh-viynakh/ (дата звернення 21.09.2024)

5. Біденко А. Центр протидії дезінформації: філософія проти менеджменту. ГО «Детектор медіа». URL: https://detector.media/infospace/article/185107/2021-02-22-tsentr-protydii-dezinformatsiifilosofiya-proty-menedzhmentu/ (дата звернення: 01.05.2024).

6. Білоусова Н., Ціось З. (2025). Цифрове мистецтво як інструмент сучасної пропаганди у системі масових комунікацій. Acta de Historia & Politica: Saeculum XXI. С. 161-170.

7. Вітюк Н. (2019). Особливості дискурсу політичної пропаганди в умовах інформаційно-психологічної війни. *Збірник наукових праць: психологія*, Вип. 24. С. 29–38.

8. Войціховський А. (2018) Кібербезпека як важлива складова системи захисту національної безпеки європейських країн. *Журнал східноєвропейського права*. № 53. С. 26-37.

9. Воронкова В. (2022). Філософія цифрової людини і цифрового суспільства: теорія і практика. Львів-Торунь: Liha-Pres, 460 с.

10. Гула Р. (2020). Концептуальні засади воєнної політики у кіберпросторі провідних держав світу та воєнно-політичних інституцій. № 4. С. 22–26.

11. Данілов О. (2020). Кіберзахист державних інформаційних ресурсів – важлива складова у процесі цифрової трансформації країни. URL: https://www.rnbo.gov.ua/ua/Diialnist/4606.html

12. Доренський О. (2015). Модель поведінки держави в умовах проявів ознак інформаційної експансії, агресії, війни. *Інформаційна безпека держави, суспільства та особистості Всеукр. наук.-практ. конф*., 16 квітня 2015 р. м. Кіровоград: зб. тез доп. Кіровоград: КНТУ. С. 131-133.

13. Дудатьєв А., Войтович О. (2017). Інформаційна безпека соціотехнічних систем: Модель інформаційного впливу. *Інформаційні технології та комп'ютерна інженерія*. №38(1). С.16–21.

14. Дудатьєв А., Куперштейн Л., Войтович О. (2023) Інформаційне протиборство: моделі реалізації та оцінювання інформаційних операцій. *Електронне фахове наукове видання «Кібербезпека: освіта, наука, техніка»*.

№ 4 (20) С. 72–80. https://doi.org/10.28925/2663-4023.2023.20.7280 (дата звернення 25.09.2024)

15. Запорожець О. (2021). Операції впливу: концептуальний вимір. Медіафорум : аналітика, прогнози, інформаційний менеджмент, №9, с.232-244.

16. Заруба О. (2017) Планування спеціальних інформаційних операцій. Інформаційна безпека людини, суспільства, держави, № 1(21), с. 140–154.

17. Застосування Сухопутних військ Збройних Сил України у конфліктах сучасності (за досвідом забезпечення національної безпеки складовими сектору безпеки і оборони у ході російсько-української війни). Практичний посібник. Львів: НАСВ, 2023, 381 с.

18. Золотухін Д. (2021) Матриця загроз інформаційної сфери. ГО «Детектор медіа»: сайт. URL: https://detector.media/infospace/article/186798/2021-04-08-matrytsya-zagroz-informatsiynoi-sfery/ (дата звернення: 01.05.2024).

19. Золотухін Д. (2021) Центр протидії дезінформації: практика імплементації. ГО «Детектор медіа»: сайт. URL: https://detector.media/infospace/article/185586/2021-03-08-tsentr-protydii-dezinformatsiipraktyka-implementatsii/ (дата звернення: 01.05.2024).

20. Золотухін Д. (2018). Біла Книга спеціальних інформаційних операцій проти України 2014–2018. Київ. 384 с.

21. Золотухін Д. (2021). Як має працювати Центр протидії дезінформації. ГО «Детектор медіа». URL: https://detector.media/infospace/article/185077/2021-02-20-yak-maie-pratsyuvaty-tsentr-protydiidezinformatsii-poyasnennya-napaltsyakh/ (дата звернення: 01.05.2024).

22. Інформаційні атаки в соціальних мережах: дослідження впливу російської дезінформації через рекламу в facebook (2024). Київ. 31 с.

23. Інформаційні виклики гібридної війни: контент, канали, механізми протидії: аналіт. доп.) / За заг. ред.А. Баровської (2016). Київ: НІСД. С. 69–80.

24. Колодяжний І., Доренський О. (2019). Методологічні засади підвищення ефективності протидії антиукраїнській пропаганді в соціальних мережах. *Інформаційні технології – 2019: VI всеукр. наук.-практ. конф. молодих*

науковців (16 трав. 2019 р., м. Київ). Київ. Университет імені Б. Грінченка. С. 53-54.

25. Мегель А., Яремчук М. (2024). Ворожі ІПСО, як вистояти та протистояти. Київ, Скіф. 96 с.

26. Наконечний В., Хлевна Ю., Половінкін І., Кузьменко М. (2024). Метод оцінки розповсюдження неправдивої інформації за допомогою спеціальних програм та технологій на базі середовища Інтернет. *Сучасний захист інформації.* № 2. С. 84-91. URL: https://journals.dut.edu.ua/index.php/dataprotect/article/ view/2983 (дата звернення 05.01.2025)

27. Панченко В. (2014). Інформаційні операції в асиметричній війні Росії проти України: підходи до моделювання. *Інформація і право*. № 3(12). С. 13–16.

28. Панченко В. (2016). Інформаційні операції в системі стратегічних комунікацій. *Стратегічні пріоритети*. *Серія: Політика*. № 4. С. 72–79.

29. Пехник А., Завгородня Ю. (2021). Сучасні загрози кібертехнологій у політичному процесі. *Актуальні проблеми політики*. № 68. С. 76-82.

30. Пріба Г., Калюжна Є. (2022). Особистість у сучасному соціо-психологічному вимірі. Херсон, Олді. 554 с.

31. Ржевська Н. (2024). Сучасна інформаційна політика: досвід США для України. *Political Studies*. № 1 (7). С. 68-85.

32. Руцький С. (2024) Кіберконфлікти у протиборстві суб'єктів політики на території європейських країн. *Сучасні виклики соціально-політичного розвитку: політико-правові та соціально-економічні виміри: матеріали всеукраїнської студентської науково-практичної конференції,* м. Одеса, 24 травня 2024 року. Одеса: ДЗ «Південноукраїнський національний педагогічний університет імені К. Д. Ушинського», Центр соціально-політичних досліджень «Politicus». С. 60-62.

33. Руцький *С. (2024). Ц*ифрова пропаганда в аспекті сучасного інформаційного протиборства. *Вісник Львівського університету*. № 55.

34. Рущенко І. (2021). Пропаганда та контрпропаганда в цифровому суспільстві: інституціоналізація. Український соціологічний журнал. № 25. С. 7-16.

35. Свідерська О. (2022). Цифрова пропаганда та ризики інформаційної безпеки у контексті російсько-української війни. *Політикус.* № 2. С. 6-65.

36. Теоретичні основи створення технологій протидії прихованим інформаційним атакам в сучасній гібридній війні / Алімпієв А. М., Бараннік В. В., Белікова Т. В., Сідченко С. О. *Системи обробки інформації*. Вип. 4. С. 113–121.

37. Трофименко О., Логінова Н., Соколов А., Чикунов П., Ахмаметьєва Г. (2024) Штучний інтелект у військовій сфері. *Кібербезпека: освіта, наука, техніка.* № 1 (25). С. 161-176.

38. Фромм Е. (2024) Втеча від свободи. Харків, КСД, 288 с.

39. Харченко М., Сапогов С., Шамраєва В., Новікова Л. (2017). Основні засоби інформаційного протиборства та інформаційної війни як явища сучасного міжнародного політичного процесу. *Вісник Харківського національного університету імені В.Н.Каразіна, Серія «Міжнародні відносини*. *Економіка. Країнознавство. Туризм*». Випуск 6. С. 77 -81.

40. Цифрова реальність у глобальній системі людина-суспільство: збірник наукових праць (2021) / за загальною редакцією Л. Г. Дротянко. Київ: НАУ, 109 с.

41. Шевчук М. (2024). До питання генези поняття інформаційної безпеки як складової національної безпеки. *Науковий вісник Ужгородського національного університету. Серія ПРАВО*. Вип. 78. Ч.2. С. 134-139.

42. Шемчук В. (2020). Загрози інформаційній безпеці: проблеми визначення та подолання. *Експерт: парадигми юридичних наук і державного управління,* № 1 (7). С. 285-296.

43. Шульська Н., Букіна Н., Адамчук Н. (2023). Типологічні маркери інформаційно-психологічних операцій (іпсо) в умовах війни в медіа. *Вчені*

записки ТНУ імені В. І. Вернадського. Серія: Філологія. Журналістика. Т. 34. №1. ч. 2. С 268-273.

44. Янишевський С. (2023). Цифрова трансформація суспільства, вплив пропаганди та дезінформації в суспільстві. Протидія дезінформації в умовах російської агресії проти України: виклики і перспективи. Харків, 2023. URL: https://www.researchgate.net/publication/376776221_Cifrova_transformacia_suspilstva_vpliv_propagandi_ta_dezinformacii_v_suspilstvi (дата звернення 21.01.2025).

45. Cyberspace. (2011). White House. URL: http://www.whitehouse.gov/sites/default/files/rss_viewer/international_strategy_for_cyberspace.pdf (дата звернення 23.02.2023)

46. Jaeger, P. T., Gorham, U., & Greene N. (2015, July). Teaching Information Policy in the Digital Age: Issues, Strategies, and Innovation. J. of Education for Library and Information Science, 56 (3). (Summer). URL: https://files.eric.ed.gov/fulltext/EJ1074656.pdf (дата звернення 20.02.2024)

47. Huntington S. (1993). Essay: The Clash of Civilizations? *Foreign Affairs*, 15 p.

48. Goldenziel J. (2022). The Russia-Ukraine Information War Has More Fronts Than You Think. URL: https://cutt.ly/yJxOq4Q [in English].

Висновки

В результаті проведеного дослідження було досягнуто відповідних висновків:

1. Проведений аналіз наукових праць переконливо свідчить про високу актуальність дослідження інформаційного протиборства в сучасному суспільно-політичному просторі. Цей науковий напрям є безперечно затребуваним викликами сьогодення, які включають стрімку цифровізацію, трансформацію політичної комунікації та ескалацію латентних форм політичної агресії в інформаційному середовищі. Огляд монографій та дисертаційних досліджень демонструє широкий спектр наукових підходів до вивчення різних аспектів інформаційного протиборства, включаючи правові, психологічні, соціальні, політичні та технічні аспекти. Незважаючи на значний науковий інтерес та вагомий обсяг проведених досліджень, залишається низка невирішених питань, що підкреслює необхідність подальших глибоких та комплексних міждисциплінарних досліджень у цій сфері. Проблеми виникнення, розвитку та протидії інформаційним війнам, формування ефективних механізмів інформаційної безпеки, а також вивчення новітніх форм інформаційного впливу та протистояння вимагають постійної наукової уваги для забезпечення національної безпеки та стабільного розвитку суспільства в умовах зростаючої інформаційної конфронтації.

2. Інформаційно-комунікаційна революція початку XXI століття кардинально змінила природу сучасного інформаційного протистояння, породивши нові можливості впливу завдяки технологіям кастомізації, аналізу великих даних та штучного інтелекту. Незважаючи на технологічні новації, сутність інформаційного протистояння як інструменту досягнення політичних цілей залишається незмінною. Водночас, сфера вивчення цієї проблематики стикається зі значними теоретико-методологічними труднощами, зокрема з термінологічною невизначеністю.

Подальше наукове осмислення потребують онтологічні, деонтологічні та епістемологічні аспекти інформаційного протистояння, включаючи етичні

питання та проблеми верифікації інформації. Для адекватного відображення сучасної динаміки інформаційного протиборства необхідне зближення різних наукових підходів, включаючи військово-прикладні, геополітичні, політико-технологічні, математичні та кібернетичні.

Концептуалізація інформаційного протистояння передбачає його розуміння як суб'єкт-суб'єктної взаємодії, відрізняючи його від інформаційної агресії (суб'єкт-об'єктної взаємодії) та інформаційної війни, яка є найбільш агресивною формою протистояння з можливим переходом у "гарячу" фазу.

Таким чином, інформаційне протистояння стало ключовим елементом політичної боротьби в сучасному світі, і подальші дослідження повинні бути спрямовані на подолання теоретичних проблем та розробку нових міждисциплінарних підходів для глибокого розуміння його динаміки та наслідків.

3.Узагальнюючи, сучасне інформаційне середовище, сформоване цифровою революцією, докорінно змінило характер інформаційного протистояння, вивівши на передній план концепцію "інформаційної війни". Ця концепція еволюціонувала від розуміння інформації як об'єкта військових дій до її сприйняття як активного інструменту досягнення політичних та військових цілей. Незважаючи на відсутність загальноприйнятого визначення, інформаційна війна розглядається як інтенсивна форма інформаційного протистояння, спрямована на встановлення домінування в інформаційному просторі противника.

Розвиток інформаційних технологій, зокрема в рамках концепції мережецентричної війни, призвів до появи нових стратегій та принципів ведення бойових дій, де інформаційна перевага стає ключовим фактором успіху. Досягнення цієї переваги передбачає комплексний підхід, що включає активні, захисні та впливові інформаційні заходи, а також інтеграцію інформаційних аспектів у всі функції ведення війни.

Водночас, глобалізація та інформатизація породили нові форми інформаційного протистояння, такі як "картографічні війни", а також

актуалізували дослідження гібридних моделей інформаційної війни на локальному рівні. Розуміння цілей та принципів інформаційної війни, включаючи попередження конфлікту, ослаблення противника, дезорієнтацію та захист власної інформації, є критично важливим в умовах зростаючої ролі інформаційного фактору в сучасних конфліктах. Таким чином, інформаційна війна та прагнення до інформаційної переваги стали визначальними характеристиками політичної та військової боротьби в цифрову епоху, вимагаючи постійного дослідження та адаптації стратегій і технологій у цій сфері.

4.Аналіз ключових аспектів інформаційних операцій, починаючи від теоретичних засад інформаційної зброї до конкретних форм і умов їх реалізації дає можливість визначити аалгоритми та форми реалізації інформаційних операцій, які часто використовуються в комплексі: психологічні операції (PSYOP) - поширення спеціально підготовленої інформації для впливу на емоційний стан, мотивацію, аргументацію дій, прийняття рішень та поведінку цільових аудиторій. Включають пропаганду та психологічні акції; дезінформація (Military Deception – MILDEC) – навмисне дезорієнтування військового командування противника щодо власних можливостей, намірів та операцій з метою спонукання його до вигідних дій; радіоелектронна боротьба (РЕБ): р радіоелектронне придушення (РЕП) - порушення роботи електронних засобів противника шляхом випромінювання перешкод; радіоелектронний захист - захист власних радіоелектронних засобів від перешкод противника; мережеві операції (Computer Network Operations – CNO); комп'ютерні мережеві атаки - дії в мережах противника з метою пошкодження або знищення інформації та виведення з ладу комп'ютерних систем; мережевий захист - моніторинг та захист власних комп'ютерних мереж від атак; використання комп'ютерних мереж противника - застосування інфраструктури ворога для досягнення власних цілей; безпекові операції (OPSEC) – процес виявлення критичної інформації, аналізу загроз та вразливостей, оцінки ризиків та

впровадження заходів для запобігання доступу противника до цієї інформації (включають диверсії, камуфляж, приховування намірів, дезінформацію).

Допоміжні елементи інформаційних операцій: безпека інформації (Information Assurance, IA) - захист інформації та інформаційних систем, забезпечення їх доступності, цілісності, автентичності, конфіденційності та непідробленості; фізична безпека (Physical Security) – захист персоналу, обладнання, об'єктів та документів від несанкціонованого доступу, шпигунства, саботажу, пошкоджень та крадіжок; фізичні атаки (Physical Attack) – ураження критично важливих інформаційних структур противника для зниження його здатності до управління та впливу; контррозвідка (Counterintelligence) – збір інформації та діяльність, спрямована на захист від шпигунства, розвідувальних дій, саботажу або вбивств, що можуть бути замовлені іноземними урядами, організаціями або терористичними групами.

Наведені алгоритми, форми та ключові умови підкреслюють складність та багатогранність інформаційних операцій як важливого елементу сучасного протистояння. Успішна реалізація таких операцій вимагає глибокого розуміння інформаційної сфери, технологічних можливостей, психології противника та ретельної координації зусиль на різних рівнях.

5. Узагальнюючи, конфронтація взаємодії суб’єктів політики в інформаційному просторі є визначальною характеристикою сучасної геополітичної ситуації. Посилення напруженості та негативних процесів у сфері глобальної безпеки, викликаних геополітичним суперництвом та зіткненням інтересів, призвели до трансформації міждержавних відносин та військового насильства, де інформаційна складова стала невід'ємною на всіх етапах конфлікту. Інформація набула властивостей зброї, а її застосування може мати наслідки, порівнянні з військовими діями.

Технології інформаційних війн, спрямовані на маніпулятивний контроль свідомості, становлять значну небезпеку, розколюючи суспільства або об'єднуючи їх агресію. Основним об'єктом впливу є суспільна та індивідуальна свідомість, а метою – підміна національних цінностей. Інформаційна зброя,

завдяки своїй універсальності, секретності та ефективності, використовується для дискредитації державних засад, розмивання ідентичності та залучення до деструктивної діяльності.

Інформаційне протиборство охоплює інформаційно-технічну та інформаційно-психологічну складові, ведучись як у воєнний, так і в мирний час за політичний вплив та інші стратегічні інтереси. Контроль над інформаційними потоками стає ключем до впливу на події та свідомість населення.

Зростаюча роль кіберсфери у політичній конфронтації призвела до появи «прохолодних війн», де держави використовують кібероперації як інструмент зовнішньої політики, уникаючи відкритого насильства. Проблеми персоналізації учасників та розрив між розумінням технологій та політики ускладнюють розробку ефективних стратегій кібербезпеки.

Для протидії загрозам у кіберпросторі необхідні чітка державна політика, нормативне регулювання, підвищення обізнаності суспільства та реальні механізми відповідальності за кіберзлочини. Міжнародна співпраця та обмін досвідом, як приєднання України до Центру НАТО з кіберзахисту, є важливими кроками у забезпеченні національної кібербезпеки.

Отже, конфронтація в інформаційному середовищі є складним та багатогранним явищем, що вимагає комплексного підходу до забезпечення інформаційної безпеки на національному та міжнародному рівнях. Розуміння сутності інформаційної війни, її технологій та принципів є критично важливим для стабільного розвитку політичних систем та глобальної безпеки.

6. Узагальнюючи, сучасний інформаційний простір став ареною гібридної війни, де традиційні інформаційні атаки тісно переплітаються з кібернетичними, створюючи нові виклики для національної та глобальної безпеки. Конвергенція дезінформації та пропаганди з кібертехнологіями ускладнює атрибуцію та протидію, а трансформація кіберпростору та соціальних мереж призводить до масштабної маніпуляції громадською думкою.

Інформаційні атаки спрямовані на глибинні емоційно-ціннісні структури суспільства, розколюючи його та дестабілізуючи функціонування. Соціальна кібербезпека стає ключовим елементом захисту від цих маніпулятивних практик. Інформаційно-кібернетичні атаки є потужним інструментом геополітичної боротьби, спрямованим на підрив різних аспектів життєдіяльності держави.

Експоненційний розвиток технологій створює нові вектори атак, а зростаюча залежність від цифрової інфраструктури підвищує вразливість. Новітні форми конфронтації в цифровому просторі, що включають автоматизовані системи поширення наративів, використання штучного інтелекту, маніпулювання алгоритмами, deepfake, доксинг, кібератаки на інфраструктуру та соціальну інженерію, характеризуються швидкістю, масштабом, складністю виявлення та технологічною складністю.

Ефективна протидія гібридним загрозам вимагає інтегрованого підходу, що поєднує технічні засоби захисту, законодавчі та регуляторні заходи, підвищення інформаційної грамотності та міжнародну співпрацю. Критичне мислення та медіа-освіта є важливими навичками для стійкості суспільства.

Отже, інформаційні та кібератаки є складними та еволюціонуючими загрозами, що вимагають постійної уваги, розвитку нових методів протидії та усвідомлення того, що інформаційна та кібербезпека є невід'ємними складовими національної безпеки в сучасному нестабільному світі.

7. Узагальнюючи цифрову пропаганду як потужний та еволюціонуючий інструмент інформаційного протиборства. Сучасні спроби маніпуляції в Інтернеті стають дедалі складнішими, поєднуючи автоматизовані кампанії ботів із зусиллями скоординованих людей та технологій штучного інтелекту.

Цифрова пропаганда використовує ілюзії та маніпуляції алгоритмами для поширення односторонніх наративів, сіяння плутанини та підриву консенсусу. Алгоритми соціальних мереж, розроблені з комерційною метою, часто посилюють когнітивні упередження та створюють ехо-камери, сприяючи поширенню неправдивої інформації.

Приклади використання цифрової пропаганди, зокрема росією під час кримської кризи демонструють її ефективність у досягненні політичних та військових цілей.

Аналіз інформаційної війни в соціальних мережах показує стратегічне використання соціально-кіберманеврів для впливу на наративи та спільноти. Стратегії «управління трендом» та використання гомофілії сприяють поширенню дезінформації в онлайн-мережах. Тематичне моделювання є важливим інструментом для розуміння поширення ідей та думок у цифровому просторі.

Зростає розуміння того, що візуальний контент набуває більшої сили впливу, що вимагає розвитку складних програмних комплексів для його аналізу. Автоматизація процесів виявлення пропаганди розглядається як спосіб уникнення людського фактору та забезпечення об'єктивності оцінок.

Реінституціоналізація пропаганди відбувається в контексті гібридних війн, де цифровізація суспільства робить людей більш вразливими до інформаційних інтервенцій. Захист свідомості вимагає розвитку інфоімунітету та медіаграмотності.

Прогнозується, що на зміну «фейковим новинам» прийде «обчислювальна пропаганда», що поєднує можливості комп'ютерів, швидкість обробки даних та великі дані для маніпулювання сенсами.

Нарешті, цифрова людина розглядається як новий етап розвитку, здатний створювати нові інформаційні феномени завдяки конвергенції штучного інтелекту, машинного навчання та потужних баз даних. Таким чином, цифрова пропаганда є складним, багатогранним та постійно еволюціонуючим явищем, що потребує глибокого розуміння та розробки ефективних стратегій протидії в умовах сучасного інформаційного протиборства.

Загалом, проведене дисертаційне дослідження є значним внеском у розвиток політичної науки, поглиблюючи теоретичне розуміння та надаючи емпірично обґрунтований аналіз феномену інформаційного протиборства в умовах цифрової реальності. Отримані результати мають важливе теоретичне

та практичне значення для розробки ефективних стратегій протидії інформаційним загрозам, забезпечення інформаційної безпеки держави та суспільства, а також для формування стійкості демократичних інститутів до деструктивних інформаційних впливів у сучасному світі.

Публікації:

1. Руцький С. (2023). Конфронтація взаємодії суб'єктів політики в інформаційному просторі. *Науковий журнал «Політикус»*. №5. С.82-86. DOI https://doi.org/10.24195/2414-9616.2023-5.12, URL: http://politicus.od.ua/5_2023/12.pdf

2. Руцький *С. (2023).* Загрози в сучасному політичному процесі: інформаційний аспект. *The 3rd International Scientific and Practical Internet conference «Modern Political Processes: Global and National Dimensions». Odesa, 2023.* URL: *http://dspace.onua.edu.ua/handle/11300/26884*

3. Руцький С. (2024). Кіберконфлікти у протиборстві суб'єктів політики на території європейських країн. *Сучасні виклики соціально-політичного розвитку: політико-правові та соціально-економічні виміри: матеріали всеукраїнської науково-практичної конференції*, м. Одеса, 24 травня 2024 року. Одеса: ДЗ «Південноукраїнський національний педагогічний університет імені К. Д. Ушинського», Центр соціально-політичних досліджень «Politicus», С. 60-62. URL: http://dspace.pdpu.edu.ua/jspui/handle/123456789/dspace.pdpu.edu.ua/jspui/handle/123456789/19629

4. Руцький С. (2024). Особливості цифрової пропаганди в умовах воєнного стану. *Матеріали III Всеукраїнської наукової конференції «Державно-правові засади формування безпекового середовища в Україні в умовах сучасних викликів»*. Одеса. ОДУВС.

5. Руцький С. (2024). *Ц*ифрова пропаганда в аспекті сучасного інформаційного протиборства. *Вісник Львівського університету. Серія філос.-політолог. студії.* 2024. Вип. 55. С.437–443. URL: http://fps-visnyk.lnu.lviv.ua/archive/55_2024/53.pdf

6. Руцький С. (2025). Медіаграмотність, як фактор розповсюдження політичної інформації. *Науковий журнал «Політикус»*. № 1. С.94-100.

7. Руцький С. (2025) Парадипломатія як стратегічний інструмент боротьби з дезінформацією в умовах інформаційного протиборства. *Міжнародна наукова конференція «Сталий розвиток регіонів, міст та спільнот в умовах глобальних перетворень: виклики, можливості, сценарії майбутнього.* м.Одеса, 16-17 травня. ОНУ імені І. І. Мечникова.