ПВНЗ «ЄВРОПЕЙСЬКИЙ УНІВЕРСИТЕТ»

Кваліфікаційна наукова праця

на правах рукопису

САВЧУК ВАЛЕРІЙ АФАНАСІЙОВИЧ

УДК 32.019.5:355.02:316.77:004.8

ДИСЕРТАЦІЯ

ІНФОРМАЦІЙНА СКЛАДОВА СУЧАСНИХ ВОЄН: ПРОВІДНІ НАРАТИВИ ТА МЕХАНІЗМИ ВПЛИВУ НА СУСПІЛЬНУ СВІДОМІСТЬ

Спеціальність: 052 Політологія

Галузь знань: 05 Соціальні та поведінкові науки

Подається на здобуття ступеня доктора філософії

Дисертація містить результати власних досліджень. Використання ідей, результатів і текстів інших авторів має посилання на відповідне джерело _____/В.А. Савчук/

Науковий керівник: Тимошенко Олена Іванівна

доктор філософських наук, професор.

Київ 2026

Валерій САВЧУК

Автор цифрового підпису Валерій САВЧУК
Дата: 2026.09.30 11:57:22 +03'00'

АНОТАЦІЯ

Савчук В. А. Інформаційна складова сучасних воєн: провідні наративи та механізми впливу на суспільну свідомість. – Кваліфікаційна наукова праця на правах рукопису.

Дисертація на здобуття ступеня доктора філософії за спеціальністю 052 «Політологія». – ПВНЗ «Європейський університет». – Київ, 2026.

У дисертаційній роботі здійснено комплексне політологічне дослідження інформаційної складової сучасних воєн, провідних наративів і механізмів їхнього впливу на суспільну свідомість. Дослідницьку увагу зосереджено на з'ясуванні того, як інформаційне протиборство впливає на сприйняття подій, довіру до інституцій, формування переконань, оцінювання політичної реальності та моделі поведінки цільових аудиторій.

Теоретико-методологічну основу дослідження сформовано через поєднання системного, структурно-функціонального та порівняльного підходів із контент-, дискурс- і наративним аналізом. Системний підхід забезпечив розгляд акторів, каналів, повідомлень і реакцій аудиторій як взаємопов'язаних елементів інформаційного протиборства; структурно-функціональний аналіз дав змогу розмежувати їхні ролі; порівняльний аналіз – виявити спільні й специфічні характеристики різних конфігурацій впливу. Контент-, дискурс- і наративний аналіз застосовано для простеження переходу від окремих повідомлень до стійких смислових конструкцій, що впливають на політичне оцінювання та поведінкові орієнтації. Емпіричний матеріал доповнено публічними експертними інтерв'ю, зібраними автором і залученими інтерпретативно як джерела фахових позицій щодо інформаційно-психологічного впливу, стратегічних комунікацій, цифрових платформ і безпекових процесів.

У теоретичній частині дослідження простежено еволюцію інформаційної складової війни від ранніх форм впливу на сприйняття та поведінку до сучасних цифрових і когнітивних технологій. Показано, що зміна носіїв і каналів комунікації супроводжувалася поступовим ускладненням цілей інформаційного впливу: від мобілізації власної спільноти, деморалізації противника та

формування зовнішньої легітимності до системної роботи з когнітивними фільтрами аудиторій. Аналіз зарубіжного та українського політологічного дискурсу дав змогу визначити гібридну, наративну та когнітивну війну як взаємопов'язані напрями осмислення сучасного інформаційного протиборства та уточнити місце українського досвіду протидії російській агресії в цьому дослідницькому полі.

Уточнено категорійно-понятійний апарат дослідження, зокрема зміст і співвідношення понять «інформаційна складова сучасної війни», «спеціальна інформаційна операція», «інформаційно-психологічна операція», «когнітивна війна», «наратив», «суспільна свідомість», «деструктивний інформаційний вплив», «механізми впливу на суспільну свідомість», «інформаційна безпека», «стратегічні комунікації» та «когнітивна стійкість». Когнітивну війну визначено як ширший стратегічний рівень впливу на процеси мислення, інтерпретації, довіри, оцінювання політичної реальності й ухвалення рішень. Спеціальні інформаційні та інформаційно-психологічні операції розглянуто як один із провідних операційних механізмів реалізації такого впливу. Запропоновано авторську п'ятиетапну аналітичну модель життєвого циклу спеціальної інформаційної операції, що охоплює когнітивне картографування цільової аудиторії, конструювання наративу, поширення, активну фазу впливу та моніторинг із подальшою адаптацією. Когнітивне картографування виокремлено як самостійний вхідний етап, що встановлює зв'язок між вразливостями аудиторії, релевантними темами й тригерами, способом інтерпретації повідомлення та можливою реакцією. Застосування моделі до кампанії «Doppelgänger» та її подальшої трансформації дозволило простежити зв'язок між аналізом аудиторії, конструюванням і поширенням наративу та адаптацією операції, а також розмежувати її операційну спроможність, цільовий когнітивний вплив і емпірично підтверджені політичні наслідки.

Дослідження механізмів ведення інформаційної війни в умовах новітніх комунікативних технологій дало змогу систематизувати інструменти виявлення та подолання деструктивних впливів. До основних груп віднесено

автоматизоване виявлення й аналіз контенту, мережевий моніторинг і виявлення бот-активності, превентивну інокуляцію та медіаосвіту, фактчекінг і цифрову верифікацію. Аналіз контенту виявляє ознаки маніпуляції, мережевий моніторинг — координовану активність, інокуляція та медіаосвіта розвивають стійкість аудиторії, фактчекінг і цифрова верифікація забезпечують перевірку тверджень та матеріалів. Контрнаративи доповнюють ці інструменти, відновлюючи зв'язну інтерпретацію подій. У результаті захист інформаційного простору розглянуто як поєднання технологічного, аналітичного, комунікаційного та освітнього компонентів.

Соціальні медіа визначено як один із провідних механізмів сучасного інформаційно-психологічного впливу. Їхня роль у сучасному інформаційно-психологічному протиборстві пов'язана з персоналізацією інформаційних потоків, алгоритмічним формуванням порядку денного, емоційним підсиленням конфліктного контенту, створенням цифрових ехо-камер та штучної видимості масової підтримки через бот-мережі й координовану активність. Таке середовище поєднує інформаційний зміст із соціальним підтвердженням, відчуттям групової належності, загрози або морального обурення, що підсилює поведінковий ефект повідомлень. Визначено, що цифрові платформи виступають середовищем швидкого масштабування наративів, а їхні алгоритмічні механізми здатні посилювати органічну комунікацію та координовані маніпулятивні кампанії.

Специфіку кібербезпеки у воєнних умовах розкрито через взаємозв'язок технічної стійкості цифрової інфраструктури, безперервності критичних сервісів, інституційної координації та довіри до державних структур. Кібербезпековий компонент інформаційного протиборства охоплює захист даних, систем і каналів комунікації, реагування на інциденти, розвиток кадрової спроможності та взаємодію між державними й безпековими інституціями. У роботі обґрунтовано зв'язок технічної стійкості цифрового середовища зі здатністю держави підтримувати інформаційну орієнтацію суспільства під час криз і воєнних операцій.

У прикладному блоці досліджено політико-правові засади забезпечення безпеки інформаційного простору України в умовах російської збройної агресії. Визначено, що дієвість державної системи захисту залежить від узгодженості нормативного регулювання, інституційної координації, моніторингу загроз, правового оформлення рішень, комунікаційного пояснення та оцінювання наслідків. Такий підхід дає змогу розглядати інформаційну безпеку як відтворюваний цикл державного реагування, здатний поєднувати правові, організаційні, комунікаційні та технологічні інструменти.

Окремий напрям становить аналіз гуманітарних складників антиукраїнських інформаційно-пропагандистських операцій. До ключових сфер впливу віднесено історичну пам’ять, мовно-культурну ідентичність, освіту, релігію, символічний простір, ціннісні орієнтири та суспільну згуртованість. Російська гуманітарна агресія розглядається як системний тиск на українську політичну спільноту через нав’язування викривлених уявлень про історію, державність, культуру та політичну суб’єктність України. Встановлено, що гуманітарний компонент інформаційного протиборства безпосередньо пов’язаний зі здатністю суспільства зберігати ідентичність, смислову цілісність і готовність до консолідованого спротиву. Відповідно, гуманітарна безпека включена до загальної системи національної та інформаційної безпеки держави.

Дослідження стратегічних комунікацій дозволило визначити їх як інструмент узгодження аналізу загроз, державного повідомлення, публічного пояснення рішень і підтримання довіри до інституцій. Стратегічні комунікації забезпечують випереджальне формування зрозумілих для суспільства пояснювальних наративів, координацію дій державних структур та зниження вразливості аудиторій до деструктивного впливу. Когнітивна стійкість у цій логіці трактується як здатність громадян і суспільних інституцій зберігати критичність сприйняття, розпізнавати маніпулятивні повідомлення, протидіяти емоційному зараженню, інформаційному перевантаженню та нав’язаним інтерпретаційним схемам.

Окреслено можливості та ризики застосування штучного інтелекту й генеративних мовних моделей у сфері інформаційної безпеки. Такі технології розширюють можливості моніторингу, класифікації, аналізу та прогнозування інформаційних загроз, автоматизують пошук аномалій і підтримують оперативне опрацювання великих масивів даних. Водночас персоналізація інформаційних потоків, варіативне генерування повідомлень і масштабування синтетичного контенту підвищують складність виявлення координованої неавтентичної активності та створюють нові умови для сегментації аудиторій, поляризації й поширення недовіри до джерел інформації. Запропонований у дисертації підхід до використання ШІ в стратегічних комунікаціях поєднує технологічну спроможність із захистом даних, правовим і етичним контролем, незалежною оцінкою та персоніфікованою відповідальністю за рішення. У межах дослідження поняття «семантичний суверенітет» використано для позначення спроможності держави й суспільства контролювати критично важливі мовні ресурси, дані та моделі, зберігаючи міжнародну взаємосумісність і відкритість до незалежної оцінки.

Наукова новизна одержаних результатів полягає у розробленні та застосуванні авторських аналітичних інструментів дослідження інформаційної складової сучасних воєн, які дають змогу простежувати взаємозв’язок між вразливостями цільових аудиторій, конструюванням і поширенням наративів, операційною адаптацією інформаційного впливу, його цільовим когнітивним ефектом та емпірично підтвердженими політичними й поведінковими наслідками. Цілісна політологічна модель виконує інтегруючу функцію, поєднуючи стратегічний, операційний, смисловий, технологічний і поведінковий рівні аналізу. Уперше запропоновано та застосовано авторську п’ятиетапну аналітичну модель життєвого циклу спеціальної інформаційної операції з когнітивним картографуванням як самостійним вхідним етапом. Аналітичні можливості моделі продемонстровано на матеріалі кампанії «Doppelgänger» та її подальшої трансформації.

Удосконалено категорійно-понятійний апарат дослідження; підхід до аналізу цифрових механізмів інформаційно-психологічного впливу; підхід до аналізу гуманітарних складників антиукраїнських інформаційно-пропагандистських операцій; підхід до осмислення захисту інформаційного простору України як поєднання політико-правових, організаційних, комунікаційних, технологічних і гуманітарних інструментів. Отримали подальший розвиток положення щодо політичної природи сучасного інформаційного протиборства, аргументація щодо когнітивної стійкості суспільства як ресурсу національної безпеки, наукові уявлення про роль стратегічних комунікацій та оцінка можливостей і ризиків використання штучного інтелекту й генеративних мовних моделей у сфері інформаційної безпеки держави.

Практичне значення результатів полягає в можливості використання сформульованих положень і висновків у діяльності органів державної влади, безпекових і комунікаційних інституцій під час аналізу інформаційних загроз, удосконалення стратегічних комунікацій, формування підходів до раннього виявлення деструктивних наративів, оцінювання ризиків цифрових платформ і розроблення моделей реагування на інформаційно-психологічний вплив. Результати дослідження можуть застосовуватися в подальших політологічних дослідженнях інформаційної війни, когнітивного впливу та інформаційної безпеки, у роботі аналітичних центрів і експертних платформ, а також у навчальному процесі під час підготовки курсів і навчально-методичних матеріалів з політології, стратегічних комунікацій, інформаційної безпеки та суміжних дисциплін.

Ключові слова: гібридна війна, когнітивна війна, спеціальна інформаційна операція, суспільна свідомість, наратив, дезінформація, соціальні медіа, стратегічні комунікації, інформаційна безпека, пропаганда, асиметричний конфлікт, постправда, штучний інтелект, геополітика, міжнародна безпека.

ABSTRACT

Savchuk V. A. The Information Component of Modern Wars: Leading Narratives and Mechanisms of Influence on Public Consciousness. – Qualifying scientific work submitted as a manuscript.

Dissertation for the degree of Doctor of Philosophy in specialty 052 “Political Science”. – Private Higher Educational Institution “European University”. – Kyiv, 2026.

The dissertation provides a comprehensive political science study of the information component of modern wars, leading narratives, and the mechanisms through which they influence public consciousness. The research focuses on how information confrontation shapes the perception of events, trust in institutions, the formation of beliefs, assessments of political reality, and behavioural patterns among target audiences.

The theoretical and methodological framework combines systems, structural-functional, and comparative approaches with content, discourse, and narrative analysis. Content, discourse, and narrative analysis are used to trace the transition from individual messages to stable meaning structures that affect political judgement and behavioural orientations. The empirical material is supplemented by public expert interviews collected by the author and used interpretatively as sources of expert perspectives on information-psychological influence, strategic communications, digital platforms, and security processes.

The theoretical part of the study traces the evolution of the information component of warfare from early practices of influencing perception and behaviour to contemporary digital and cognitive technologies. Changes in media and communication channels are shown to have been accompanied by a gradual expansion of the objectives of information influence: from mobilising one’s own community, demoralising an adversary, and building external legitimacy to systematic work with the cognitive filters of target audiences. The analysis of foreign and Ukrainian political science discourse identifies hybrid, narrative, and cognitive warfare as interconnected directions in the conceptualisation of contemporary information confrontation and

clarifies the place of Ukraine's experience of countering Russian aggression within this field of research.

The dissertation refines the categorical and conceptual framework of the research, including the content and interrelation of the concepts of the "information component of modern warfare", "special information operation", "information-psychological operation", "cognitive warfare", "narrative", "public consciousness", "destructive information influence", "mechanisms of influence on public consciousness", "information security", "strategic communications", and "cognitive resilience". Cognitive warfare is defined as a broader strategic level of influence on thinking, interpretation, trust, the assessment of political reality, and decision-making. Special information and information-psychological operations are treated as one of the principal operational mechanisms through which such influence is implemented. The dissertation proposes an original five-stage analytical model of the life cycle of a special information operation, encompassing cognitive mapping of the target audience, narrative construction, dissemination, the active phase of influence, and monitoring with subsequent adaptation. Cognitive mapping is distinguished as an independent initial stage that establishes the relationship between audience vulnerabilities, relevant themes and triggers, the interpretation of a message, and a possible response. Application of the model to the Doppelgänger campaign and its subsequent transformation makes it possible to trace the relationship between audience analysis, narrative construction and dissemination, and operational adaptation, while distinguishing operational capacity, intended cognitive influence, and empirically substantiated political consequences.

The analysis of information warfare mechanisms under conditions of new communication technologies systematises the principal tools for detecting and countering destructive influence. The main groups include automated content detection and analysis, network monitoring and bot activity detection, preventive inoculation and media literacy education, and fact-checking and digital verification. Content analysis detects signs of manipulation; network monitoring identifies coordinated activity; inoculation and media literacy education build audience resilience; fact-checking and

digital verification assess claims and materials. Counter-narratives complement these tools by restoring a coherent interpretation of events.

Social media are identified as one of the principal mechanisms of contemporary information-psychological influence. Their role in present-day information-psychological confrontation is associated with the personalisation of information flows, algorithmic agenda-setting, emotional amplification of conflict-oriented content, the formation of digital echo chambers, and the artificial appearance of mass support through bot networks and coordinated activity. This environment combines informational content with social proof, perceptions of group belonging, threat, or moral outrage, thereby strengthening the behavioural effects of messages.

The specificity of cybersecurity under wartime conditions is examined through the relationship between the technical resilience of digital infrastructure, continuity of critical services, institutional coordination, and trust in public institutions. The cybersecurity component of information confrontation includes the protection of data, systems, and communication channels, incident response, the development of human capacity, and interaction between public and security institutions. The study substantiates the relationship between the technical resilience of the digital environment and the state's ability to maintain societal informational orientation during crises and military operations.

The applied part of the dissertation examines the political and legal foundations of protecting Ukraine's information space under conditions of Russian armed aggression. The effectiveness of the state protection system is shown to depend on the coherence of regulatory arrangements, institutional coordination, threat monitoring, legal formalisation of decisions, public communication, and assessment of consequences.

A separate line of analysis concerns the humanitarian components of anti-Ukrainian information and propaganda operations. The principal spheres of influence include historical memory, linguistic and cultural identity, education, religion, symbolic space, value orientations, and social cohesion. Russian humanitarian aggression is examined as systematic pressure on the Ukrainian political community

through the imposition of distorted interpretations of Ukraine's history, statehood, culture, and political agency. The study establishes that the humanitarian component of information confrontation is directly linked to society's capacity to preserve identity, semantic coherence, and readiness for consolidated resistance. Humanitarian security is therefore incorporated into the broader system of national and information security.

The study of strategic communications defines them as an instrument for coordinating threat analysis, state messaging, public explanation of decisions, and the maintenance of trust in institutions. Strategic communications support the proactive formation of explanatory narratives that are comprehensible to society, the coordination of public-sector action, and the reduction of audience vulnerability to destructive influence. Within this logic, cognitive resilience is understood as the capacity of citizens and social institutions to preserve critical perception, recognise manipulative messages, and withstand emotional contagion, information overload, and imposed interpretative schemes.

The dissertation outlines the opportunities and risks associated with artificial intelligence and generative language models in the field of information security. These technologies expand the possibilities for monitoring, classification, analysis, and forecasting of information threats, automate anomaly detection, and support the rapid processing of large data sets. At the same time, personalisation of information flows, variable generation of messages, and the scaling of synthetic content increase the complexity of detecting coordinated inauthentic activity and create new conditions for audience segmentation, polarisation, and the spread of distrust toward information sources. The approach proposed in the dissertation for the use of AI in strategic communications combines technological capacity with data protection, legal and ethical oversight, independent evaluation, and personalised responsibility for decisions. Within the study, the concept of "semantic sovereignty" is used to denote the capacity of the state and society to control critically important language resources, data, and models while preserving international interoperability and openness to independent evaluation.

The scientific novelty of the results lies in the development and application of original analytical tools for studying the information component of modern wars, which make it possible to trace the relationship between target-audience vulnerabilities, the construction and dissemination of narratives, the operational adaptation of information influence, its intended cognitive effects, and empirically substantiated political and behavioural consequences. The integrated political science model performs an integrating function by linking the strategic, operational, semantic, technological, and behavioural levels of analysis. For the first time, an original five-stage analytical model of the life cycle of a special information operation is proposed and applied, with cognitive mapping distinguished as an independent initial stage.

The dissertation improves the categorical and conceptual framework of research; the approach to analysing digital mechanisms of information-psychological influence; the approach to analysing the humanitarian components of anti-Ukrainian information and propaganda operations; and the understanding of information-space protection in Ukraine as a combination of political-legal, organisational, communicative, technological, and humanitarian instruments. The study further develops propositions concerning the political nature of contemporary information confrontation, the argument for cognitive resilience as a resource of national security, scholarly understanding of the role of strategic communications, and the assessment of opportunities and risks associated with artificial intelligence and generative language models in the state information-security domain.

The practical significance of the results lies in the possibility of applying the formulated propositions and conclusions in the work of public authorities, security institutions, and communication bodies when analysing information threats, improving strategic communications, developing approaches to the early detection of destructive narratives, assessing digital-platform risks, and designing response models to information-psychological influence. The findings may also be used in further political science research on information warfare, cognitive influence, and information security, in the work of analytical centres and expert platforms, and in teaching and the

preparation of educational materials in political science, strategic communications, information security, and related disciplines.

Keywords: hybrid warfare, cognitive warfare, special information operation, public consciousness, narrative, disinformation, social media, strategic communications, information security, propaganda, asymmetric conflict, post-truth, artificial intelligence, geopolitics, international security.

СПИСОК ПУБЛІКАЦІЙ ЗДОБУВАЧА ЗА ТЕМОЮ ДИСЕРТАЦІЇ

Праці, у яких опубліковано основні наукові результати дисертації

Статті у наукових фахових виданнях України:

1. Савчук В. А. Інструменти виявлення та подолання деструктивних впливів та пропагандистських наративів інформаційних операцій: типологія, основні характеристики. *Актуальні проблеми філософії та соціології*. 2025. Вип. 54. С. 224–229. DOI: 10.32782/apfs.v054.2025.33.

2. Савчук В. А. Історична еволюція інформаційної складової гібридних воєн: від біблійних текстів до алгоритмів соціальних мереж. *Наукові праці Міжрегіональної Академії управління персоналом. Політичні науки та публічне управління*. 2025. № 2(78). С. 157–162. DOI: 10.32689/2523-4625-2025-2(78)-23.

3. Савчук В. А. Гуманітарні складники антиукраїнських інформаційно-пропагандистських операцій: сучасні домінанти та механізми протидії. *Філософія та політологія в контексті сучасної культури*. 2025. Т. 17, № 2. С. 76–81. DOI: 10.15421/352551.

4. Савчук В. А. Інформаційна складова сучасних воєн у політологічному дискурсі: зарубіжний та український контексти. *Епістемологічні дослідження в філософії, соціальних і політичних науках*. 2025. Т. 8, № 2. С. 198–203. DOI: 10.15421/342557.

5. Савчук В. А. Когнітивна війна: теоретичні засади та інституційна практика. *Регіональні студії*. 2025. № 42. С. 154–160. DOI: 10.32782/2663-6170/2025.42.24.

Тези, опубліковані за матеріалами конференцій

1. Савчук В. А. Стратегії та інструменти інформаційно-психологічного впливу в російській гібридній агресії проти України. *Протидія дезінформації в умовах російської агресії проти України: виклики і перспективи* : тези доп. учасників міжнар. наук.-практ. конф. (Анн-Арбор – Харків, 12–13 груд. 2023 р.). Харків, 2023. С. 286–289. DOI: 10.32782/PPSS.2023.1.74.

2. Савчук В. А. Інформаційні війни як об’єкт міждисциплінарних наукових досліджень. *Сучасна наука: дослідження, економіка та інновації* : зб. наук. праць за матеріалами 3-ї Міжнар. наук.-практ. конф. (Загреб, Хорватія, 22–24 жовт. 2025 р.). Загреб, 2025. С. 282–284. URL: https://isu-conference.com/en/archive/modern-science-research-economy-and-innovation-22-10-25 (дата звернення: 07.08.2026).

ЗМІСТ

ВСТУП 17

РОЗДІЛ 1. ТЕОРЕТИКО-МЕТОДОЛОГІЧНИЙ ВИМІР ІНФОРМАЦІЙНОГО СКЛАДНИКА СУЧАСНИХ ВОЄН 26

1.1. Інформаційна складова сучасних воєн у політологічному дискурсі: закордонний та український контексти 26

1.2. Методологічний інструментарій та категорійно-понятійний апарат дослідження 46

1.3. Спеціальні інформаційні операції як один з основних механізмів впливу на суспільну свідомість та поведінку у воєнних умовах 68

Висновки до розділу 1 83

РОЗДІЛ 2. МЕХАНІЗМИ ВЕДЕННЯ ІНФОРМАЦІЙНОЇ ВІЙНИ В УМОВАХ ПОШИРЕННЯ НОВІТНІХ КОМУНІКАТИВНИХ ТЕХНОЛОГІЙ 87

2.1. Інструменти виявлення та подолання деструктивних впливів та наративів інформаційних операцій: типологія, основні характеристики 87

2.2. Соціальні медіа як механізм інформаційно-психологічного впливу на суспільну свідомість і поведінку 103

2.3. Специфіка застосування механізмів кібербезпеки у воєнних умовах 118

Висновки до розділу 2 130

РОЗДІЛ 3. ІНФОРМАЦІЙНИЙ СУПРОВІД ПРОТИДІЇ РОСІЙСЬКІЙ ЗБРОЙНІЙ АГРЕСІЇ ПРОТИ УКРАЇНИ 134
3.1. Політико-правові засади забезпечення безпеки інформаційного простору України у воєнних умовах 134
3.2. Основні гуманітарні складники антиукраїнських інформаційно-пропагандистських операцій 146
3.3. Основні інструменти російської гуманітарної агресії проти України та протидія їхньому впливу на суспільну свідомість і поведінку 157
3.4. Перспективи впровадження технологій штучного інтелекту в систему стратегічних комунікацій та інформаційного захисту держави 169
Висновки до розділу 3 184
ВИСНОВКИ 188
СПИСОК ВИКОРИСТАНИХ ДЖЕРЕЛ 194
ДОДАТОК А. СПИСОК ПУБЛІКАЦІЙ І ВІДОМОСТІ ПРО АПРОБАЦІЮ 236

ВСТУП

Актуальність теми дисертаційного дослідження зумовлена тим, що в умовах сучасного воєнно-політичного протиборства інформаційна складова сучасних воєн перестала бути допоміжним елементом силового конфлікту і перетворилася на самостійну площину боротьби. У сучасних війнах вирішального значення набуває не лише контроль над територією, ресурсами чи інфраструктурою, а й здатність впливати на способи сприйняття подій, формування переконань, оцінок і моделей поведінки цільових аудиторій. Саме така логіка покладена в основу дисертації, де в єдиному аналітичному полі поєднано питання інформаційної війни, спеціальних інформаційних операцій, когнітивної війни, наративів, стратегічних комунікацій, кібербезпеки, а також ролі штучного інтелекту й генеративних мовних моделей у трансформації сучасного інформаційного впливу.

У зарубіжному науковому дискурсі проблеми пропаганди, масового переконання, дезінформації, гібридної війни, наративного впливу та когнітивного протиборства розробляли Г. Арендт, Ж. Еллюль, Г. Лассвелл, М. Маклуен, Ж. Бодріяр, Ф. Гоффман, М. Ґалеотті, К. Пол, М. Меттьюз, К. Вордл, Х. Дерахшан, Б. Клавері, Ф. дю Клюзель, Й. Розенбек, С. ван дер Лінден, Т. Нюгрен та інші дослідники. Водночас помітну частину сучасного джерельного поля становлять не лише академічні праці, а й офіційні та аналітичні матеріали безпекових і дослідницьких структур, які працюють із цією проблематикою в прикладному режимі. Йдеться насамперед про напрацювання Командування НАТО з питань трансформації щодо когнітивної війни, документи й звіти НАТО зі стратегічних комунікацій, звіти Європейської служби зовнішніх дій щодо іноземного інформаційного маніпулювання та втручання, аналітику EUvsDisinfo, а також матеріали OECD і UNESCO, у яких окремо розглядаються ризики генеративного штучного інтелекту, синтетичної дезінформації та змін в інформаційному середовищі. Це дає підстави стверджувати, що зарубіжний масив досліджень уже охоплює гібридний, наративний, когнітивний,

операційний і технологічний рівні аналізу, але здебільшого розгортає їх як окремі лінії.

В українському науковому середовищі проблеми інформаційної війни, смислового впливу, спеціальних інформаційних операцій, психологічних механізмів маніпуляції, стратегічних комунікацій та інформаційної безпеки розробляли В. Горбулін, Г. Почепцов, В. Зеленін, С. Максименко, Д. Золотухін, М. Каптан та інші автори. Поряд із власне академічними працями, важливе значення для дослідження мають аналітичні доповіді Національного інституту стратегічних досліджень, матеріали Центру протидії дезінформації при РНБО України, Центру стратегічних комунікацій та інформаційної безпеки, а також інших українських структур, що здійснюють постійний моніторинг інформаційних загроз, фіксацію наративів, виявлення інформаційних операцій і підготовку оперативних аналітичних продуктів. Саме це поєднання академічних досліджень із матеріалами структур, які працюють у режимі поточного спостереження за інформаційним середовищем, є принципово важливим для теми дисертації. Воно дозволяє розглядати інформаційну складову сучасних воєн не лише як теоретичну конструкцію, а і як реальний політичний процес, у якому взаємодіють наративи, технології, інституції, гуманітарні чинники й механізми впливу на суспільну свідомість.

За таких умов зберігається потреба у комплексному політологічному дослідженні, яке не розводило б окремо аналіз гібридної війни, дезінформації, спеціальних інформаційних операцій, когнітивного впливу, гуманітарних механізмів агресії, стратегічних комунікацій і технологічних змін, пов’язаних із штучним інтелектом, а поєднувало б їх у межах єдиного дослідницького підходу. Для України ця потреба має особливе значення у зв’язку з тривалою російською агресією, що супроводжується масштабними інформаційно-пропагандистськими операціями, спрямованими не лише на політичну дестабілізацію, а й на підрив історичної пам’яті, ідентичності, ціннісних орієнтирів і суспільної згуртованості. Саме цим визначається актуальність дисертації, у якій поєднано аналіз провідних наративів, спеціальних

інформаційних операцій, когнітивної війни, ролі стратегічних комунікацій, гуманітарних складників антиукраїнських інформаційно-пропагандистських операцій та перспектив використання штучного інтелекту в системі інформаційного захисту держави.

Зв'язок роботи з науковими програмами, планами, темами. Дисертаційне дослідження пов'язане з науково-дослідною темою ПВНЗ «Європейський університет» 0120U105123 «Інституціональний розвиток соціально-політичного простору в умовах глобальної світової нестабільності» (початок виконання – листопад 2020 р., завершення – грудень 2025 р.). У дисертації досліджуються інституційні механізми протидії інформаційно-психологічному впливу, дезінформаційним практикам, інформаційним загрозам і кіберзагрозам. Окрему увагу приділено ролі державних, безпекових і комунікаційних структур у забезпеченні інформаційної безпеки та стійкості суспільної свідомості в умовах гібридної війни. Така проблематика відповідає змістовому спрямуванню зазначеної науково-дослідної теми.

Мета і завдання дослідження. Метою дисертаційного дослідження є комплексне політологічне дослідження інформаційної складової сучасних воєн, провідних наративів та механізмів впливу на суспільну свідомість. Для досягнення поставленої мети визначено такі завдання: 1) дослідити теоретико-методологічні засади аналізу інформаційної складової сучасних воєн у політологічному дискурсі; 2) уточнити категорійно-понятійний апарат дослідження та визначити провідні наративні лінії російського інформаційного впливу; 3) проаналізувати спеціальні інформаційні операції як один з основних механізмів впливу на суспільну свідомість та поведінку у воєнних умовах; 4) з'ясувати механізми ведення інформаційної війни в умовах поширення новітніх комунікативних технологій; 5) визначити роль соціальних медіа як механізму інформаційно-психологічного впливу; 6) розкрити специфіку застосування механізмів кібербезпеки у воєнних умовах; 7) дослідити політико-правові засади забезпечення безпеки інформаційного простору України у воєнних умовах; 8) проаналізувати гуманітарні складники антиукраїнських інформаційно-

пропагандистських операцій; 9) систематизувати основні інструменти російської гуманітарної агресії проти України; 10) окреслити роль стратегічних комунікацій у системі протидії деструктивним інформаційним впливам; 11) обґрунтувати перспективи впровадження технологій штучного інтелекту в систему інформаційного захисту держави.

Об'єкт дослідження – інформаційна складова сучасних воєн як сфера політичного протиборства, у межах якої здійснюється цілеспрямований вплив на суспільну свідомість, політичні оцінки, довіру до інституцій і поведінкові орієнтації цільових аудиторій.

Предмет дослідження – провідні наративи, механізми їх формування, поширення та впливу на суспільну свідомість, а також політичні, комунікаційні й технологічні механізми протидії деструктивним інформаційним впливам у сучасних війнах, з особливою увагою до умов російської збройної агресії проти України.

Теоретико-методологічна основа дослідження зумовлена складністю самого предмета дослідження, оскільки інформаційна складова сучасних воєн постає як явище, у якому політичні, технологічні та соціально-психологічні ефекти тісно переплетені. У цій роботі методологічний інструментарій виконує конструктивну функцію, адже забезпечує внутрішню узгодженість аналізу, впорядковує емпіричний матеріал і дає змогу переходити від опису окремих інформаційних впливів до пояснення їхньої логіки, механізмів і наслідків. Саме тому теоретико-методологічна основа дослідження не зводиться до формального переліку методів, а безпосередньо підпорядкована загальній логіці дисертації та її предметові.

Базовими для дослідження є системний, структурно-функціональний і порівняльний підходи. Системний підхід дає змогу розглядати інформаційну складову війни як сукупність взаємопов'язаних елементів, що діють у змінному середовищі та перебувають у стані постійної взаємодії. Структурно-функціональний аналіз дозволяє зосередитися на ролях, які виконують окремі елементи цієї системи, і простежити, як вони розподіляються між каналами,

організаційними структурами та практиками комунікації. Порівняльний аналіз, своєю чергою, забезпечує зіставлення різних інформаційних кампаній і конфігурацій впливу, що дає змогу відрізняти специфічне від типового та уникати механічного зведення різних за природою явищ до однієї схеми. У такому поєднанні ці підходи формують основний аналітичний каркас дослідження. Для дослідження змісту, організації та поширення смислових конструкцій застосовано контент-, дискурс- і наративний аналіз, що дало змогу простежити перехід від окремих повідомлень до стійких схем політичного тлумачення й поведінкових орієнтацій аудиторій.

Окремий матеріал дослідження становлять публічні експертні інтерв'ю, зібрані автором. У межах дисертації їх залучено інтерпретативно як джерела експертних позицій щодо інформаційно-психологічного впливу, стратегічних комунікацій, цифрових платформ та безпекових процесів. Зміст інтерв'ю співвіднесено з тематичними напрямами, визначеними завданнями дослідження, що дає змогу зіставляти теоретичні й доктринальні положення з практичними фаховими інтерпретаціями. Водночас категорійно-понятійний апарат вибудовується через поєднання нормативно-правового і доктринально-аналітичного рівнів, що дозволяє уточнити зміст ключових категорій і зробити їх придатними для подальшого аналізу емпіричного матеріалу. Таке поєднання методологічних підходів забезпечує цілісність дослідження та створює підстави для послідовного аналізу його теоретичного й емпіричного рівнів.

Наукова новизна одержаних результатів полягає у розробленні та застосуванні авторських аналітичних інструментів дослідження інформаційної складової сучасних воєн, які дають змогу простежувати взаємозв'язок між вразливостями цільових аудиторій, конструюванням і поширенням наративів, операційною адаптацією інформаційного впливу, його цільовим когнітивним ефектом та емпірично підтвердженими політичними й поведінковими наслідками. Цілісна політологічна модель виконує в цій логіці інтегруючу функцію, поєднуючи стратегічний, операційний, смисловий, технологічний і поведінковий рівні аналізу.

Уперше:

– запропоновано та застосовано авторську п’ятиетапну аналітичну модель життєвого циклу спеціальної інформаційної операції, що охоплює когнітивне картографування цільової аудиторії, конструювання наративу, поширення, активну фазу впливу та моніторинг із подальшою адаптацією. Ключовим авторським елементом моделі є виокремлення когнітивного картографування як самостійного вхідного етапу, результатом якого стає визначення зв’язку між вразливостями аудиторії, релевантними темами й тригерами, способом інтерпретації повідомлення та можливою реакцією. Це дає змогу простежити, як результати аналізу аудиторії задають параметри конструювання наративу, а надалі пов’язуються з каналами його поширення, зміною операційних тактик та межами емпірично підтвердженого політичного або поведінкового ефекту; аналітичні можливості моделі продемонстровано на матеріалі кампанії «Doppelgänger» та її подальшої трансформації.

Удосконалено:

– категорійно-понятійний апарат дослідження інформаційної складової сучасних воєн через уточнення змісту та співвідношення основних категорій, необхідних для аналізу провідних наративів і механізмів впливу на суспільну свідомість;

– науковий аналіз механізмів ведення інформаційної війни в умовах поширення новітніх комунікативних технологій, завдяки чому показано роль соціальних медіа, цифрових платформ і алгоритмічних систем у формуванні сучасного інформаційно-психологічного впливу;

– підхід до аналізу гуманітарних складників антиукраїнських інформаційно-пропагандистських операцій, що дозволяє розглядати їх не лише як інструмент політичної дестабілізації, а і як засіб впливу на історичну пам’ять, ідентичність, ціннісні орієнтири та суспільну згуртованість;

– підхід до осмислення захисту інформаційного простору держави як поєднання політико-правових, організаційних, комунікаційних, технологічних і гуманітарних інструментів протидії деструктивному впливу.

Отримали подальший розвиток:

– положення щодо політичної природи сучасного інформаційного протиборства, в якому визначального значення набуває здатність впливати на способи сприйняття реальності, формування переконань та моделі соціально-політичної поведінки;

– аргументація щодо необхідності формування довготривалої когнітивної стійкості суспільства як одного з базових ресурсів національної безпеки;

– наукові уявлення про роль стратегічних комунікацій у системі протидії деструктивним інформаційним впливам;

– оцінка можливостей і ризиків використання технологій штучного інтелекту та генеративних мовних моделей у сфері інформаційної безпеки держави.

Практичне значення одержаних результатів полягає в тому, що сформульовані в дисертації теоретичні положення, уточнений категорійно-понятійний апарат і зроблені аналітичні висновки можуть бути використані не лише в подальших політологічних дослідженнях, а й у прикладній роботі, пов’язаній із протидією деструктивним інформаційним впливам. Насамперед ідеться про можливість використання результатів дослідження у діяльності органів державної влади та безпекових інституцій під час розроблення підходів до захисту інформаційного простору, удосконалення стратегічних комунікацій, аналізу провідних наративів, виявлення механізмів впливу на суспільну свідомість та оцінювання ризиків, що виникають у зв’язку з поширенням новітніх комунікативних технологій. Така спрямованість прямо випливає із загальної логіки рукопису, де результати дослідження пов’язано з проблемами інформаційної війни, когнітивного впливу, стратегічних комунікацій та інформаційної безпеки, а також із практичною діяльністю державних і безпекових структур.

Окреме прикладне значення мають ті результати, які стосуються аналізу спеціальних інформаційних операцій, гуманітарних складників антиукраїнських інформаційно-пропагандистських операцій, ролі соціальних медіа, цифрових

платформ і алгоритмічних систем поширення контенту в сучасному інформаційно-психологічному впливі. У практичній площині вони можуть бути використані для вдосконалення аналітичного супроводу рішень у сфері інформаційної безпеки, для підготовки рекомендацій щодо раннього виявлення деструктивних наративів, для розроблення моделей реагування на інформаційні загрози, а також для посилення спроможності держави поєднувати політико-правові, комунікаційні, технологічні й гуманітарні інструменти захисту. Не менш важливим є і той блок висновків, що стосується стратегічних комунікацій та перспектив використання штучного інтелекту і генеративних мовних моделей, оскільки він може бути врахований під час оновлення підходів до моніторингу, аналізу та прогнозування інформаційних загроз у воєнних умовах.

Практичне значення роботи пов’язане також з її методологічною та освітньою придатністю. Використаний у дисертації підхід до тематичного зіставлення теоретичних і доктринальних положень із публічними експертними інтерпретаціями може бути застосований у подальших дослідженнях сучасного інформаційного протиборства. Положення і висновки дисертації можуть бути залучені до навчального процесу під час підготовки курсів і навчально-методичних матеріалів з політології, інформаційної безпеки, стратегічних комунікацій, інформаційно-психологічного впливу та суміжних дисциплін, а також у роботі аналітичних центрів і експертних платформ, що займаються дослідженням сучасних воєнних і безпекових процесів.

Апробація результатів дисертації.

Основні положення та результати дисертаційного дослідження апробовано у виступах і доповідях на міжнародних науково-практичних конференціях, тематика яких безпосередньо пов’язана з проблемами інформаційної війни, дезінформації та міждисциплінарного вивчення сучасних форм інформаційного протиборства. Зокрема, окремі результати дослідження були представлені на міжнародній науково-практичній конференції «Протидія дезінформації в умовах російської агресії проти України: виклики і перспективи» (Анн-Арбор – Харків, 12–13 грудня 2023 р.) та на 3-й Міжнародній науково-практичній конференції

«Сучасна наука: дослідження, економіка та інновації» (Загреб, Хорватія, 22–24 жовтня 2025 р.). Саме в межах цих наукових заходів було оприлюднено й обговорено підходи до аналізу стратегій та інструментів інформаційно-психологічного впливу в умовах російської гібридної агресії, а також положення щодо розгляду інформаційних війн як об’єкта міждисциплінарних наукових досліджень.

Публікації. Основні положення дисертаційного дослідження викладені у 7 наукових публікаціях, з яких 5 вийшли друком у наукових фахових виданнях України, 2 опубліковано у вигляді тез доповідей на міжнародних науково-практичних конференціях**.**

Структура та обсяг дисертації. Специфіка проблем, що стали предметом дисертаційного дослідження, зумовила логіку і структуру роботи. Робота складається із вступу, трьох розділів, поділених на підрозділи, висновків, списку використаних джерел (335 найменувань) та додатка. Загальний обсяг становить 237 сторінок, із них основний текст – 177 сторінок, список використаних джерел на 42 сторінках.

РОЗДІЛ 1. ТЕОРЕТИКО-МЕТОДОЛОГІЧНИЙ ВИМІР ІНФОРМАЦІЙНОГО СКЛАДНИКА СУЧАСНИХ ВОЄН

1.1. Інформаційна складова сучасних воєн у політологічному дискурсі: закордонний та український контексти

Історія воєн людства нерозривно пов’язана з історією комунікації: від сакральних ритуалів, що формували первісні уявлення про світоустрій, до мережевих платформ, здатних впливати на сприйняття сучасних конфліктів. У межах цього дослідження інформаційна складова війни розглядається як історично змінна система впливу на три групи аудиторій: власну спільноту, противника і зовнішніх спостерігачів. Для власної спільноти вона виконує мобілізаційну та легітимаційну функції. Для противника – функції залякування, дезорієнтації, деморалізації та провокування хибних рішень. Для зовнішніх аудиторій – функцію пояснення війни у вигідній для суб’єкта дії системі координат. Саме така багатовекторність дає підстави розглядати інформаційний вимір війни як сталий елемент воєнного протиборства, що змінював свої носії й технології, але зберігав орієнтацію на сприйняття, очікування, емоції та поведінку. Теоретичне осмислення інформаційної складової сучасних воєн потребує ретроспективної декомпозиції, оскільки феномен організованого збройного насильства від самого початку був нерозривно пов’язаний із розвитком суспільної комунікації. У межах політологічного аналізу ми виходимо з тези, що інформаційний вимір війни не є вторинним чи допоміжним щодо кінетичних дій, а є невід’ємною частиною воєнного протиборства, в площині якої вирішуються питання легітимності, морального домінування та кінцевого політичного результату [1].

Онтологічні витоки цього зв’язку простежуються ще в архаїчних формах людського співіснування. Як показує антропологічний аналіз Б. Генкса, воєнні практики в багатьох ранніх суспільствах були тісно пов’язані з ритуальними та символічними формами [2], проте вже в найдавніших культурах війна поставала як складний комплекс ритуальних та символічних практик. Обґрунтований Дж.

Е. Гаррісон зв’язок слова, ритуалу та дії в класичному міфо-ритуальному просторі [3] дає підстави розглядати символічні практики як важливий складник підготовки, легітимації та переживання колективного насильства. У межах цього дослідження такий підхід дозволяє простежити ранні форми впливу на сприйняття й поведінку, що супроводжували фізичне протиборство. У цьому контексті війна з самого початку постає не лише як фізичне протистояння, а як боротьба за уми, де перемогу здобуває той, хто здатен краще конструювати реальність, підтримувати бойовий дух і деморалізувати супротивника ще до першого удару. Ця закономірність зберігається у наступних історичних епохах, збагачуючись новими засобами. Якщо у доісторичних культурах функцію інформаційної дії виконували ритуали, символи та архетипи, то в біблійній традиції спостерігаємо приклади усвідомленого інформаційно-психологічного впливу. Особливе значення в цій традиції мають образи Божої волі, пророчих снів, страху перед «Божим судом», що виконують роль ранньої політичної пропаганди та маніпуляції. Це дозволяє стверджувати, що інформаційний вплив на ранніх етапах історії людства супроводжував фізичне протиборство: перемога здобувалася не лише мечем, а й здатністю конструювати реальність, яка деморалізує супротивника та підтримує бойовий дух власної спільноти.

Важливим етапом еволюції інформаційного складника є перехід від стихійних ритуалів до усвідомлених стратегій інформаційно-психологічного впливу. Біблійний сюжет про Гедеона та його перемогу над мідіянитянами дає матеріал для авторської гіпотези: цей епізод може розглядатися як один із найдавніших письмово зафіксованих описів інформаційно-психологічної операції проти противника. Підставою для такого трактування є структура самої оповіді. Перед атакою в таборі мідіянитян виникає символічне передчуття поразки: один із воїнів бачить сон про хлібину, що руйнує намет, а тлумачення цього сну пов’язує майбутню катастрофу з Гедеоном [4]. З позицій сучасної політології, дії Гедеона є класичним проявом рефлексивного управління. Свідоме скорочення війська до трьохсот воїнів, використання специфічного акустичного та візуального інструментарію (сурми, смолоскипи, розбивання

глечиків) та експлуатація сакрального наративу, який поєднував Божу волю з діями Гедеона, були спрямовані на створення ілюзії чисельної та божественної переваги [4]. Мідіянитяни реагують на сконструйовану картину загрози, поєднуючи її з уже наявним страхом перед Божою карою. Психологічний ефект, підсилений попередньою роботою зі снами та передчуттями ворога [4], спричинив когнітивний колапс у таборі мідіянитян, зруйнувавши волю до опору ще до вирішального фізичного зіткнення. Для теми нашого дослідження тут важливий сам механізм: інформаційна дія впливає на очікування противника, змінює його оцінку ситуації та створює передумови для поведінкової дезорганізації.

В епоху Античності інформаційний складник воєн зазнав інституціоналізації, стаючи елементом державної політики та військової стратегії. Для аналітичного впорядкування матеріалу в межах цього дослідження доцільно умовно розрізнити дві традиції осмислення впливу у війні.

Західна парадигма (логоцентризм та легітимація). Поліси й імперії, змагаючись між собою, формували наративи, покликані переконати не лише власних громадян, а й сусідні держави і майбутні покоління у правомірності власної агресії, героїзмі захисту чи винятковості цивілізаційної місії. У давньогрецькому світі важливу роль у цьому процесі відігравала розвинена політична риторика, яка, зокрема в часи Перикла (V ст. до н. е.), трансформувала колективну пам’ять про війну в інструмент консолідації громади. Його знаменита «Поховальна промова», яку наводить Фукідід, створює образ смерті як найвищої громадянської доблесті, де загибель на полі бою означає не втрату, а піднесення: захисники полісу загинули не тому, що були слабкі, а тому, що обрали честь [5]. Іншим аспектом є перехід до стратегічного обману як інтелектуальної зброї, уособленої в образі Одіссея. План із «Троянським конем» у Гомеровій «Одіссеї» використовуємо як ретроспективну аналітичну аналогію сучасної спеціальної інформаційної операції, пов’язаної з експлуатацією довіри та символьного навантаження («дар богам») [6].

Стародавній Рим довів практику інформаційного супроводу до рівня

системної державної машини. Юлій Цезар у «Записках про Галльську війну» виступає не лише як полководець, а як стратегічний комунікатор, який через письмові хроніки вибудовував аргументацію на користь нібито безальтернативної римської експансії як засобу забезпечення порядку [7]. За часів імператора Августа цей вплив став візуально-тотальним: через архітектуру, монети та тріумфальні арки формувався простір, у якому кожен громадянин мав не читати, а бачити вічність і непереможність імперії (за П. Занкером [8]).

Східна парадигма (ментальна домінанта). Фундаментом цієї традиції є трактат Сунь-цзи «Мистецтво війни» (VI ст. до н. е.). Він містить один із найдавніших системних викладів принципів обману, дезорієнтації противника та досягнення політичного результату без вирішального фізичного зіткнення [9]. Ці положення можуть розглядатися як рання інтелектуальна передумова сучасного аналізу впливу на сприйняття і рішення, але не як готова концепція когнітивної війни. Практичне використання психологічного тиску в середньовічний період (XIII–XIV ст.) простежується у воєнно-політичних стратегіях Монгольської імперії. Монгольська стратегія демонструє інший історичний приклад системного використання страху, розвідки та поширення перебільшених уявлень про чисельність і жорстокість війська для схилення міст до капітуляції [10]. Контроль над сприйняттям ворога давав змогу досягати стратегічних цілей із меншими фізичними втратами.

Аналіз монгольських методів управління страхом дозволяє провести функціональну паралель із використанням залякування у сучасних конфліктах. У контексті гібридної агресії Російської Федерації психологічний тиск поєднується з воєнними засобами і спрямовується на придушення суб’єктності супротивника. Російська ядерна риторика, примусове ядерне сигналізування та удари по цивільній і критичній інфраструктурі використовуються як інструменти стратегічного залякування [11]. Інформаційний ефект таких дій полягає у спробі вплинути на політичні рішення демократичних суспільств через страх перед подальшою ескалацією. Таке порівняння стосується функціональної подібності залякування і не означає прямої історичної спадкоємності між монгольськими

практиками та інформаційною стратегією Російської Федерації.

Якісна зміна у розумінні інформаційної складової відбулася в епоху Відродження (XIV–XVI ст.) через раціоналізацію та секуляризацію політичної думки. Нікколо Макіавеллі у праці «Державець» (1513 р.) відмовився від релігійного виправдання війни, натомість обґрунтував роль репутації та образу правителя як автономних ресурсів сили. Його концепція поєднання якостей «лева» (фізичний примус) та «лисиці» (інформаційна маніпуляція) стала першим у західному дискурсі теоретичним обґрунтуванням єдності сили та обману. Макіавеллі довів, що для суб'єкта політики здатність «здаватися» (керувати сприйняттям) є більш значущою для утримання влади, ніж реальний стан ресурсів. У сучасному прочитанні Макіавеллі, запропонованому британським істориком політичної думки К. Скіннером, увага зосереджується на політичному значенні репутації, видимих чеснот і керування сприйняттям правителя [12]. У згаданий період відбулася трансформація і в дипломатичній сфері, де складні церемоніали та протокольні заходи почали виконувати функцію приховування реальних стратегічних намірів. Інформація почала сприйматися як ресурс, здатний компенсувати дефіцит воєнної потужності. Поширення друкарства у XV–XVI століттях створило технологічні передумови для переходу від комунікації, орієнтованої переважно на еліти, до значно ширшого тиражування політичних і релігійних наративів. Це радикально змінило масштаби та швидкість поширення воєнно-політичних повідомлень під час конфліктів.

Період Реформації став одним із перших масштабних інформаційних конфліктів ранньомодерної доби, у якому друковані тексти, листівки, сатиричні зображення й релігійна символіка застосовувалися для масового поширення конкуруючих світоглядних позицій. Створення у 1622 році Конгрегації поширення віри (Congregatio de Propaganda Fide) засвідчило подальшу інституціоналізацію системної релігійної комунікації. У XVIII–XIX століттях поширення грамотності та формування національних держав сприяли розвитку централізованих медіасистем. Французька революція використала брошури, бюлетені та агітаційні газети як інструмент мобілізації. У політичній культурі

наполеонівської доби сила друкованого слова вже усвідомлювалася як чинник, здатний конкурувати з воєнним примусом [13]. У Британії політична сатира у вигляді карикатур Джеймса Ґілрея і Томаса Роулендсона набула стратегічного значення: вони формували негативний, відразливий образ ворога і підкріплювали державну позицію [14]. З появою нових візуальних медіа інформаційний вплив став ще більш емоційним. Під час Кримської війни фотограф Роджер Фентон створив серію знімків для британської аудиторії. Його фотографія «The Valley of the Shadow of Death» стала важливим етапом у формуванні візуальної репрезентації війни для широкої аудиторії, поєднуючи документальну претензію з ретельно вибудуваною композицією [15]. Ці матеріали поширювалися через газети та виставки, зближуючи документальну фіксацію з пропагандистським представленням війни. З початком Першої світової війни (1914–1918) інформаційна політика перетворилася на систему державного контролю, а пропаганда – на організовану зброю масового впливу. У Великій Британії 1914 року було створено Бюро воєнної пропаганди, відоме як Wellington House; у 1917 році його функції розширив Департамент інформації, а в 1918 році було утворено Міністерство інформації [16]. Ніколас Рівз характеризує британську воєнну пропаганду як важливий зразок державної координації новинного контролю й кіновиробництва в умовах війни [17]. Одним із найвідоміших продуктів стала документальна стрічка The Battle of the Somme (1916), яку в рік виходу переглянули близько 20 мільйонів людей – майже половина тодішнього населення Великої Британії [18]. У Німеччині пропаганду організовувала військова цензура та відомство закордонних справ. Особливої уваги надавали карикатурам, листівкам і газетам. Історик Девід Велч підкреслює, що Німеччина рано усвідомила значення інформаційного фронту, однак не змогла здобути довіру міжнародної аудиторії [19]. У міжвоєнний період методи пропаганди еволюціонували в ідеологічні машини тоталітарних режимів. Радянський Союз створив індустрію масових кампаній: від плакатів до кіно. Стрічки Сергія Ейзенштейна (Броненосець Потьомкін) і хроніки використовувалися для формування образу «народного героя» та демонізації

ворога. У творчій і теоретичній практиці Сергія Ейзенштейна монтаж поставав не лише як художній прийом, а і як інструмент ідеологічного впливу [20]. Тема інформаційної складової Другої світової війни дуже об'ємна і, водночас, достатньо вивчена. Тому в рамках даного дослідження обмежимось констатацією, що пропаганда перестала бути виключно засобом впливу на тил – її почали використовувати як інструмент безпосереднього ведення війни, що супроводжувалася психологічними та інформаційними операціями на зовнішню й внутрішню аудиторії [21]. У нацистській Німеччині інституалізація пропаганди стала елементом державного управління ще до війни. Із 1933 року діяло Міністерство народної просвіти та пропаганди під керівництвом Йозефа Ґеббельса, яке координувало усі засоби масової інформації, включно з кінематографом, радіо та пресою. У геббельсівській моделі пропаганди контроль над інформаційним середовищем розглядався як засіб формування масової лояльності та політичної мобілізації [22]. Геббельсівська пропаганда зосереджувалася на деморалізації противника, антисемітизмі, виправданні агресії та формуванні культу фюрера, значну увагу приділяючи створенню образу зовнішнього ворога як абсолютного зла – «більшовицької орди» чи «англосаксонських колонізаторів». У Радянському Союзі централізовані методи масової мобілізації формувалися впродовж 1917–1929 років, коли більшовицька влада поєднала партійний контроль, агітацію, пресу, кіно й політичну освіту в єдину пропагандистську систему [23]. У роки Другої світової війни радянська пропаганда спиралася на традиційні й героїчні образи, покликані мобілізувати населення на захист держави [24]. Одним із найвиразніших візуальних символів цієї мобілізації став плакат Іраклія Тоїдзе «Батьківщина-мати кличе!» [25]. У кінематографі одним із найпомітніших прикладів став документальний фільм «Розгром німецьких військ під Москвою», присвячений обороні столиці та контрнаступу [26]. У межах радянської пропагандистської системи кінодокументалістика подавала оборону й контрнаступ як доказ здатності СРСР вистояти й перемогти [24]. У роки війни створювалася нова радянська міфологія, де війна подавалася як світоглядна і моральна боротьба цивілізацій. У США та

Великій Британії пропагандистська діяльність хоч і мала в основі демократичну основу, але так само координувалася на державному рівні. У США в 1942 році створено Відомство воєнної інформації (Office of War Information), яке координувало Голлівуд, радіо, пресу. Наприклад, студія Disney випустила понад 30 агітаційних мультфільмів, включно з Der Fuehrer's Face (1943), який висміював Гітлера [27]. Узагальнюючи підхід Гарольда Лассвелла, можна виокремити три взаємопов'язані умови дієвості воєнної пропаганди: цілеспрямованість повідомлення, його повторюваність та адаптацію до емоційної структури цільової аудиторії [28]. Попри ідеологічну відмінність, усі сторони конфлікту активно застосовували як класичні пропагандистські прийоми, так і інноваційні засоби комунікації для досягнення стратегічних цілей.

Після завершення Другої світової війни світ увійшов у нову фазу глобального протистояння – Холодну війну (1947–1991), що мала характер не стільки прямого збройного конфлікту, скільки масштабної ідеологічної, інформаційної та психологічної боротьби. Саме в цей період інституціоналізується поняття «інформаційної війни» у військових і дипломатичних стратегіях наддержав. У США діяли кілька паралельних механізмів зовнішнього інформаційного впливу. Агентство інформації Сполучених Штатів (USIA), створене 1953 року, координувало публічну дипломатію та мовлення «Голосу Америки» [29]. Окремо функціонували «Радіо Вільна Європа» і «Радіо Свобода», орієнтовані на аудиторії соціалістичних держав і СРСР [30]. СРСР вів активну «антиімперіалістичну» інформаційну кампанію і поширював ідеї соціалізму, використовуючи спонсоровані радянським урядом і партією міжнародні структури, насамперед антиколоніальні й національно-визвольні рухи в Азії, Африці і Латинській Америці. Особливу роль в інформаційному протистоянні відігравали візуальні медіа. Джон Льюїс Гаддіс показує, що телебачення перетворило ключові події Холодної війни – від спортивних змагань до космічних запусків – на видимі для масової аудиторії ідеологічні сюжети [31]. Так, трансляції польоту Юрія Гагаріна у 1961 році або висадки американців на Місяць у 1969 році ставали

інформаційними перемогами для кожної зі сторін. Протистояння капіталістичної і комуністичної ідеології в період Холодної війни неодноразово набувало форми локальних збройних конфліктів, під час яких інформаційна складова ставала фронтом боротьби за глобальну легітимність і підтримку громадськості. У Корейській війні США вперше широко застосували так звані психологічні операції (PSYOP), зокрема, масове розповсюдження листівок із закликами до дезертирства серед північнокорейських солдатів. Під час Корейської війни було поширено понад 2,5 млрд листівок, а також застосовувалося гучномовне мовлення поблизу фронту [32]. Радянська та китайська сторона, у свою чергу, активно транслювали наратив про злочини «американського імперіалізму» і забезпечували фінансову і методологічну підтримку антивоєнних рухів і акцій у всьому світі. В'єтнамська війна продемонструвала, що відносно автономне телевізійне висвітлення могло послаблювати контроль держави над героїзованою інтерпретацією конфлікту. Американський дослідник медіа Деніел Галлін у спеціальному дослідженні взаємодії медіа і держави під час В'єтнамської війни показує, що зі зміною політичного консенсусу телевізійне висвітлення дедалі частіше репрезентувало війну як суперечливу моральну й політичну проблему [33]. Один із найвідоміших знімків – фото Ніка Ута з дівчинкою Кім Фук, що тікає з палаючого села, стало тригером зміни суспільного ставлення до війни. Американський генерал Вільям Уестморленд у своїх мемуарах пов'язував поразку у В'єтнамській війні не лише з воєнними чинниками, а й із втратою підтримки в американському суспільстві [34]. Конфлікт за Фолклендські острови (1982) між Великою Британією та Аргентиною також став прикладом вдалого інформаційного менеджменту. Британська влада суворо контролювала журналістів, формуючи позитивний образ військової кампанії, натомість аргентинський уряд поширював через національні медіа переможні зведення, які виявились неправдивими. Дослідник Філіп Найтлі розглядає Фолклендську війну як приклад кампанії, у якій воєнний успіх супроводжувався ефективним інформаційним контролем і пропагандистським менеджментом [35].

Упродовж двох світових воєн і Холодної війни інформаційна складова набула такого масштабу, що її вже неможливо було пояснювати лише через історію окремих пропагандистських практик. Перед політичною наукою постало питання: яким чином великі людські маси починають бачити війну, ворога, державу і власну участь у конфлікті через образи, підготовлені політичними інституціями, медіа й пропагандистськими структурами. Одним із перших цю проблему вивів у площину політичної науки Гарольд Д. Лассвелл – американський політолог, дослідник політичної комунікації та пропаганди. У роботі «Техніка пропаганди у світовій війні» він розглянув пропаганду Першої світової війни як організовану роботу із символами, емоціями, колективними установками й образом ворога [36]. У такій логіці пропаганда діє через добір тем, повторення, моральне виправдання власної сторони, демонізацію противника, підтримання бойового духу та управління очікуваннями союзників. Значення Лассвелла для аналізу інформаційної складової війни полягає в тому, що він дозволяє побачити пропаганду як технологію політичного цілепокладання, де повідомлення підпорядковане бажаному ефекту в масовій поведінці. Війна в такому підході ведеться також у просторі настроїв, страхів, лояльностей і готовності прийняти певне пояснення насильства. Волтер Ліппман, американський політичний мислитель і дослідник громадської думки, доповнює цей підхід аналізом самого сприйняття. У своїй роботі «Громадська думка» він розглянув громадську думку через проблему опосередкованого доступу людини до політичної реальності [37]. Його ідея ментальних картин політичної реальності дає змогу пояснити, чому масова аудиторія реагує на події через стереотипи, скорочені образи й готові ментальні схеми. Під час війни більшість громадян спирається на медіа, груповий досвід, символи, історичні асоціації, офіційну мову й уже наявні уявлення про загрозу. Звідси випливає важливе уточнення для теорії інформаційної війни: пропагандистський вплив значно частіше підхоплює наявний страх, травму, образ ворога або відчуття несправедливості й надає їм політично потрібного напряму. Лассвелл і Ліппман задають два сумісні рівні аналізу. Перший стосується організації впливу: хто

формує повідомлення, які символи обирає, яку емоцію посилює, яку поведінку очікує отримати. Другий пояснює когнітивну передумову такого впливу: масова свідомість працює через спрощення, стереотипи, довіру до посередників і готові образи політичного світу. У такому поєднанні інформаційна війна постає як боротьба за кероване сприйняття реальності. Її сила визначається здатністю поширити повідомлення й водночас вбудувати його в уже наявну систему уявлень аудиторії про правоту, загрозу, безпеку, зраду та справедливість. Організоване поширення повідомлень і робота з ментальними образами пояснюють початковий рівень масового переконання. Стійкіші форми інформаційного впливу виникають тоді, коли повторювані політичні образи поступово входять у повсякденну мову, освітні практики, моральні оцінки, історичні аналогії та уявлення про належний порядок. У цій площині відкривається значення концепції гегемонії, розробленої італійським політичним мислителем марксистської традиції Антоніо Грамші. У його підході влада утримується через здатність домінантної сили закріпити власне бачення світу як звичне, природне й прийнятне для значної частини суспільства [38]. Для аналізу інформаційної складової війни це дає змогу точніше описати ті випадки, коли пропагандистська теза набуває вигляду самоочевидного здорового глузду: образ ворога, уявлення про історичне право, відчуття цивілізаційної переваги або переконання в неминучості певного політичного порядку стають не окремими повідомленнями, а стабільними схемами сприйняття. Ернст Кассірер, німецько-американський філософ культури й один із провідних дослідників символічних форм, поглиблює цей аналіз через поняття політичного міфу. У праці «Міф держави» він показує, як модерна політика здатна організовувати масову поведінку через символічні конструкції, що апелюють до страху, образу ворога, надії на спасіння, уявлення про вождя, народ або історичну місію [39]. Політичний міф у цьому сенсі діє як готова схема пояснення складної реальності. Він спрощує події, надає їм емоційної визначеності, персоніфікує загрози й переводить політичний вибір у сферу морального обов’язку. Саме тому російські конструкції «історичної єдності», «штучності України», «захисту

російськомовних» або «боротьби з фашизмом» доцільно розглядати як міфологізовані схеми політичного пояснення, через які агресія набуває вигляду нібито природної, історично обґрунтованої та морально виправданої дії.

Тоталітарний досвід XX століття загострив ще одну проблему інформаційного впливу – здатність влади створювати замкнену систему пояснень, у якій факт поступово втрачає статус спільної підстави для судження. Теоретикиня політології Ганна Арендт у «Витоках тоталітаризму» аналізує тоталітарну пропаганду як механізм, що поєднує ідеологію, масову самотність, конспірологічні пояснення, образ ворога й руйнування довіри до спільного світу фактів [40]. Для аналізу інформаційної складової війни ця позиція має принципове значення: організована брехня діє найнебезпечніше тоді, коли вона перестає виглядати як окреме неправдиве повідомлення й перетворюється на цілісну картину реальності. У такій картині будь-який доказ може бути оголошений фальсифікацією, будь-яка критика – ворожою атакою, будь-яка суперечність – підтвердженням змови. Саме за цією логікою сучасні інформаційні операції часто прагнуть не стільки переконати аудиторію в одному факті, скільки позбавити її впевненості в самій можливості відрізнити факт від маніпуляції.

Мішель Фуко, французький філософ і один із найвпливовіших теоретиків влади, знання та дискурсу другої половини XX століття, дає змогу точніше описати інший рівень цієї проблеми. У праці «Археологія знання» він розглядає дискурс як систему правил, що визначає, які висловлювання можуть бути визнані значущими, які інституції надають їм авторитету і в яких межах формується легітимне знання [41]. У контексті інформаційної війни це дозволяє змістити увагу від окремих фейків до боротьби за самі процедури визнання істини: хто має право говорити від імені експертизи, які джерела вважаються надійними, які слова описують подію, де проходить межа між доказом, оцінкою і пропагандистським конструктом. Агресор у такій ситуації атакує не лише зміст повідомлень, а й довіру до інституцій перевірки, професійної журналістики, наукової експертизи та раціональної дискусії. Через це інформаційна складова

сучасної війни охоплює боротьбу за мову опису подій, авторитет джерел і критерії, за якими суспільство відрізняє доказ, оцінку та пропагандистський конструкт. Застосування підходу Фуко до цифрового середовища є авторською інтерпретацією, що дозволяє аналізувати боротьбу за процедури визнання інформації достовірною [41].

Відповідаючи на питання, у який спосіб пропагандистські смисли засвоюються в повсякденній комунікації, французький філософ і соціолог Жак Еллюль, у праці «Пропаганда: формування людських установок» розглядає пропаганду як організований процес пристосування людини до заданого соціального й політичного порядку [42]. Його підхід дозволяє точніше описати механізм накопичувального впливу: аудиторія багаторазово стикається з подібними поясненнями в новинах, політичній мові, експертних коментарях, візуальних образах і групових розмовах, унаслідок чого певна інтерпретація поступово набуває форми практичного орієнтира. У воєнних умовах ця властивість посилюється, оскільки страх, невизначеність і потреба швидко пояснити події роблять суспільство чутливішим до простих, емоційно виразних і повторюваних схем. Для цього дослідження істотним є саме такий механізм: пропаганда передає зміст і водночас виробляє звичку реагувати на події в заданому емоційно-політичному режимі. Коли така звичка стає частиною публічної комунікації, змінюється сама якість суспільного обговорення.

Юрґен Габермас, німецький філософ і соціальний теоретик, у дослідженні публічної сфери пов’язує публічність із можливістю раціонального обговорення спільних справ [43]. У праці про комунікативну дію він розвиває ідею порозуміння як основи суспільної взаємодії [44]. У контексті інформаційної війни ця оптика дає змогу пояснити розсинхронізацію суспільства: спільні критерії доказу слабшають, емоційна мобілізація витісняє аргумент, експертиза дедалі частіше сприймається як маска політичного інтересу, а дискусія перетворюється на зіткнення взаємно закритих позицій. Атака спрямовується на довіру до правил обговорення, джерел і процедур перевірки. У результаті суспільство втрачає здатність виробляти узгоджену оцінку подій саме тоді, коли

така здатність є умовою політичної стійкості.

Теоретичне осмислення пропаганди, дискурсу й публічної комунікації потребує врахування ще одного чинника – самого технічного середовища, у якому повідомлення створюється, поширюється і сприймається. У гайдеггерівському питанні про техніку важливою для цього дослідження є думка про те, що техніка не зводиться до нейтрального інструмента в руках людини. Вона задає певний спосіб відкриття світу, впорядковує те, що може бути побачене, виміряне, використане й підпорядковане дії [45]. У площині інформаційної війни це означає, що канал, платформа, алгоритм, інтерфейс і швидкість поширення повідомлень є частиною самого механізму впливу. Технічне середовище не просто переносить пропагандистський зміст; воно змінює умови його сприйняття, посилює одні реакції, приглушує інші, скорочує час на перевірку й підштовхує аудиторію до швидких емоційних оцінок. Цю логіку в медійному вимірі розгортає Маршалл Маклуен у праці «Розуміння медіа: розширення людини». Його підхід дає змогу точніше побачити, чому інформаційний вплив залежить не лише від змісту повідомлення, а й від форми комунікаційного середовища [46]. Телебачення, радіо, друкована преса, соціальні мережі, короткі відео, месенджери й алгоритмічні стрічки по-різному організовують увагу, пам’ять, темп реакції та емоційну залученість. Для сучасної війни це має безпосереднє значення: одна й та сама теза, подана в офіційному повідомленні, вірусному ролику, анонімному телеграм-каналі або персоналізованій рекомендації, матиме різний політичний ефект. Комунікаційний формат змінює не тільки форму подачі, а й поведінкову траєкторію аудиторії – від короткої емоційної реакції до повторного поширення, участі в конфлікті інтерпретацій або втрати довіри до будь-якого джерела. Жан Бодріяр у «Симулякрах і симуляції» переводить цю проблему у площину заміщення реальності її знаковими копіями. Для нашого дослідження важливим є твердження автора, що політична подія починає існувати для масової аудиторії передусім як медійний образ, монтаж, символ, мем, карта або повторюваний наратив [47]. У таких умовах боротьба точиться вже не тільки за повідомлення

про подію, а за її видимість, емоційний контур і місце в колективному сприйнятті. Симулятивне середовище дає агресорові змогу створювати псевдоподії, імітувати підтримку, продукувати фальшиві голоси «народу», підміняти доказ видовищем і перетворювати політичну агресію на керований спектакль легітимації. Саме тому цифрові інформаційні операції небезпечні не лише кількістю фейків, а здатністю створювати для аудиторії альтернативну сцену реальності, у якій фальсифіковане, змонтоване або алгоритмічно посилене починає діяти як політичний факт.

Отже, політична й соціально-філософська думка ХХ століття формує цілісне теоретичне підґрунтя для подальшого аналізу інформаційної складової сучасних воєн. У політологічному дискурсі було сформовано понятійний апарат, який дозволив описувати пропаганду, підробку фактів, маніпуляцію масовою свідомістю, політичний міф, дискурс, публічну комунікацію та медійне середовище як взаємопов’язані механізми впливу на сприйняття реальності. Задовго до формалізації цих підходів у військових документах саме теоретичне осмислення масової комунікації, влади, ідеології та медіа дало змогу розглядати позиційне зіткнення ідеологій у «сфері смислів», описуючи пропаганду, організовану брехню і маніпуляцію масовою свідомістю як інструменти політичного впливу.

Кінець ХХ ст. став переломною віхою, коли інформаційні операції з дисципліни «психологічної підтримки» перетворилися на повноцінний елемент військового планування. Показовим є перегляд американської воєнної доктрини. Відмінність від попередньої рамки command and control warfare (війни проти систем командування й управління противника) полягала у розширенні самого предмета інформаційного протиборства. У Joint Pub 3-13.1 «Об’єднаній доктрині війни проти систем командування й управління» 1996 року центр уваги зосереджувався на впливі на командування, управління, зв’язок, ухвалення рішень і відповідні інформаційні системи противника [48]. Натомість видання Об’єднаного комітету начальників штабів США Joint Pub 3-13 «Об’єднана доктрина інформаційних операцій» 1998 року вже визначало інформаційні

операції (information operations) як дії, спрямовані на інформацію та інформаційні системи противника із одночасним захистом власної інформації та власних інформаційних систем [49]. Документ підкреслював, що інформаційні операції застосовуються на всіх етапах кампанії, у всьому спектрі воєнних дій і на кожному рівні війни – стратегічному, оперативному й тактичному. Саме в цьому полягала доктринальна зміна: інформаційний компонент почав розглядатися як наскрізна складова спільних операцій, а не лише як підтримка боротьби з командно-управлінськими структурами противника. JP 3-13 також наголошував, що різні спроможності мають бути інтегровані в узгоджену стратегію інформаційних операцій і поєднуватися з повітряними, сухопутними, морськими, космічними та спеціальними операціями. До наступальних спроможностей документ відносив безпеку операцій (OPSEC), військовий обман (MILDEC), психологічні операції (PSYOP), радіоелектронну боротьбу (EW), фізичну атаку або знищення елементів інформаційної інфраструктури, спеціальні інформаційні операції (SIO), а за потреби – атаки на комп'ютерні мережі [49]. Відтак на оперативному рівні США перейшли від розуміння інформаційної складової як «підтримки бойових дій» до концепції, у якій панування в інформаційному просторі визначає успіх спільної воєнної кампанії. Подібна логіка, хоч і з відмінною ідеологічною мотивацією, проявилася у пострадянському безпековому середовищі. Доктрина інформаційної безпеки Російської Федерації 2000 року закріпила інформаційну сферу як окремий об'єкт державної безпеки та визначила зовнішній інформаційно-психологічний вплив серед загроз національним інтересам [50]. Водночас сам документ ще не містив цілісної доктрини наступальних інформаційних операцій; її подальше формування потребує аналізу пізніших воєнних і стратегічних текстів. Статтю начальника Генерального штабу ЗС РФ В. Герасимова «Цінність науки у передбаченні» 2013 року в західній аналітичній літературі часто пов'язували з умовним поняттям «доктрина Герасимова». Водночас це позначення не є офіційною назвою російської воєнної доктрини й радше узагальнює дискусію про поєднання воєнних та невоєнних засобів, інформаційного впливу,

політичного й економічного тиску [51]. Саме ця інтегрована логіка згодом матеріалізувалася у ворожих діях проти України – і в численних ІПСО, спрямованих на обґрунтування необхідності «захисту російськомовних», і в симулякрах «референдумів» на тимчасово окупованих територіях. М. Ґалеотті наголошує, що поняття «доктрина Герасимова» є аналітичним скороченням, а не назвою офіційного російського документа; водночас воно відображає увагу до поєднання військових і невійськових інструментів впливу [52]. Спираючись на український досвід протидії гібридній агресії, у межах цього дослідження доцільно виокремити три практичні аспекти російської моделі: руйнування довіри всередині цільового суспільства через керовану дезінформацію; використання цивільної ІТ-інфраструктури для маскування кібератак; легалізацію постправди як інструменту зовнішньої політики [53].

У 2007 році Френк Гоффман, старший науковий співробітник Національного університету оборони США, запропонував поняття hybrid warfare для опису конфліктів, у яких один актор поєднує конвенційні воєнні спроможності, нерегулярну тактику, терористичні дії та кримінальні практики в єдиному операційному просторі [54]. Інформаційний і психологічний вплив у такій моделі є складниками ширшого поєднання різнорідних засобів, але не вичерпують змісту концепції. Експерти Крістофер Пол і Міріам Меттьюз з некомерційної дослідницької організації RAND Corporation, аналізуючи російську модель пропаганди, визначили її як «пожежний шланг брехні» (firehose of falsehood). Ефективність цієї моделі базується на швидкому й масовому тиражуванні суперечливої інформації, що випереджає можливу верифікацію [55]. У 2025 році Управління головного науковця Організації НАТО з науки і технологій опублікувало дослідницький звіт «Cognitive Warfare», у якому людське пізнання розглядається як дедалі важливіше середовище сучасного протиборства [56]. Документ засвідчує розвиток концепції в дослідницькому середовищі НАТО, але не є затвердженою союзною доктриною.

Аналіз зарубіжних джерел дає підстави вважати, що у західному дискурсі інформаційна складова сучасних війн часто концептуалізується через рамки

гібридної, наративної та когнітивної війни (hybrid, narrative/strategic narrative and cognitive warfare). Водночас поле досліджень лишається термінологічно конкурентним і ширшим за ці три категорії. Другий контур ґрунтовно досліджений у звіті Atlantic Council «Narrative Warfare» (2023), дослідження для якого координувала Ніка Алексєєва. У ньому простежено, як кремлівські та прокремлівські медіа формували взаємопов'язані наративи для виправдання агресії проти України [57]. Інший звіт DFRLab – «Undermining Ukraine» (2023), координований Романом Осадчуком, – аналізує операції, спрямовані на послаблення глобальної довіри до України [58]. Третій теоретичний пласт стосується когнітивної війни. К. Деппе і Г. Шааль у науковій статті 2024 року здійснили політологічний концептуальний аналіз дослідницької концепції когнітивної війни NATO ACT [59]. Шведські дослідники запропонували аналітичну рамку оцінювання стійкості й психологічного захисту, що враховує характер загрози, вразливості, захисні спроможності, координацію, правову основу та оцінювання ефективності [60]. Звіт SCSP аналізує використання Китаєм штучного інтелекту й алгоритмічної персоналізації в когнітивному протиборстві [61]. Матеріали симпозіуму Norwich University звертають увагу на те, що надлишок і суперечливість даних формують сучасний прояв «туману війни», який ускладнює оцінювання ситуації й ухвалення рішень [62].

В українському політологічному середовищі осмислення інформаційної війни стало пріоритетним напрямом після 2014 року, коли анексія Криму та збройна агресія на Донбасі супроводжувалися масштабною інформаційною атакою з боку Російської Федерації. Наукова й аналітична спільнота України розпочала активне розроблення термінів, категорій та теоретичних моделей, спрямованих на пояснення й протидію деструктивному інформаційному впливу. Ключовим у цьому контексті є внесок професора Георгія Почепцова, який у низці праць сформулював підхід до інформаційної війни як війни за смисли, символи та ідеологічні конструкти. Г. Почепцов пов'язує інформаційне протиборство з боротьбою за смислові моделі, через які людина інтерпретує політичну реальність [63]. У цій же семіотичній оптиці професор кафедри

психології Українського державного університету імені Михайла Драгоманова Всеволод Зеленін окреслює український медіапростір як середовище, де зіткнення відбувається насамперед на рівні значень. Всеволод Зеленін пов’язує міфодизайн із конструюванням смислів і символів, здатних дезорієнтувати масову свідомість та посилювати медіатравматичні ефекти [64]. У межах цієї логіки увага переноситься з потоків повідомлень на рамки інтерпретації, через які події набувають емоційного й політичного значення. С. Максименко, М. Назар та Ю. Ірхін виокремлюють когнітивний, емоційний і поведінковий рівні інформаційно-психологічного впливу [65]. Український експерт з медіакомунікацій і кібербезпеки Д. Золотухін наголошує, що протидія дезінформації має бути частиною ширшої стратегії інформаційної безпеки, а не лише оперативним реагуванням на фейки. В інтерв’ю автору цього дисертаційного дослідження Дмитро Золотухін звертає увагу на здатність Росії перетворювати культурні, спортивні й медійні події на інструменти інформаційного впливу [66]. Для позначення цієї технології в експертному дискурсі використовується поняття вепонізації (weaponization). З початком повномасштабного вторгнення Росії у лютому 2022 року сприйняття інформаційної складової російсько-української війни як самостійної і багато в чому вирішальної арени протиборства стає панівним в українському політологічному дискурсі. З такою рамкою сприйняття узгоджується висновок старшого наукового співробітника Центру воєнно-стратегічних досліджень Національного університету оборони України імені І. Черняховського М. В. Каптана, який пов’язує застосування Росією технологій гібридної війни проти України з перетворенням інформаційної сфери на ключову арену протиборства [67]. У цій постановці інформаційна складова війни проявляється як постійний тиск на здатність держави й суспільства утримувати зв’язну картину реальності, не розпорошуючись між конкуруючими смисловими рамками. Водночас у цьому ж полі стає видимою внутрішня вразливість, яку противник експлуатує через швидкість і масштаб інформаційних впливів: «в Україні відсутня єдина дієва мережа Ситуаційних центрів, так Міністерство оборони України не є

виключенням» [67, с. 281]. Ця теза важлива як індикатор того, що інформаційна складова війни в українському контексті осмислюється не тільки як зовнішня атака, а й як проблема цілісності та зібраності інтерпретаційного поля в умовах тривалого протистояння. Той самий вимір війни у публічному медіапросторі набуває форми щоденної протидії фейкам, маніпуляціям і наративам російської пропаганди. У підсумках роботи Центру стратегічних комунікацій та інформаційної безпеки за 2024 рік така діяльність українських урядових і недержавних структур окреслюється як безперервний моніторинг загроз та оперативне спростування найбільш значущих фейкових повідомлень і маніпуляцій [68]. Окремий акцент на щоденному меседжбоксі, покликаному підтримувати політику «одного голосу», фіксує у публічно-аналітичній мові уявлення про війну як безперервний процес смислового тиску, що має власну динаміку й магістральні теми. Водночас дослідження характеризує структурну напругу, властиву для інформаційної війни: противник працює не лише на переконання аудиторій, а й на розсинхронізацію позицій та множення конкуруючих інтерпретацій усередині самого інформаційного поля.

У межах розглянутого масиву зарубіжні праці переважно вибудовують доктринальні та концептуальні моделі гібридної, наративної й когнітивної війни, а також пропонують стандартизовані критерії оцінювання інформаційних впливів. Український дискурс, сформований безпосереднім досвідом російської агресії після 2014 року, більше орієнтований на емпіричні алгоритми швидкої контрдезінформації, горизонтальну мобілізацію суспільства та практичне поєднання державних і громадських механізмів протидії. Таке розмежування відображає домінантні акценти, оскільки обидва дискурси поєднують теоретичні конструкції, прикладні рекомендації та аналіз конкретних кейсів. Правоохоронний контур протидії поступово інтегрує європейську термінологію FIMI: у лютому 2025 року Департамент комунікації МВС за підтримки Консультативної місії ЄС провів навчальну конференцію для комунікаційних підрозділів системи МВС щодо виявлення та протидії іноземним маніпуляціям інформацією [69].

Отже, інформаційна складова сучасної війни є історично тривалим політичним механізмом впливу на сприйняття, довіру, емоції та поведінку цільових аудиторій. Вважаємо, що це поняття доцільно уточнювати через поєднання адресата впливу, політичної функції та очікуваного ефекту. Для власної спільноти визначальними є мобілізація, підтримання легітимності дій і готовності до спротиву. Для противника – деморалізація, дезорієнтація й послаблення волі до опору. Для зовнішніх аудиторій – формування прийнятного пояснення війни, переконання у правомірності дій і моральній перевазі. Історична ретроспектива засвідчує сталість цієї логіки: змінювалися носії, технології та інституційні форми впливу, однак незмінною залишалася боротьба за те, як аудиторія бачить війну, кому довіряє, кого визнає ворогом і які дії вважає виправданими.

У межах такого підходу інформаційну складову війни розглядаємо як багаторівневий політичний процес, що охоплює повідомлення, канали, пропагандистські прийоми, доктринальні моделі та практики протидії. Такий підхід дає змогу чіткіше визначити співвідношення між інформаційною складовою війни, інформаційно-психологічним впливом, наративом і доктринальними моделями інформаційного протиборства. Західний дискурс формує переважно концептуально-доктринальну мову опису, тоді як український досвід російсько-української війни загострює гуманітарний і безпековий зміст цієї проблематики: боротьбу за історичну пам’ять, мовно-культурну ідентичність, державну суб’єктність, довіру до інституцій і здатність суспільства зберігати цілісну оцінку подій під тиском ворожих наративів. У результаті можемо конкретизувати інформаційну складову сучасної війни як процес формування способів сприйняття, оцінювання політичної реальності та поведінкових реакцій суспільства в умовах воєнного протиборства [70].

1.2. Методологічний інструментарій та категорійно-понятійний апарат дослідження

У цьому дослідженні методологічний інструментарій виконує

конструктивну функцію: він забезпечує внутрішню узгодженість аналізу інформаційної складової сучасних воєн як складного явища, де технологічні, політичні та соціально-психологічні ефекти переплетені й не зводяться до одного виміру. Відтак методи, на які спираємося, є способом упорядкування емпіричного матеріалу та дисципліною аргументації, що дозволяє переходити від опису інформаційних впливів до пояснення їхньої логіки, механізмів і наслідків.

Першим опорним підходом є системний аналіз, оскільки він дозволяє розглядати інформаційну складову війни як сукупність взаємопов'язаних елементів, які діють у середовищі постійних збурень і зворотних зв'язків. І. Осадчук у методичних матеріалах із навчальної дисципліни «Теорія політики» акцентує системний підхід серед базових теоретико-методологічних засад політологічного аналізу, ув'язуючи його з дослідженням політичних процесів та інститутів у їхній взаємодії із «середовищем» [71]. Відтак інформаційна складова сучасної війни розуміється як система, де одночасно функціонують актори (державні та недержавні), інфраструктури (медіа, цифрові платформи, канали комунікації, потоки повідомлень), а також процедури їхнього продукування, посилення й корекції. Тривалість інформаційного впливу залежить від того, чи залишається повідомлення разовим подразником, чи входить у повторювану зв'язку джерел, каналів, наративів, емоційних тригерів і поведінкових стимулів. Разовий вплив здатний спричинити короткочасну дезорієнтацію, однак його політичний результат швидко обмежується за умов оперативного спростування, слабкої якості повідомлення, низької довіри до джерела або відсутності підтримувального наративного середовища. Показовим прикладом короткочасного впливу є deepfake-відео із нібито закликом Володимира Зеленського скласти зброю у березні 2022 року: одна з версій відео набрала понад 120 тис. переглядів у Twitter, однак попередження про можливі deepfake-маніпуляції, оперативне спростування Володимира Зеленського та видалення ролика платформами обмежили час його неконтрольованого поширення [72]. Стійка когнітивна схема формується тоді, коли повідомлення багаторазово

повторюється, переноситься між медіа, соціальними мережами, дипломатичними заявами й псевдоекспертними майданчиками, а також прив’язується до вже наявних страхів, упереджень або конфліктів ідентичності. У такій логіці функціонував російський наратив про нібито «американські біолабораторії в Україні»: він просувався через медійні й дипломатичні канали та виносився Росією на рівень Ради Безпеки ООН, де Ідзумі Накаміцу повідомила, що ООН не має відомостей про програму біологічної зброї в Україні [73]. Подібний механізм багатоканального закріплення повідомлень демонструє операція Secondary Infektion, у межах якої фальшиві акаунти, підроблені документи й розміщення матеріалів на сотнях платформ використовувалися для провокування конфліктів між західними державами, атак на критиків Кремля та дискредитації України [74]. У першому випадку системна конфігурація впливу виявилася недостатньою для тривалого закріплення повідомлення; у другому й третьому випадках повторення, багатоканальність, інституційне або псевдоінституційне підсилення та емоційна сумісність із попередніми уявленнями аудиторії підтримували наратив як готову схему пояснення політичної реальності. Саме тому в межах системного підходу ключовим стає конфігурація зв’язків між джерелом повідомлення, каналом поширення, повторюваністю, емоційним резонансом, легітимацією та поведінковим ефектом. Окремо підкреслимо, що інформаційні впливи аналізуються як динамічні процеси, що змінюються у відповідь на контрдії, інформаційні «провали», резонанс у спільнотах і трансформацію політичного контексту.

Структурно-функціональний аналіз доповнює системний підхід і зосереджує увагу на функціях окремих елементів системи та розподілі цих функцій між структурами. У згаданих методичних матеріалах структурно-функціональний підхід подається як компонент методологічної підготовки політичного аналізу, що підсилює здатність пояснювати функціонування політичних інститутів і процесів. У класичній традиції порівняльної політології Ґ. Алмонд пов’язує аналіз політичних систем із логікою структур і функцій, задаючи рамку, релевантну для пояснення того, як елементи політичного

порядку виконують різні ролі в межах системи [75].

Для дослідження інформаційної складової воєн це важливо з двох причин. По-перше, з погляду інтерпретації: замість того щоб описувати сукупність інформаційних повідомлень, розрізняємо їхні функції – мобілізаційні, деморалізаційні, дезорганізаційні, відволікальні або такі, що створюють «шум» і перевантажують увагу. По-друге, це дозволяє відділити наміри від можливостей: одна й та сама функція може реалізовуватися різними структурами (офіційними медіа, мережами ботів, лідерами думок, «експертними» майданчиками), і саме інституційна будова комунікаційного середовища визначає, які канали стають провідними, а які – маргінальними. У результаті структурно-функціональна перспектива дає підстави переходити від опису інформаційних кампаній до пояснення їхньої внутрішньої організації та стійкості.

Третім загальнонауковим інструментом є порівняльний аналіз, який у цій роботі застосовується до кількох взаємопов’язаних рівнів дослідження. На понятійному рівні порівнюються зарубіжні й українські підходи до тлумачення інформаційної війни, спеціальних інформаційних / інформаційно-психологічних операцій, когнітивної війни, наративу, стратегічних комунікацій та інформаційної безпеки. На емпіричному рівні зіставляються різні типи інформаційних кампаній і операцій, передусім ті, що були пов’язані з російською агресією проти України після 2014 року та після початку повномасштабного вторгнення у 2022 році. Таке зіставлення дає змогу відрізняти короткострокові дезорганізаційні впливи від довготривалих наративних конструкцій, спрямованих на зміну довіри до інституцій, сприйняття війни, оцінку союзників і готовність суспільства до спротиву. На інструментальному рівні порівнюються канали й механізми поширення впливу: традиційні медіа, соціальні мережі, месенджери, бот-мережі, псевдоекспертні майданчики, дипломатичні комунікації та алгоритмічні системи підсилення контенту. На рівні протидії зіставляються реактивні практики спростування, превентивні підходи на зразок пребанкінгу, інструменти фактчекінгу, стратегічні комунікації та технологічні засоби моніторингу інформаційних загроз. Д. Коллієр у розділі «The Comparative

Method» підкреслює, що порівняння є фундаментальним інструментом аналізу, який загострює опис і відіграє роль у формуванні понять через виявлення подібностей і контрастів між випадками [76]. Для цього дослідження така логіка має прикладне значення: порівняльна перспектива дозволяє співвідносити інформаційні впливи як зіставні конфігурації змінних – цільові аудиторії, типи наративів, інтенсивність і тривалість впливу, ступінь державної координації, поєднання інформаційного, психологічного й кіберкомпонентів, а також характер протидії. Саме це захищає аналіз від надмірного розширення термінів і дає змогу коректно розмежовувати різні за масштабом явища: фейк, дезінформаційну кампанію, спеціальну інформаційну операцію, когнітивний вплив і стратегічну комунікацію.

Системний підхід задає спосіб бачити інформаційну складову як взаємодію елементів у змінному середовищі та дозволяє коректно формулювати причинно-наслідкові зв’язки без редукції до одного чинника. Структурно-функціональний аналіз деталізує внутрішню організацію цієї взаємодії, розкриваючи, як саме розподіляються ролі між каналами, організаційними структурами й практиками комунікації. Порівняльний аналіз забезпечує перевірку аналітичних категорій на різних прикладах і тим самим підсилює валідність узагальнень у межах заявленого предмета дослідження. Поєднання системного, структурно-функціонального та порівняльного аналізу забезпечує послідовний перехід від визначення елементів інформаційного протиборства до зіставлення їхніх функцій, конфігурацій і проявів у конкретних випадках.

Окрему групу емпіричних матеріалів становлять сім публічних експертних інтерв’ю, оприлюднених на YouTube-каналі «РІЗНІ ЛЮДИ» автора цього дослідження у вересні 2024 – лютому 2025 року. Матеріали відібрано цілеспрямовано за критеріями професійної компетентності респондентів, тематичної відповідності предмету дисертації, публічної доступності та наявності змістових фрагментів, релевантних завданням дослідження. До цільової вибірки включено інтерв’ю з експертами, які мають наукові, аналітичні або практичні напрацювання у сферах інформаційної війни, медіакомунікацій,

інформаційно-психологічного впливу, політичного аналізу, стратегічних комунікацій, суспільної раціональності та ціннісних конфліктів у воєнний час. Експертний статус респондентів визначається через їхню фахову належність до відповідного проблемного поля, наявність публічних аналітичних або наукових робіт та участь у професійних дискусіях. У дисертації інтерв'ю залучено інтерпретативно як джерела експертних позицій, а їхній зміст проаналізовано за тематичними напрямами, визначеними завданнями дослідження. Такий підхід дає змогу зіставляти теоретичні й доктринальні положення з практичними інтерпретаціями інформаційного протиборства.

До пріоритетного масиву емпіричних матеріалів належить інтерв'ю з Дмитром Золотухіним у випуску «Як перемогти в інфовійні?». Його включення до вибірки зумовлене фаховою спеціалізацією респондента у сфері медіакомунікацій, інформаційної безпеки та протидії дезінформації; цей матеріал використано для аналізу практичних уявлень про інформаційну війну, ризики цифрових платформ і механізми протидії деструктивним впливам [66]. До цього ж блоку належить розмова з Всеволодом Зеленіним у випуску «Чому ми програємо інформвійну?», оскільки респондент працює з проблематикою психологічних механізмів впливу, міфодизайну, семантичного протиборства та розпізнавання інформаційно-психологічних операцій; інтерв'ю залучено для аналізу пояснювальних схем щодо ІПСО та механізмів сприйняття інформаційних загроз [77]. Окремий емпіричний сегмент становить інтерв'ю з Сергієм Ягодзінським у випуску «Українська філософія, хейт, війна», оскільки респондент як доктор філософських наук і професор репрезентує філософсько-політологічний рівень осмислення суспільної раціональності, публічного мислення, ціннісних конфліктів і деформацій комунікативного простору у воєнний час [78]. У сукупності ці інтерв'ю дають змогу поєднати теоретико-методологічний аналіз із живим експертним дискурсом і використати його як допоміжний емпіричний матеріал для тематичного зіставлення способів пояснення інформаційних впливів.

Для порівняння політичних інтерпретацій і способів проблематизації

стратегічних рішень сформовано цільову вибірку публічних експертних інтерв'ю. Її межі визначаються професійною компетентністю респондентів, тематичною відповідністю змісту розмов предмету дисертації та репрезентацією різних типів експертного бачення: медійно-комунікаційного, політологічного, дипломатичного й історико-політичного. Матеріали розглядаються як публічні експертні інтерв'ю з тематично структурованою розмовою. Їх використання дає змогу аналізувати способи публічного пояснення політичної реальності, але не передбачає статистичної репрезентативності й обмежується складом гостей та редакційною логікою авторського медіапроєкту.

Інтерв'ю з колишнім першим заступником генерального директора НТКУ Олександром Харебіним на авторському каналі «РІЗНІ ЛЮДИ» залучається для аналізу медійних пояснень, оцінок міжнародного контексту та способів інтерпретації стратегічних рішень у публічному просторі [79]. Підставою для включення цього матеріалу до вибірки є професійний досвід респондента у сфері медіауправління та його здатність пояснювати політичні процеси через логіку комунікацій, інформаційного порядку денного й публічного сприйняття. Інтерв'ю з політологом Олегом Саакяном «Війна, мир і стратегія України» використовується для аналізу сценарних уявлень, аргументів про стратегічне планування, політичну суб'єктність України та можливі траєкторії розвитку воєнно-політичної ситуації [80]. Його включення до вибірки зумовлене фаховою належністю респондента до політологічного аналізу й регулярною участю в експертному обговоренні питань війни, миру та державної стратегії.

Окремий зовнішньополітичний сегмент становить інтерв'ю з колишнім міністром закордонних справ України Павлом Клімкіним, яке використовується для аналізу зв'язку між безпековими темами, міжнародною суб'єктністю України та стратегічними комунікаціями на дипломатичному рівні [81]. Експертний статус респондента в цьому випадку ґрунтується на його практичному досвіді керівництва зовнішньополітичним відомством і участі у формуванні української дипломатичної позиції в умовах російської агресії. Для історико-політичного тла й аналізу смислових аргументів про війну та

ідентичність долучається інтерв'ю з істориком Олександром Палієм «Ми всі скіфи» [82]. Його значення для вибірки полягає в можливості простежити, як історичні сюжети, образи минулого та уявлення про походження політичної спільноти використовуються для пояснення сучасного протистояння, осмислення української суб'єктності та формування уявлень про історичну тяглість і ціннісну єдність українського суспільства.

Міждисциплінарність цього дослідження є необхідною умовою точного опису об'єкта. Інформаційна складова сучасної війни розгортається одночасно на кількох рівнях: від державних інституцій та психології сприйняття до технологічних інфраструктур і публічного мовлення. Обмеження аналізу політичним рівнем спростило б причинно-наслідкові зв'язки [83].

У цьому дослідженні поєднання системного, структурно-функціонального та міждисциплінарного інструментарію обране для узгодженого аналізу політичних, технологічних і соціально-психологічних складників інформаційного протиборства [84]. Така методологічна синергія дозволяє не лише розширити предметне поле, а й суттєво поглибити аналіз складних об'єктів:

– політологія визначає ключових акторів і конфігурації влади;
– соціологія висвітлює групові структури та канали поширення смислів;
– психологія пояснює механізми переконання;
– кібербезпека виявляє технологічні вразливості;
– комунікативістика визначає правила конструювання повідомлень і режими довіри.

Практичний сенс полягає у системному поєднанні теоретичних напрацювань із прикладними методами дослідження. У межах цієї роботи виходимо з того, що сучасний політичний аналіз не може спиратися лише на «логіку наративів» або лише на «логіку платформ». Будь-яка інтерпретація має проходити процедуру узгодження, де політичні цілі корелюють із технологічними каналами, а психологічні механізми – з реальною архітектурою цифрової комунікації. Така методологічна композиція дозволяє уникнути

однобічності: як техно-детермінізму (коли все зводиться до алгоритмів), так і суто риторичного пояснення (коли ігнорується роль інфраструктури). Інформаційні впливи розглядаються як цілісний результат взаємодії політичної волі, соціальних умов, когнітивних особливостей та цифрових інструментів. Саме цей синтез і формує емпіричну реальність сучасної інформаційної війни.

Щоб кожне поняття можна було операціоналізувати в подальшому аналізі емпіричного матеріалу й не підміняти наукову роботу декларативними означеннями, доцільно поєднати нормативно-правовий рівень, на якому значення термінів визначається відповідними актами, і доктринально-аналітичний рівень, де категорії використовуються для опису реальних практик інформаційного протиборства. Такий підхід узгоджується з доктринальним баченням НАТО, у якому стратегічні комунікації розуміються як управлінська функція командування, що виходить із розуміння інформаційного середовища й на основі цього організовує застосування комунікаційних засобів для формування установок і поведінки цільових аудиторій [85].

У роботі «інформаційний простір» позначає сферу циркуляції повідомлень і смислів, тоді як «інформаційне середовище» – ширшу сукупність аудиторій, акторів, технологічних систем, інформації та процесів взаємодії між ними. У доктринальному аналізі перевага надається терміну «інформаційне середовище» [85].

Поняття «стратегічні комунікації» доцільно трактувати як інтегративну категорію, що дозволяє описувати узгодженість між політичними цілями, комунікаційними рішеннями та публічними діями сторін конфлікту. Доктринальний підхід визначає стратегічні комунікації як узгоджене використання дій, образів і слів для досягнення поведінкових ефектів у релевантних аудиторіях. Це дає змогу в подальших розділах розглядати стратегічні комунікації як спосіб управління ефектами в інформаційно-психологічному вимірі воєн.

Термін «наратив» у цьому дослідженні потрібний як місток між мовними конструкціями та поведінковими наслідками, адже залучення цієї дефініції

пояснює, як окремі повідомлення складаються в послідовну картину подій для цільових аудиторій і задають очікувані схеми оцінювання та реагування. У концептуально-доктринальному забезпеченні НАТО наратив розуміється як усний або письмовий виклад подій та інформації, упорядкований у логічну послідовність з метою впливу на поведінку цільової аудиторії [85]. Для подальшого аналізу інформаційної складової сучасних воєн це означає, що наративи мають розглядатися не як декоративні «історії», а як інструменти закріплення пояснювальних схем, що підштовхують аудиторію до передбачуваних оцінок і дій.

У межах цього дослідження «провідність» наративу визначається не статистичним рейтингом його поширеності, а сукупністю аналітичних ознак. До провідних відносимо наративи, які стабільно відтворюються в різних кампаніях і каналах, зберігають стратегічну політичну функцію впродовж тривалого часу, адаптуються до кількох цільових аудиторій і повторно виявляються в розглянутих емпіричних кейсах. Такий критерій дозволяє відрізнити стійку смислову конструкцію від ситуативного повідомлення або одиничного інформаційного вкиду. Відповідно, поняття «провідні наративи» використовується як аналітична категорія для позначення стійких і стратегічно значущих смислових ліній інформаційного протиборства, а не як результат суцільного кількісного ранжування.

Під «суспільною свідомістю» у межах роботи розуміємо сукупність відносно стійких способів колективного сприйняття й оцінювання політичної реальності, що проявляються через довіру до інституцій, уявлення про легітимність і загрозу, історичну пам’ять, ідентичність, ціннісні орієнтації та поширені поведінкові установки. Це робоче визначення не ототожнює суспільну свідомість із громадською думкою або індивідуальними когнітивними реакціями: суспільна свідомість описує ширший рівень відносно стійких інтерпретаційних схем, тоді як громадська думка фіксує ситуативні оцінки, а індивідуальні реакції становлять один із рівнів формування колективних ефектів. У подальшому аналізі вплив на суспільну свідомість описується через зміни або

спроби змінити довіру, оцінювання подій, ідентифікаційні орієнтири й поведінкові установки; наявність такого впливу в конкретному випадку фіксується лише в межах даних, які його емпірично підтверджують.

Поняття «дезінформація» та «мізінформація» є ключовими для розмежування умисних і неумисних форм поширення хибних повідомлень, а отже для коректного опису механізмів впливу й відповідальності акторів. У міждисциплінарному підході, запропонованому Клер Вордл і Хосейном Дерахшаном, мізінформація описується як поширення хибної інформації без наміру завдати шкоди, тоді як дезінформація описується як свідоме створення або поширення хибної інформації з наміром завдати шкоди. Таке розмежування дозволяє в подальшому аналізі не підміняти різні явища універсальним ярликом і відділяти помилку, маніпуляцію та організовану операційну діяльність [86].

Інструменти протидії дезінформації в понятійному апараті доцільно систематизувати як превентивні та реактивні практики, зокрема через зв’язок між інокуляцією, пребанкінгом і дебанкінгом. У дослідженні Розенбека, ван дер Ліндена та Нюгрена пребанкінг подано як превентивну інтервенцію, що спирається на теорію психологічної інокуляції та використовує аналогію з імунізацією для формування стійкості до типових маніпулятивних прийомів. Пребанкінг слід трактувати як технологію попередження, коли аудиторії заздалегідь демонструють типові прийоми введення в оману, щоб зменшити їхню ефективність у реальних інформаційних атаках [87].

Трактування категорії «кібербезпека» в межах дослідження ґрунтується на нормативно-правовому підході, що дозволяє чітко окреслити технічні та організаційні межі захисту цифрового середовища. Для подальшого аналізу інформаційної складової сучасних воєн це важливо, тому що кібербезпека визначає технічний рівень захисту цифрового середовища, який у гібридних конфліктах часто працює синхронно з інформаційно-психологічними впливами, але не зводиться до них [88].

Особливе місце в понятійному апараті посідає категорія «когнітивна війна», яка дає змогу простежити перехід від маніпулювання інформаційними потоками

до цілеспрямованого впливу на сприйняття, оцінювання та ухвалення рішень.

Інституціоналізація поняття «когнітивна війна» у стратегічних документах і публічних комунікаціях відбувається за умов відсутності усталених дефініцій і вимірюваних метрик. Через це у безпековому дискурсі зберігається концептуальна та інституційна невизначеність. Не розмежовано належним чином cognitive warfare, класичні інформаційно-психологічні операції (PSYOPS) і кібероперації. Відсутність узгодженої системи показників, яка б дозволяла оцінювати когнітивну перевагу, породжує розрив між доктринальними інтенціями і практичними режимами стратегічних комунікацій.

Для України, яка перебуває під постійним інформаційно-психологічним тиском з боку агресора, незалежно від інтенсивності кінетичної складової протистояння з Росією, це ускладнює розробку національних механізмів протидії і інтеграцію когнітивного виміру в систему безпеки [89].

Після анексії Криму (2014) та початку гібридної агресії на Донбасі в українській науковій спільноті почався поступовий перехід у розумінні інформаційної війни: від акценту на технологіях передачі повідомлень до дослідження впливу на самі механізми мислення індивіда та масових аудиторій. У низці досліджень, починаючи з 2015 року, з’являються перші спроби концептуалізувати гібридну агресію Росії, в тому числі як війну за людську свідомість і вигідне агресору сприйняття дійсності. Так, у 2015 р. один із провідних українських фахівців у сфері комунікативних технологій професор Георгій Почепцов акцентував, що інформаційна війна фактично спрямована на психічний ефект у свідомості людей, а інформаційні потоки є лише засобом досягнення цього результату [90].

У дослідженні «Інформаційне супроводження російської гібридної агресії в Донбасі (2014–2016)» О. Курбан характеризує інформаційне супроводження російської агресії як цілеспрямований вплив на світоглядні настанови аудиторії та наголошує на ролі соціальних онлайн-мереж у поширенні таких повідомлень [91]. У межах цього дослідження наведені положення можна інтерпретувати як опис окремих механізмів, які згодом увійшли до концептуалізації когнітивної

війни.

Розуміння інформаційної складової сучасної гібридної війни як «битви за свідомість» отримало розвиток у наступних дослідженнях української наукової спільноти. У статті «Війна в когнітивному просторі» Георгій Почепцов зміщує акцент із руху інформації на боротьбу за наративи та когнітивний простір. У цьому ж тексті автор використовує поняття «інформаційна бульбашка» і «когнітивна безпека», обґрунтовуючи, що когнітивний простір є ціллю інформаційного впливу як у мирних політичних процесах, так і у воєнній ситуації [63].

У 2020–2021 роках NATO Innovation Hub активізував дослідницькі ініціативи щодо когнітивної війни. Fall Innovation Challenge 2021 був спрямований на пошук технологічних і організаційних рішень для захисту когнітивної сфери, однак не означав її доктринального визнання шостим операційним доменом НАТО [92].

Важливий етап концептуалізації пов’язаний із дослідницькою працею Б. Клавері та Ф. дю Клюзеля, підготовленою в середовищі NATO Innovation Hub. Автори визначають когнітивну війну як використання технологічних засобів для зміни когнітивних процесів обраних цілей [93, с. 2]. Це визначення має характер експлораторної концепції, а не затвердженої доктрини Альянсу. У межах цієї концепції об’єктом впливу стають процеси сприйняття, пам’яті, емоційного оцінювання, формування переконань і ухвалення рішень, а технологічні засоби розглядаються як інструменти їхньої цілеспрямованої модифікації.

У 2010-х концепт взяла на озброєння Народно-визвольна армія Китаю (НВАК). У часописі Народно-визвольної армії Китаю PLA Daily викладач Академії військових наук Китаю Ян Цуньше ґрунтовно досліджує поняття «когнітивна війна» разом із визначенням «операції в когнітивному домені». У своїй статті «Аналіз характеристик та тенденцій розвитку операцій когнітивної області» від 16 серпня 2022 р. автор розкладає поняття «когнітивної війни» на три складники: «когнітивна перевага» – спроможність нав’язати ворогові власний образ ситуації, «когнітивне придушення» – руйнування здатності

супротивника до раціональної оцінки та «когнітивне формування» – довгострокове конструювання вигідної ворогові системи цінностей. Автор обґрунтовує, що саме когнітивний простір виступає базовим майданчиком для конвертації військової переваги у політичний результат. Відтак консолідація зусиль військового та політичного керівництва у межах когнітивного протиборства спрямована на здобуття права визначати характер діяльності, контролювати її перебіг і оцінювати фінальний результат [94]. У відповідь на доктринальний зсув у науково-політологічному дискурсі керівництво КПК здійснило кардинальні організаційні перетворення в структурі китайських збройних сил. У квітні 2024 року КНР офіційно оголосила про формування нового роду військ – Сил інформаційного забезпечення (Information Support Force), покликаних консолідувати кібер-, електронну та когнітивну проєкцію сили для досягнення когнітивної переваги на рівні театру та стратегії. Аналітики Asian Military Review підкреслюють, що нова служба має забезпечити безперервний ланцюг від збору даних до модифікації сприйняття, тобто перехід від інформаційної інтеграції до безпосереднього впливу на процеси мислення опонента [95]. Можемо стверджувати, що китайський підхід демонструє найпослідовніше інституційне оформлення когнітивної сфери як окремого бойового домену й виводить «битву за свідомість» на рівень окремого виду військ.

Помітним внеском у поширення поняття в українському публічному дискурсі стала публікація Дмитра Золотухіна 2021 року, у якій когнітивну війну розглянуто через образ «шостого поля бою» [96]. Водночас у нормативно-правовому полі України цей термін не отримав усталеного визначення. Для кращого розуміння того, як інформаційний сигнал перетворюється на зміну поведінки, доцільно звернутися до трьох дисциплін, що конвергували у XXI столітті: когнітивної психології, нейронаук і поведінкової економіки. У цьому теоретичному трикутнику когнітивна психологія пояснює архітектуру мислення, нейронауки досліджують механізми уваги, емоційного кодування й пам’яті, а поведінкова економіка показує, як архітектура вибору впливає на рішення без

прямого примусу. Д. Канеман розрізняє швидкий, автоматичний та інтуїтивний режим мислення (Система 1) і повільний, контрольований та ресурсомісткий режим (Система 2) [97]. За умов дефіциту часу й уваги люди частіше покладаються на автоматичні оцінки, що підвищує значення способу подання інформаційного сигналу. Для операторів інформаційно-психологічних дій критично утримати аудиторію в рамках Системи 1, адже тоді повідомлення минає свідомий контроль. Будь-яка успішна когнітивна атака прагне залишитися в полі «швидкого мислення», де сигнал приймається підсвідомо і миттєво конвертується у поведінку. Другий наріжний камінь когнітивного впливу – ефект ілюзорної правди (illusory truth effect), що описує зростання сприйняття достовірності твердження внаслідок його повторення. Його вперше системно продемонстрували Л. Гашер, Д. Голдстайн і Т. Топпіно: повторне пред'явлення правдоподібних тверджень підвищувало їхню суб'єктивну достовірність [98]. Подальше дослідження Л. Фаціо та співавторів показало, що повторення підвищує оцінку правдивості тверджень навіть тоді, коли учасники мають знання, що їм суперечать [99]. Г. Пеннікук, Т. Кеннон і Д. Ренд встановили, що попереднє ознайомлення з неправдивими новинними заголовками підвищувало оцінку їхньої точності під час повторного пред'явлення [100].

У практичному контексті механізми уваги й пам'яті безпосередньо пов'язані з функціонуванням соціальних мереж. В експерименті Ф. Чіоссі та співавторів взаємодія зі стрічкою коротких відео TikTok погіршувала виконання завдання на проспективну пам'ять порівняно з умовами Twitter, YouTube і відсутності медіаактивності. Автори пов'язують результат із поєднанням короткого відеоформату та швидкого перемикання контекстів [101]. Такі ефекти можуть підсилюватися технологіями поведінкової економіки. Зокрема, концепція «архітектури вибору» (choice architecture), запропонована Річардом Талером і Кассом Санстейном, передбачає не прямий примус, а м'яке «штовхання» (nudge) до певної дії через структурування інформаційного середовища – порядок опцій, візуальні акценти та короткі підказки [102]. У когнітивних операціях такі підштовхування можуть використовуватися як

мікротригери, що спрямовують увагу й полегшують прийняття певної інтерпретації повідомлення. Для аналізу когнітивної вразливості важливими є три взаємопов'язані чинники:

1. швидкість автоматичної обробки сигналу, яка підвищує роль первинної інтуїтивної оцінки [97];
2. повторюваність повідомлення, що посилює відчуття знайомості та суб'єктивної правдивості [98];
3. емоційна значущість, яка впливає на увагу, кодування та збереження окремих деталей повідомлення [103].

У контексті інформаційного впливу застосування генеративного ШІ ґрунтується на здатності моделей швидко створювати й варіювати повідомлення, локалізувати їх для різних аудиторій та масштабувати повторне поширення контенту [61]. Завдяки цьому механізми автоматичної обробки, знайомості й емоційної активації можуть послідовно використовуватися в інформаційних кампаніях.

Великі мовні та мультимодальні моделі можуть знижувати вартість масового створення, локалізації й варіювання текстового та візуального контенту. У поєднанні з даними про аудиторії та платформними механізмами поширення це створює можливості для масштабнішої персоналізації інформаційного впливу, однак її фактичний рівень у конкретній операції має встановлюватися емпірично [61]. А. Гассан і С. Барбер показали, що зростання частоти пред'явлення твердження від одного до 27 разів посилює ефект ілюзорної правди за логарифмічною залежністю, причому найбільша зміна спостерігається після другого пред'явлення [104]. Генеративні відеосистеми переводять текстові наративи у візуальну сферу. Створені за їхньою допомогою deepfake-ролики ускладнюють розмежування факту й вигадки та підвищують когнітивні витрати на перевірку візуальної інформації. У fMRI-дослідженні Кунгуй Су та співавторів перегляд персоналізованих TikTok-відео супроводжувався вищою активацією окремих компонентів мережі пасивного режиму мозку та вентральної тегментальної ділянки порівняно з

неперсоналізованими відео [105]. Цей результат вказує на зв'язок персоналізації з процесами самореференції та системою винагороди, але сам по собі не доводить формування стійкої поведінкової залежності. Виходячи з наведеного, можемо стверджувати, що ядром когнітивної війни є персоналізовані тригери, багаторазове підкріплення й емоційна петля, які поступово змінюють мисленнєві схеми аудиторії. У практиці російських інформаційно-психологічних кампаній проти України це проявляється через поєднання трьох механізмів: адаптації повідомлень до очікувань конкретних аудиторій, автоматизованого або напівавтоматизованого підсилення через соціальні мережі та використання мультимедійного контенту, який надає маніпулятивному повідомленню емоційної переконливості. У дослідженні Д. Гайслер, Д. Бера, Н. Прелльохса і С. Фойеррігеля проаналізовано 349 455 проросійських повідомлень у Twitter за період після початку повномасштабного вторгнення; автори встановили, що ці повідомлення отримали близько 251 тис. ретвітів і потенційно охопили приблизно 14,4 млн користувачів, а 20,28 % поширювачів були класифіковані як боти, причому значна частина таких акаунтів була створена на початку вторгнення [106]. Підвищену бот-активність зафіксовано в Індії, Південній Африці та Пакистані – державах, які утрималися під час голосування за резолюцію Генеральної Асамблеї ООН ES-11/1 [106]. У межах цього дослідження така географія поширення розглядається як ознака диференційованої роботи з міжнародними аудиторіями, однак не дає підстав безпосередньо встановлювати мотиви або ставлення населення цих країн.

Мультимедійне підсилення цього впливу добре ілюструє російська операція в TikTok, спрямована на дискредитацію колишнього міністра оборони України Олексія Резнікова та ширше – українського керівництва. У межах цієї кампанії тисячі фейкових акаунтів поширювали короткі відео щонайменше сімома мовами, у яких за допомогою AI-озвучки, зображень вілл, автомобілів, фотографій українських посадовців і візуальних натяків на розкіш просувався наратив про нібито збагачення української еліти під час війни [107]. За даними DFRLab і BBC Verify, TikTok видалив понад 12 800 акаунтів, пов'язаних із цією

операцією; сама платформа охарактеризувала її як найбільшу інформаційну операцію, виявлену на TikTok [107]. У цьому випадку мультимедійний формат виконував когнітивно-підсилювальну функцію: зображення предметів розкоші, синтетична озвучка й короткий відеомонтаж створювали у глядача відчуття «наочного доказу», хоча самі твердження були побудовані на сфабрикованих або непідтверджених зв'язках. Саме така комбінація візуального сигналу, емоційного контрасту й алгоритмічного поширення схиляла аудиторію до потрібної агресору оцінки – сприйняття України як корумпованої держави, що нібито не заслуговує на подальшу міжнародну підтримку.

У ширшому міжнародному контексті подібна адаптація повідомлень простежується у зміні російських наративів залежно від аудиторії. Аналітики Digital Forensic Research Lab у звіті Atlantic Council Undermining Ukraine: How Russia widened its global information war in 2023 зазначають, що Росія у 2023 році активніше використовувала TikTok, Telegram та інші соціальні платформи для розширення міжнародної аудиторії, особливо в країнах Глобального Півдня, де російські державні медіа зберігали помітну присутність. У цьому ж аналізі показано, що російські операції поєднували координовані неавтентичні мережі, експлуатацію регіональних образ на Захід, підроблені документи та локалізовані версії антиукраїнських наративів [108]. У такий спосіб російський інформаційний вплив підбирає аргументи, образи й канали під конкретне середовище сприйняття, а потім підсилює їх бот-мережами, псевдоекспертними майданчиками, відеоформатами та платформними алгоритмами. Звіт DFRLab показує, що російські кампанії адаптували наративи, аргументи й канали до конкретних регіональних аудиторій [108]. У межах запропонованого понятійного апарату такі практики можна інтерпретувати як когнітивно орієнтовані операції, оскільки їхньою метою є зміна способів оцінювання війни, довіри до джерел і готовності підтримувати певні політичні рішення.

Чітке категоріальне розмежування понять є необхідною умовою аналізу механізмів реалізації інформаційної складової сучасних воєн. У сучасному науковому дискурсі терміни «інформаційна війна», «кампанія з дезінформації»

та «операція» нерідко вживаються як синоніми, що суттєво розмиває аналітичну перспективу й заважає ідентифікувати специфічні загрози. Проте принциповим є розрізнення стратегічного рівня війни як загального стану протиборства та операційного рівня – як серії дискретних, раціонально керованих актів впливу.

Якщо інформаційна війна (Information Warfare) може розглядатися як глобальна парадигма або, у підході Джеффрі Едгара, викладача Військово-морського коледжу в Ньюпорті (США), як стратегія досягнення вирішальної переваги через контроль над інформаційним простором [109], то спеціальна інформаційна операція (СІО) виступає як операційний механізм, що забезпечує конвертацію стратегічного замислу у площину цілеспрямованої трансформації когнітивних установок та поведінкових моделей об’єкта впливу. У цьому контексті СІО є складною формою впливу з чітким вектором спрямованості. Вихідною точкою для розуміння природи СІО є її виражена суб’єктність та високий ступінь організованості. На відміну від регулярного «фонового» впливу, СІО завжди має конкретного виконавця, визначені ресурси та багаторівневу структуру. Це дозволяє нам інтерпретувати спеціальну інформаційну операцію як активну цілеспрямовану атаку на когнітивну систему цільової аудиторії, де інформація використовується як зброя прецизійного ураження.

Суттєвого значення для методологічної цілісності аналізу набуває категоріальне окреслення поняття СІО та простеження його генези у вітчизняному безпековому дискурсі. Нормативним тлом цього понятійного поля була Доктрина інформаційної безпеки України 2009 року [110]. У сучасному вітчизняному безпековому дискурсі поряд використовуються поняття «спеціальна інформаційна операція» та «інформаційно-психологічна операція» [111]. Вони позначають організовані й цілеспрямовані дії інформаційного впливу, однак не повинні механічно ототожнюватися: обсяг понять залежить від конкретного нормативного, доктринального або аналітичного контексту. НАТО визначає PSYOPS як заплановані дії із застосуванням комунікацій та інших засобів щодо схвалених аудиторій для впливу на їхнє сприйняття, установки й поведінку [112]. Г. Почепцов пов’язує спеціальні інформаційні операції з

керованим конструюванням смислів і впливом на процеси ухвалення рішень [113]. У цій площині ознака «спеціальності» вказує на залучення нетривіальних каналів, засобів цифрової мімікрії та технологій маніпулювання.

Для глибшої систематизації матеріалу запропонуємо розширену ієрархічну модель рівнів інформаційної присутності агресора.

1. «Фоновий» інформаційний вплив: тривале насичення простору ідеологемами, що формує базове середовище сприйняття. Це стратегічний рівень пропаганди, який готує підґрунтя для того, щоб агресивні кроки сприймалися цільовою аудиторією як логічні або неминучі. Прикладом такого впливу є багаторічне просування російською владою ідеологеми про «історичну єдність» росіян та українців, штучність української державності й нібито органічну належність України до російського історико-культурного простору. В аналізі Центру східних досліджень статтю В. Путіна 2021 року розглянуто як ідеологічне заперечення самостійної української політичної суб'єктності [114].
2. Інформаційна кампанія: відкрита або напівприхована повторювана діяльність, що має чіткий тематичний центр, визначені цільові аудиторії, систему поширення повідомлень і проміжні показники ефективності. Прикладом такого рівня є кремлівська кампанія, спрямована на поглиблення напруження між Володимиром Зеленським і Валерієм Залужним та загальну дискредитацію українського військово-політичного керівництва. У розслідуванні The Washington Post на основі внутрішніх кремлівських документів показано, що в січні 2023 року групі російських посадовців і політичних технологів було поставлено завдання закріпитися в українських соціальних мережах для поширення дезінформації; серед ключових цілей називалися дискредитація військового й політичного керівництва України, розкол української еліти, деморалізація військових і дезорієнтація населення [115]. Ця кампанія мала власні кількісні показники: зокрема, звіти фіксували виробництво понад 1300 текстів і 37 тис. коментарів на тиждень, а окремі вкиди, пов'язані з темою можливого

політичного протиставлення Залужного Зеленському, збирали мільйони переглядів у соціальних мережах [115]. Такий приклад демонструє інформаційну кампанію як системну роботу з повторюваною темою, мережевою інфраструктурою, цільовими аудиторіями й регулярним моніторингом ефектів.

3. Спеціальна інформаційна операція: тактичний або оперативний механізм, у межах якого обмежена за часом і простором сукупність спеціально підготовлених інформаційних дій спрямовується на швидкий дезорганізаційний, емоційний або поведінковий ефект. Показовим прикладом є розсилка фейкових SMS- і Telegram-повідомлень мешканцям Харкова навесні 2024 року, коли на тлі концентрації російських військ біля кордону люди отримували нібито офіційні попередження із символікою ДСНС про загрозу оточення міста та необхідність виїхати до визначеної дати. Reuters наводить оцінку начальника поліції Харківської області Володимира Тимошка, який назвав такі повідомлення психологічною операцією, спрямованою на провокування паніки; український безпековий посадовець також повідомив, що Росія часто використовувала пристрої, прикріплені до БПЛА «Орлан-10», зокрема системи «Леєр-3», які імітують базові станції мобільного зв’язку й дають змогу масово надсилати повідомлення на телефони в зоні дії [116]. Цей приклад відрізняється від інформаційної кампанії вузькою прив’язкою до конкретної аудиторії, часу, географії та бажаної поведінкової реакції: мешканців Харкова намагалися схилити до панічного виїзду з міста саме в період підготовки російського наступу на північному сході України.

У такій логіці фоновий вплив створює довготривале смислове середовище, інформаційна кампанія концентрує це середовище довкола конкретного політичного сюжету, а спеціальна інформаційна операція використовує підготовлені наративи й технологічні засоби для швидкого впливу на поведінку визначеної аудиторії. Саме це розмежування дозволяє уникнути механічного ототожнення різних рівнів інформаційного протиборства й точніше описувати

їхню роль у впливі на суспільну свідомість.

К. Пол і М. Швілле використовують еволюцію сил спеціальних операцій як організаційну модель для розвитку спеціалізованих інформаційних сил [117]. У цій дисертації, з огляду на термінологічну неоднорідність джерел, запроваджується робоче розмежування: «СІО» використовується для позначення ширшої організаційно-операційної категорії, а «ІПСО» – під час аналізу конкретних практик інформаційно-психологічного впливу. Це розмежування має аналітичний, а не загальнообов'язковий доктринальний характер.

Для систематизації зазначених категорій та подолання термінологічної розмитості в сучасному безпековому дискурсі, понятійний апарат дослідження запропоновано структурувати через ієрархічну трирівневу модель аналізу інформаційної присутності акторів. Такий підхід дозволяє чітко розмежувати довготривалий «фоновий» вплив, тематично центровану інформаційну кампанію та оперативно-тактичний рівень спеціальних інформаційних операцій. Розведення стратегічного цілепокладання та конкретних дискретних дій дає змогу розглядати інформаційну складову воєн як динамічний політичний процес, що розгортається в різних просторово-часових масштабах.

Теоретико-методологічну основу аналізу когнітивної війни розширено через поєднання підходів когнітивної психології, поведінкової економіки та досліджень цифрових платформ. Це дає змогу зіставляти автоматичну обробку інформації, ефекти повторення, архітектуру вибору та технологічне масштабування повідомлень без зведення когнітивного впливу до одного універсального механізму.

Публічні експертні інтерв'ю залучено інтерпретативно як допоміжний емпіричний матеріал для зіставлення теоретичних і доктринальних положень із практичними оцінками інформаційного протиборства. Їхній зміст аналізувався за тематичними напрямами, визначеними завданнями дослідження. Публічний експертний дискурс використовується для порівняння теоретичних і доктринальних положень із практичними інтерпретаціями російської агресії, але не розглядається як самодостатня процедура їхньої верифікації. Сформована

методологічна композиція створює аналітичну основу для подальшого аналізу структури, динаміки та провідних наративів інформаційно-психологічного протиборства.

1.3. Спеціальні інформаційні операції як один з основних механізмів впливу на суспільну свідомість та поведінку у воєнних умовах

Якщо когнітивна війна визначає стратегічну логіку впливу на сприйняття, установки та процеси ухвалення рішень противника, її прикладна реалізація здійснюється через скоординовані інформаційно-психологічні кампанії та когнітивні атаки. Йдеться про узгоджені дії, спрямовані на емоції, судження й поведінку цільових аудиторій, що використовують традиційні та цифрові технології й розгортаються також нижче порога збройного конфлікту [59]. Виходячи з цієї логіки, СІО доцільно розглядати як цілісну систему взаємопов'язаних дій, об'єднаних спільним задумом і послідовністю впливу.

Теоретична декомпозиція СІО дає змогу виокремити її фундаментальну архітектуру, у якій ініціатор визначає політичну або воєнну мету, а безпосередні виконавці забезпечують її реалізацію в інформаційному середовищі. У межах робочої моделі ініціаторами виступають державні інституції, розвідувальні органи та спеціалізовані підрозділи інформаційної боротьби. Для ускладнення атрибуції вони залучають проксі-структури: ботоферми, мережі анонімних медіаресурсів та агентів впливу, інтегрованих в інформаційне поле об'єкта. Така організація підтримує «правдоподібне заперечення» причетності ініціатора та знижує ризик санкцій, дипломатичної, економічної або іншої відповіді.

Об'єкт спеціальної інформаційної операції у контексті когнітивної війни розглядається як складна багаторівнева система. Мішенню виступають окремі індивіди, соціальні групи та когнітивні фільтри суспільства – ціннісні орієнтири, історична пам'ять і довіра до державних інститутів. Одним із цільових результатів СІО є послаблення здатності аудиторії відрізняти перевірені відомості від маніпулятивних інтерпретацій. Наслідком такого впливу стає ерозія соціальної згуртованості та спроможності суспільства до консолідованого

спротиву й раціонального ухвалення рішень у кризових ситуаціях.

Відкритість джерела дає змогу розмежувати відкриту державну пропаганду і приховані операційні форми впливу. Спеціальний характер СІО визначається координацією дій, конкретним політичним або воєнним цілепокладанням та маскуванням суб'єкта, наміру чи механізму впливу. Прикладом відкритої державної пропаганди є підручник з історії Росії для 11 класу за редакцією В. Мединського та А. Торкунова, у якому виправдовується російська агресія проти України та глорифікуються її учасники. У травні 2026 року Шевченківський районний суд міста Києва заочно засудив редакторів видання за сприяння впровадженню російських освітніх стандартів і пропагандистських матеріалів на тимчасово окупованих територіях України [118].

На противагу відкритій пропаганді, спеціальна інформаційна операція поєднує маскування стратегічного наміру, суб'єкта або каналів впливу зі скоординованим поширенням повідомлень. У міжнародному операційному середовищі показовим прикладом є викрита французькою державною службою VIGINUM, що діє при Генеральному секретаріаті з питань оборони та національної безпеки Франції, мережа «Portal Kombat». У лютому 2024 року VIGINUM описала щонайменше 193 сайти, які автоматизовано збирали та поширювали проросійські матеріали, імітуючи локальні новинні ресурси для аудиторій у європейських країнах [119]. У вимірі безпосереднього впливу на українське суспільство релевантним кейсом є операція «Texonto», ідентифікована аналітиками міжнародної компанії з кібербезпеки ESET як російська психологічна операція, спрямована на громадян України. Вона реалізовувалася через хвилі електронних розсилок, замаскованих під технічні або інформаційні повідомлення українських установ. Їхній зміст експлуатував побоювання щодо перебоїв з опаленням, дефіциту медикаментів і продовольства, посилюючи панічні настрої та недовіру до спроможності державних інституцій [120].

Латентність є базовим принципом спеціальної інформаційної операції. Вона охоплює приховування джерела, стратегічного наміру та механізму впливу.

Об’єкт сприймає нав’язані судження й рішення як результат власного осмислення, оскільки деструктивні наративи маскуються під природні суспільні дискусії, спираються на реальні внутрішні суперечності та поширюються через канали з високим рівнем довіри. Н. Новицька, В. Петрик і В. Кудико визначають спеціальну інформаційну операцію як «спланованої дії, спрямовані на ворожу, дружню або нейтральну аудиторію з метою схилення до прийняття управлінських рішень або/та вчинення дій, вигідних для суб’єкта інформаційного впливу» [121, с. 106]. Це визначення підкреслює цільову спрямованість СІО та її орієнтацію на поведінковий результат. Ще однією ознакою спеціального статусу СІО є синергія багатоканального впливу. Політичні повідомлення, матеріали анонімних медіаресурсів, вірусні відео та висловлювання лідерів думок взаємно підкріплюють один і той самий маніпулятивний конструкт. Повторення схожих тез через формально різні канали створює враження широкого суспільного підтвердження та знижує готовність аудиторії до перевірки. Показовим є Portal Kombat: ресурси цієї мережі масово передруковували матеріали з російських і проросійських джерел, завдяки чому одна теза багаторазово відтворювалася через пов’язані сайти [119]. Для користувача така структура створювала враження збігу оцінок у різних медіа, хоча джерельна база залишалася спільною.

В умовах когнітивної війни спеціальні операції спрямовуються також на створення стану стратегічної дезорієнтації. Тактика «інформаційного шуму» передбачає продукування взаємовиключних версій однієї події та виснаження уваги об’єкта впливу. У межах цієї логіки надлишок суперечливих повідомлень ускладнює перевірку відомостей, посилює недовіру до джерел і створює сприятливі умови для емоційного маніпулювання. Цільовим ефектом стає зниження якості суспільних та управлінських рішень. Отже, СІО становить один із прикладних інструментів когнітивної війни, через який технологічні засоби поширення поєднуються з використанням психологічних закономірностей сприйняття.

Доктринальна рамка сучасних операцій у когнітивній сфері, які здійснює

Російська Федерація, спирається також на радянські розробки у сфері рефлексивного управління. Володимир Лефевр – радянський і американський психолог та математик, який працював у Каліфорнійському університеті в Ірвайні, – сформував засади рефлексивної теорії. У спільній статті В. Лефевр і Джонатан Девід Фарлі – математик, пов'язаний на час публікації з Центром міжнародної безпеки і співробітництва Стенфордського університету, – пояснюють рефлексивну теорію як напрям математичної психології, розроблений на початку 1960-х років і використаний радянським військовим істеблішментом. На відміну від раціоналістичних припущень теорії ігор, ця модель виходить із того, що суб'єкт діє відповідно до власного образу світу та уявлення про образ світу опонента [122, с. 636]. У монографії «Алгебра сумління» В. Лефевр формалізував багаторівневу модель суб'єкта, у якій уявлення про себе й іншого включаються до процесу оцінювання ситуації та вибору дії [123]. Ефективність рефлексивного впливу залежить від логічної сумісності повідомлення з картиною світу адресата. Суперечність із попередніми уявленнями створює умови для переходу до повільнішої аналітичної обробки, яку Д. Канеман позначає як Систему 2 [97]. У 1990-х роках концепт рефлексивного управління був адаптований до військової сфери фахівцями інформаційних структур Генерального штабу РФ. Американський військовий аналітик Тімоті Томас, який спеціалізується на радянських і російських військових студіях, визначає російський підхід так: «рефлексивне управління – це засіб передачі партнеру або супротивнику спеціально підготовленої інформації, яка схиляє його добровільно ухвалити заздалегідь заплановане рішення, бажане для ініціатора дії» (переклад автора) [124, с. 237]. Посилаючись на С. Іонова, Т. Томас наводить чотири базові методи передавання інформації противнику з метою впливу на його рішення [124, с. 244–245]:

1. тиск силою – застосування переваги, демонстрація сили, психологічні атаки, ультиматуми, погрози санкціями, провокаційні маневри та інші дії, що звужують простір рішень противника [124, с. 244–245];
2. подання неправдивої інформації про ситуацію – приховування реального

стану сил, створення хибних об’єктів, блеф щодо озброєння, зміна способу дій, підривні дії та провокації [124, с. 244–245];

3. вплив на алгоритм ухвалення рішення противником – систематичне відтворення очікуваних схем дій, поширення навмисно викривленої доктрини, вплив на елементи системи управління й ключових осіб, передавання хибних вихідних даних [124, с. 244–245];
4. зміна часу ухвалення рішення – несподіваний початок бойових дій або передавання інформації про аналогічний конфлікт, що підштовхує противника до поспішного вибору [124, с. 244–245].

Сучасні російські ІПСО, основним каналом поширення яких стали соціальні мережі, у даному дослідженні аналізуються за авторською схемою «посів – внутрішнє відтворення – посилення» (англ. seed – mirror – amplify). Її ілюструє справа Voice of Europe, яку у березні 2024 року викрила чеська Служба безпеки та інформації (Bezpečnostní informační služba, BIS) – внутрішня розвідувальна служба Чеської Республіки, відповідальна за збирання й оцінювання інформації, важливої для безпеки держави. За даними BIS, цей медійний майданчик фінансувався з Російської Федерації та використовувався для впливу на громадську думку в європейських країнах [125]. Російські тези набували вигляду внутрішньої європейської дискусії завдяки участі європейських політиків і коментаторів, яким Voice of Europe надавав медійний простір. У травні 2024 року Рада Європейського Союзу – інституція ЄС, у якій уряди держав-членів беруть участь в ухваленні законодавства та координації політик Союзу, – запровадила санкції проти Voice of Europe, визначивши його як онлайн-медіа, залучене до системної міжнародної кампанії маніпулювання інформацією для дестабілізації України, Європейського Союзу та його держав-членів [126]. «Етична алгебра» Лефевра передбачає вплив через структуру вибору, що зближує її з концептом «підштовхування» (англ. nudge). У логіці Річарда Талера та Касса Санстейна вплив реалізується через зміну архітектури вибору, яка спрямовує людину до бажаного рішення зі збереженням формальної свободи вибору [102]. У воєнному вимірі цифрові реакції користувача – перегляд, уподобання або поширення –

стають сигналами для подальшого налаштування інформаційного середовища. На нашу думку, концепт «підштовхування» і практики рефлексивного управління сходяться у спільній точці – цілеспрямованій зміні умов, у яких адресат інтерпретує ситуацію та ухвалює рішення. Дослідження Texty.org.ua, незалежного українського медіа, що спеціалізується на журналістиці даних, показало майже лінійну залежність між мовою попередніх переглядів та мовою рекомендацій YouTube на основі даних 205 українських і 122 польських користувачів [127]. Для інформаційного впливу це означає, що попередня поведінка користувача поступово звужує коло тем, голосів і пояснень, представлених у його стрічці.

Наступним логічним кроком у розгортанні аналітичної моделі спеціальних інформаційних операцій є їхня функціональна типізація, що дозволяє структурувати різнорідні методи впливу за вектором їхньої спрямованості та тривалістю очікуваного ефекту. Класифікація СІО повинна відображати динаміку адаптації суб’єкта-агресора до вразливостей конкретного суспільства. Оскільки когнітивна війна оперує передусім сенсами та сприйняттям, типологія операцій будується навколо того, який саме аспект свідомості чи соціальної взаємодії має бути деформований у процесі впливу.

Першим критерієм визначаємо домінантний вектор деструктивної дії. За ним розрізняємо дестабілізуючі, дезорієнтуючі та дискредитуючі операції. Дестабілізуючі впливи спрямовані на ерозію внутрішньої стійкості державної системи та розхитування суспільного консенсусу. Ю. Найдон, С. Наумюк та їхні співавтори пов’язують деструктивний інформаційний вплив із порушенням стабільності функціонування держави та її конституційного ладу через системне маніпулювання суспільною думкою [128]. У межах запропонованої типології цільовим ефектом таких операцій є послаблення здатності соціальних інститутів виконувати свої функції в умовах внутрішнього розколу та хаотизації протестних настроїв.

Дезорієнтуючі операції спрямовані на механізми аналізу й ухвалення рішень. Чед Бріггс, професор Університету Джонса Гопкінса, та Юрій Даник,

доктор технічних наук і професор, показують, що когнітивні операції в умовах гібридного протиборства використовують інформаційне й кіберсередовище для впливу на процеси ухвалення рішень [129]. У межах авторської типології інформаційний шум, суперечливі дані та викривлені повідомлення розглядаються як засоби ускладнення оцінювання ситуації й підвищення ризику помилкових рішень. Окремий сегмент становлять дискредитуючі операції, мішенню яких є довіра як складник соціального капіталу. У листопаді 2023 року український фактчекінговий проєкт StopFake зафіксував поширення deepfake-відео, у якому особа, схожа на тодішнього Головнокомандувача Збройних сил України Валерія Залужного, нібито закликала до непокори командуванню та виступу проти Президента України [130]. У даному дослідженні цей кейс віднесено до дискредитуючих операцій, спрямованих на формування уявлення про розкол між політичним і військовим керівництвом. Окремим різновидом дискредитації є атака на національні символи. У січні 2025 року EUvsDisinfo зафіксував дезінформаційне повідомлення, у якому український тризуб і напис «Слава Україні» на одязі помилково називали нацистськими символами [131]. У цьому випадку об’єктом ураження стає символічна основа державної ідентичності: національний герб, історична пам’ять і мова публічної солідарності. Н. Нетеса та В. Мокляк розглядають спеціальні інформаційні операції як складну багатоетапну систему заходів у структурі гібридної війни [132]. У запропонованій типології атаки на посадових осіб і національні символи віднесено до дискредитаційного напряму.

За часовим горизонтом розрізняємо реактивні та стратегічні СІО. Реактивні СІО є короткостроковими «бліц-операціями», прив’язаними до конкретної події, тоді як стратегічні СІО підтримують багаторічний вплив. Реактивні операції орієнтовані на швидку зміну настроїв під час виборів, техногенних катастроф або воєнних загострень. Прикладом такої «бліц-операції» стала російська кампанія навколо нібито підготовки Україною «брудної бомби» восени 2022 року. У жовтні 2022 року російські посадовці почали поширювати твердження про підготовку Україною радіологічного пристрою на власній території. Цей сюжет

з’явився на тлі воєнного загострення на півдні України й був розрахований на негайний психологічний ефект: посіяти страх перед ядерною ескалацією, поставити під сумнів дії українського керівництва та змусити західні уряди реагувати на російський порядок денний. Міжнародне агентство з атомної енергії (International Atomic Energy Agency, IAEA) провело інспекції на трьох українських об’єктах на запит уряду України й 3 листопада 2022 року повідомило про відсутність ознак незадекларованої ядерної діяльності або матеріалів [133]. Короткий часовий цикл, прив’язка до конкретної фази бойових дій і спрямованість на швидку зміну міжнародного сприйняття дають підстави розглядати цей випадок як реактивну інформаційну операцію.

Стратегічні операції підтримують сталу інтерпретаційну рамку протягом тривалого часу, адаптуючи її до нових подій і політичних обставин. Виразним прикладом є російський наратив про «нацистську Україну». За оцінкою EUvsDisinfo, цей сюжет став одним із наріжних елементів прокремлівської дезінформації від протестів Євромайдану 2013–2014 років, коли проєвропейський виступ українського суспільства почали описувати як «нацистський переворот» [134]. Надалі цей наратив використовувався для дискредитації української державності, армії, національних символів і громадянської мобілізації. У 2022 році він був включений у виправдання повномасштабної агресії через тезу про «денацифікацію» України. У даному дослідженні стратегічний характер операції визначається її тривалістю й адаптивністю: один і той самий смисловий каркас застосовувався до різних подій, від Майдану й війни на Донбасі до оборони України після 24 лютого 2022 року. Цільовим результатом такого впливу є закріплення образу України як «небезпечного» й «нелегітимного» утворення, проти якого нібито допустимі силові дії.

Методологічна різноманітність СІО дозволяє виділити операції, у яких спеціальний характер впливу маскується через інформаційний привід, медіа-двійники, фальшиві громадські ініціативи або внутрішніх ретрансляторів. Олександр Верголяс, дослідник Науково-дослідного інституту інтелектуальної

власності, звертає увагу на роль інформаційного приводу в маскуванні спеціального характеру операції [135]. Для поширення деструктивних наративів використовуються внутрішні ретранслятори або проксі-актори – публічні особи, журналісти, політичні коментатори чи лідери думок, чия впізнаваність і формальна належність до інформаційного простору цільової держави підвищують довіру до повідомлення. Їхня участь дозволяє подавати зовнішній наратив як елемент внутрішньої суспільної дискусії.

На нашу думку, релевантним прикладом використання proxy instrument (проксі-інструмента) в українському медіаполі є діяльність телеведучої та блогерки Діани Панченко, колишньої ведучої заблокованих за рішенням РНБО телеканалів «112 Україна», NewsOne та ZIK. Її публічна риторика в українському інформаційному просторі відтворювала ключові тези російських інформаційних операцій під виглядом «захисту свободи слова», «пацифізму» та «критичного аналізу дій влади». Впізнаваність української журналістки й доступ до легального медійного майданчика сприяли ретрансляції тез про «зовнішнє управління країною», «громадянський конфлікт на Донбасі» та «штучність мовного питання» як елементів внутрішньої дискусії. У січні 2023 року Служба безпеки України повідомила Д. Панченко про підозру у виправдовуванні збройної агресії РФ та поширенні матеріалів, що підтримували російську пропаганду. Наведені факти дають підстави в межах авторської інтерпретації розглядати її медійну діяльність як використання впізнаваного українського комунікатора у ролі проксі-інструмента російського інформаційного впливу [136]. Іншим механізмом є astroturfing – імітація низової громадської ініціативи. У 2016 році СБУ повідомила про блокування спроб російських спецслужб створити в регіонах України фейкові «народні ради», замасковані під локальні громадські рухи та спрямовані на дестабілізацію ситуації [137].

Технологію розмивання істини визначаємо як «стратегію множинних версій». Її логіка полягає в одночасному поширенні великої кількості суперечливих повідомлень, що ускладнює перевірку інформації та орієнтацію аудиторії; така характеристика відповідає описаній К. Полом і М. Меттьюз

російській моделі «пожежного шланга брехні» [55]. У межах спеціальної інформаційної операції множинність пояснень створює когнітивне перевантаження, виснажує увагу та послаблює довіру до можливості встановити перевірену версію події. Показовим прикладом стала російська інформаційна кампанія навколо масових убивств цивільного населення в Бучі навесні 2022 року, яку Європейська служба зовнішніх справ розглядає в контексті іноземного інформаційного маніпулювання [138]. У межах цього дослідження множинність версій розглядаємо як засіб відволікання уваги від установлених фактів, розмивання відповідальності та ускладнення консолідованої політико-правової реакції.

Розглянуті типи СІО відрізняються цілями, тривалістю та механізмами впливу. Дестабілізуючі операції спрямовуються на стійкість інститутів і суспільний консенсус, дезорієнтуючі – на якість оцінювання ситуації та ухвалення рішень, дискредитуючі – на довіру до посадових осіб, інституцій і символів. Функціональна та часова типологія створює підґрунтя для аналізу повторюваних етапів підготовки, поширення й адаптації інформаційного впливу. Це дозволяє перейти до авторської моделі життєвого циклу СІО.

Для систематизації матеріалу в даному дослідженні пропонується авторська п’ятиетапна модель життєвого циклу СІО: когнітивне картографування аудиторії, конструювання наративу, поширення, активна фаза впливу та моніторинг із подальшою адаптацією. Модель має аналітичний характер: у конкретних операціях її етапи накладаються, повторюються або реалізуються паралельно.

Першим і принципово важливим етапом авторської моделі є когнітивне картографування цільової аудиторії. Під ним розуміємо системний аналіз особливостей аудиторії, що визначають її сприйнятливість до інформаційного впливу. Йдеться про страхи й очікування, стійкі переконання, ціннісні орієнтири, рівень довіри до державних і суспільних інституцій, звичні джерела інформації та суперечності, що вже існують у певній соціальній групі. Завдання цього етапу полягає у визначенні тих особливостей сприйняття політичної реальності, через

які певне повідомлення може набути для аудиторії переконливості.

Такий підхід спирається на дослідження психологічних механізмів інформаційного впливу. Хілкка Гран, дослідниця факультету інформаційних технологій Університету Ювяскюля (Фінляндія), та Джеймс Паммент, дослідник Інституту психологічного захисту Лундського університету (Швеція), показують, що операції впливу використовують обмеження уваги, особливості пам'яті, емоційні реакції, когнітивні упередження та особливості ухвалення рішень [139]. Для нашої моделі це важливо, оскільки одна й та сама інформація може сприйматися по-різному залежно від уже сформованих переконань, емоційної реакції та способу оцінювання повідомлення.

Результатом когнітивного картографування стає не формальний опис аудиторії, а визначення зв'язку між її конкретною вразливістю, темою або тригером, способом інтерпретації повідомлення та можливою реакцією. Саме цей зв'язок задає вихідні параметри для наступного етапу – конструювання наративу. У такому розумінні когнітивне картографування відрізняється від звичайної сегментації аудиторії: воно спрямоване на пояснення того, чому певний наратив може бути прийнятий конкретною групою і через які особливості її сприйняття він здатний впливати на оцінювання подій, довіру та подальшу поведінку.

Запропонована модель співвідноситься з поширеними підходами до структурованого аналізу інформаційних операцій. У методології Європейської служби зовнішніх справ рамка ABCDE використовується для впорядкування характеристик інформаційного впливу, тоді як DISARM забезпечує стандартизований опис його тактик і технік [138]. Авторська модель не дублює ці класифікаційні функції: її предметом є послідовність розгортання СІО та функціональний перехід від аналізу аудиторії до конструювання, поширення, активізації й адаптації наративного впливу. Ключовою відмінністю є виокремлення когнітивного картографування як самостійного вхідного етапу, на якому встановлюється зв'язок між вразливістю аудиторії, релевантним тригером, очікуваною інтерпретацією та можливою реакцією. Отже, ABCDE і

DISARM використовуються для опису ознак, тактик і технік інформаційної активності, тоді як запропонована модель слугує для реконструкції внутрішньої логіки життєвого циклу СІО та перевірки зв'язків між її етапами.

На основі отриманого когнітивного профілю починається другий етап – конструювання деструктивного наративу. Чед Бріггс і Юрій Даник зазначають, що в архітектурі когнітивної війни інформація використовується як інструмент впливу в реальному часі [129]. Наратив пристосовується до вразливостей аудиторії та розраховується на поширення через емоційне залучення користувачів. Конструювання охоплює добір зрозумілих образів, повторюваних смислових формул і правдоподібних елементів, які полегшують включення маніпулятивного повідомлення в наявні уявлення цільової групи. Класичним взірцем такого «інформаційного вірусу» став сфабрикований у липні 2014 року сюжет про «розіп'ятого хлопчика» у Слов'янську [140]. Попри абсолютну вигаданість, цей наратив ідеально відповідав вимогам когнітивної атаки: він апелював до найсильніших емоцій (гніву та жаху), блокував раціональну перевірку фактів і миттєво поширився соціальними мережами, створюючи у реципієнтів стійкий образ ворога, що було необхідно для виправдання подальшої ескалації бойових дій.

Третій етап життєвого циклу – поширення наративу через визначені канали й платформи, у якому ключову роль відіграє мультиканальна архітектура поширення контенту. Суб'єкт-агресор використовує синхронізовану мережу каналів: офіційні державні медіа, анонімні телеграм-канали, групи в месенджерах і ботоферми. Наталія Семенюк, начальниця науково-дослідного відділу Центрального науково-дослідного інституту Збройних сил України, пов'язує когнітивну війну з взаємодією віртуального й фізичного вимірів гібридного протиборства [141]. У межах авторської моделі цей етап забезпечує одночасну присутність наративу в різних каналах і його пристосування до окремих сегментів аудиторії.

Важливою характеристикою цієї фази є алгоритмічний мікротаргетинг, завдяки якому окремі сегменти аудиторії отримують повідомлення, узгоджені з

їхньою попередньою поведінкою та уподобаннями. Така персоналізація звужує спектр доступних пояснень і підсилює повторення однорідних тез. Аналіз рекомендацій YouTube, проведений Texty.org.ua, засвідчив тісний зв’язок між мовою попередніх переглядів і мовою контенту, який система пропонує користувачеві [127]. У межах СІО алгоритмічне звуження інформаційного середовища підтримує повторюваність потрібного наративу та формує враження його поширеності. Кожна соціальна група отримує той фрагмент повідомлення, який найбільше відповідає її внутрішнім упередженням і страхам.

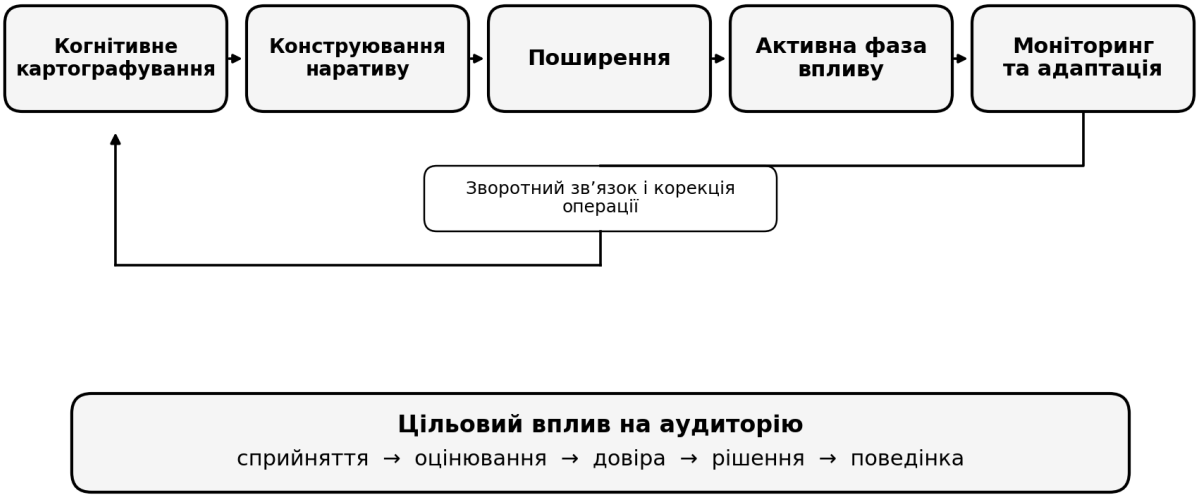


Рис. 1.1. Авторська модель життєвого циклу спеціальної інформаційної операції

Джерело: розроблено автором.

Узагальнимо авторську модель життєвого циклу СІО у схемі та аналітичній таблиці.

Таблиця 1.1. Авторська аналітична модель життєвого циклу СІО

Етап життєвого циклу	**Основна мета (когнітивне завдання)**	**Інструментарій та методи реалізації**	**Аналітичні ознаки та очікувані ефекти**
1. Когнітивне картографування	Визначення вразливостей аудиторії та зв'язку між релевантними темами, тригерами, способами інтерпретації й можливою реакцією.	Аналіз відкритих даних, суспільних суперечностей, ціннісних орієнтирів, моделей довіри та комунікаційної поведінки; сегментація аудиторії.	Визначений зв'язок «вразливість – тема або тригер – інтерпретація – можлива реакція», що задає параметри конструювання наративу.
2. Конструювання наративу	Створення наративу, узгодженого з уразливостями й очікуваннями аудиторії.	Аналіз наративів, сторітелінг, дезінформація, візуальна маніпуляція.	Смислова відповідність вразливостям аудиторії та потенціал поширення.
3. Поширення	Поширення наративу через визначені канали й платформи з охопленням цільових груп.	Мультиканальне поширення, анонімні ресурси, ботоферми, мікротаргетинг.	Охоплення цільових груп і повторюваність повідомлень у різних каналах.
4. Активна фаза впливу	Трансформація інтерпретацій, установок і поведінкових реакцій.	Рефлексивне управління, емоційне підсилення, повторення повідомлень.	Зміни в інтерпретаціях, установках і поведінкових реакціях.
5. Моніторинг та адаптація	Оцінювання реакцій аудиторії та коригування змісту й каналів поширення.	Аналіз охоплення, тональності реакцій і змін поведінки аудиторії.	Динаміка охоплення, реакцій аудиторії та коригування наративу.

Примітка. Наведені інструменти й аналітичні ознаки мають варіативний характер і застосовуються відповідно до цілей, середовища та конфігурації конкретної спеціальної інформаційної операції.

Четвертий і п’ятий етапи авторської моделі – активна фаза впливу та моніторинг із подальшою адаптацією – забезпечують підтримання й коригування операції. На етапі моніторингу ініціатор оцінює охоплення, тональність суспільних реакцій та зміни в поведінці цільових груп. Валентина Панченко, кандидатка технічних наук і старша наукова співробітниця, розглядає зворотний зв’язок як складник оцінювання результативності інформаційних операцій у системі стратегічних комунікацій [142]. Отримані дані використовуються для коригування змісту, каналів і темпу поширення повідомлень. Цифрові платформи додатково підсилюють резонансний контент відповідно до власних алгоритмів ранжування. У межах авторської моделі результативність СІО оцінюється за змінами суспільних установок, довіри та поведінкових реакцій. Еволюція російської дезінформації навколо збиття рейсу MH17 ілюструє послідовне висування взаємовиключних версій. Після версії про український винищувач поширювалися твердження про український комплекс «Бук» і повідомлення нібито іспанського авіадиспетчера. У доповіді Парламентської асамблеї Ради Європи ці версії охарактеризовано як суперечливі та підкріплені маніпульованими радарними й супутниковими даними [143, с. 11]. Така зміна пояснень підтримувала стан невизначеності й відволікала увагу від установлених міжнародним розслідуванням обставин.

Кінцеві цілі життєвого циклу СІО полягають у послабленні довіри до інституцій, погіршенні якості рішень і зниженні готовності суспільства до консолідованого спротиву. Такий ефект формується через послідовне використання вразливостей аудиторії, повторення наративів та адаптацію каналів їх поширення. Цифрові технології масштабують окремі етапи цього процесу та пришвидшують оброблення даних про реакції аудиторії.

Отже, життєвий цикл спеціальної інформаційної операції у даному дослідженні представлено як авторську аналітичну модель, що поєднує когнітивне картографування, конструювання наративу, поширення, активний вплив та моніторинг із подальшою адаптацією. Розуміння цієї послідовності створює основу для системної протидії, оскільки дозволяє ідентифікувати ознаки

підготовки інформаційного впливу на ранніх етапах. СІО розглядається як один із провідних інструментів сучасної гібридної війни, спрямований на зміну сприйняття, установок і поведінки цільової аудиторії. Такий підхід вимагає від держави технічного захисту інформаційного простору та стратегій підвищення когнітивної стійкості громадян як складника національної безпеки.

Висновки до розділу 1

Узагальнення результатів теоретико-методологічного аналізу інформаційного складника сучасних воєн дозволяє сформулювати низку концептуальних положень, що становлять підґрунтя для дослідження механізмів впливу на суспільну свідомість.

1. Аналіз генезису та сучасного стану наукового дискурсу засвідчив трансформацію ролі інформації в структурі збройних конфліктів – від допоміжного забезпечення воєнних дій до самостійного стратегічного виміру протиборства. Опрацювання зарубіжних та українських досліджень дало змогу сформувати аналітичну логіку, у межах якої інформаційна складова сучасних воєн охоплює боротьбу за способи інтерпретації подій, довіру, політичні оцінки та поведінкові орієнтації аудиторій. Український дослідницький дискурс, сформований значною мірою під впливом досвіду російської агресії, конкретизує зв’язок інформаційного впливу з політичною суб’єктністю, національною ідентичністю та стійкістю державних і суспільних інституцій. Це дозволяє розглядати інформаційну складову сучасної війни як багаторівневий політичний процес, у якому смисловий і когнітивний вплив пов’язаний із досягненням стратегічних цілей конфлікту.
2. Систематизація категорійно-понятійного апарату дозволила уточнити ключові дефініції дослідження. Встановлено, що «інформаційна складова сучасної війни» є багатофакторною системою, яка поєднує технологічні канали зв’язку та складні когнітивно-психологічні стратегії. Через усунення певної розмитості понять «інформаційна війна» та

«інформаційно-психологічна операція» обґрунтовано необхідність їх розмежування за масштабом і часовими межами, де інформаційну війну визначено як тривалий стратегічний рівень інформаційного протиборства, а операції – як інструментальні акти реалізації конкретних політичних цілей. У цьому контексті концептуалізовано поняття когнітивної війни, що пояснює перехід від маніпулювання окремими повідомленнями до деструктивного впливу на процеси мислення, інтерпретації, суспільної довіри й ухвалення рішень з метою дестабілізації державних інститутів.

3. Методологічний інструментарій дослідження ґрунтується на принципі міждисциплінарності, що дозволяє комплексно охопити об’єкт вивчення. Застосування системного підходу сприяло обґрунтуванню інформаційного простору як цілісного середовища, де державні структури, медійні платформи та індивідуальна свідомість перебувають у стані постійної взаємодії. Через інтеграцію дискурс-аналізу виявлено й експліковано приховані маніпулятивні конструкції в стратегічних наративах. Залучення когнітивного підходу надало змогу з’ясувати теоретичні механізми, через які зовнішні інформаційні потоки можуть сприяти формуванню стійких внутрішніх переконань, пов’язаних із моделями політичної поведінки. На основі цього аргументовано, що сучасна методологія має обов’язково враховувати фактор цифровізації, оскільки алгоритми соціальних медіа перестають бути суто нейтральними каналами й через механізми ранжування активно структурують видимість контенту та суспільний порядок денний.
4. На основі аналізу спеціальних інформаційних операцій запропоновано п’ятиетапну аналітичну модель їхнього життєвого циклу: когнітивне картографування цільової аудиторії, конструювання наративу, поширення, активну фазу впливу та моніторинг із подальшою адаптацією. Когнітивне картографування виокремлено як самостійний вхідний етап, на якому встановлюється зв’язок між конкретними вразливостями аудиторії, значущими для неї темами й тригерами, способом інтерпретації

повідомлення та можливою реакцією. Результати цього етапу задають параметри конструювання наративу, його поширення через визначені канали й платформи та подальшого коригування операції. Модель має аналітичний, а не жорстко лінійний характер: у конкретних СІО окремі етапи можуть накладатися, повторюватися або реалізовуватися паралельно. Її застосування дозволяє розмежовувати операційну спроможність СІО, цільовий когнітивний вплив та емпірично підтверджені політичні й поведінкові наслідки.

5. Результати аналізу підтверджують, що інформаційна складова виконує функцію посилення впливу в сучасних конфліктах, дозволяючи агресору маскувати наміри та створювати ілюзію легітимності своїх дій. Аргументовано, що безпека інформаційного простору остаточно перейшла з розряду технічних питань до сфери стратегічних пріоритетів національної безпеки. На цій основі розвинено наукові уявлення про роль стратегічних комунікацій, які трактовано як інструмент випереджального формування зрозумілих для суспільства пояснювальних наративів, координації державного повідомлення та підтримання тривалої довіри до інституцій. Теоретичне осмислення цих процесів дозволило довести, що захист власного смислового поля та стійкість суспільної свідомості до зовнішніх впливів є безпосередньо похідними від спроможності стратегічних комунікацій знижувати базову вразливість громадян до маніпуляцій та підтримувати міцність соціальних зв’язків.
6. Визначено, що інформаційні механізми впливу мають тривалий ефект, який проявляється у поступовій трансформації ціннісних орієнтацій суспільства. Аргументовано, що інформаційне протиборство не обмежується періодом активних бойових дій, а триває постійно, охоплюючи всі сфери суспільного життя. Здійснено політологічну типологізацію вразливостей свідомості, у результаті якої з’ясовано, що найдеструктивніше операції впливають на ті сегменти, де відсутні чіткі світоглядні орієнтири або фіксується високий рівень соціальної

фрустрації. З огляду на це, формування стратегічної стійкості інформаційного простору обґрунтовано як процес, що потребує глибокого врахування психологічних та політологічних аспектів сприйняття інформації під час формування стратегій національної безпеки й консолідованої відповіді суспільства на зовнішню агресію.

Підсумовуючи, можна стверджувати, що сформована теоретико-методологічна база дозволяє перейти до детального вивчення конкретних інструментів впливу в умовах поширення новітніх комунікативних технологій. Викладені аргументи доводять, що інформаційний складник є одним із визначальних чинників сучасної війни, який потребує постійного наукового переосмислення та оперативного реагування на нові виклики.

РОЗДІЛ 2. МЕХАНІЗМИ ВЕДЕННЯ ІНФОРМАЦІЙНОЇ ВІЙНИ В УМОВАХ ПОШИРЕННЯ НОВІТНІХ КОМУНІКАТИВНИХ ТЕХНОЛОГІЙ

2.1. Інструменти виявлення та подолання деструктивних впливів та наративів інформаційних операцій: типологія, основні характеристики

З огляду на стрімку еволюцію методів і технологій когнітивного впливу особливої актуальності набуває розроблення й застосування ефективних інструментів виявлення та нейтралізації деструктивного контенту. Сучасний інструментарій протидії дезінформації формується на перетині технологічних інновацій, медіаосвіти, критичного аналізу та міждисциплінарних методик. Його розвиток визначається одночасним ускладненням цифрового середовища, зростанням швидкості поширення повідомлень і переходом інформаційних операцій до мультимодальних форматів, у яких текст взаємодіє із зображенням, відео, аудіо та мережевою поведінкою користувачів. За цих умов окремий інструмент охоплює лише визначену ділянку інформаційного процесу, тому наукова систематизація має враховувати технологічні, функціональні й організаційні відмінності між засобами протидії. У даному дослідженні систематизуємо ці інструменти за ступенем автоматизації, технологічною основою, сферою застосування та функціональною спрямованістю. Така систематизація охоплює ручні, автоматизовані й гібридні рішення; технології обробки природної мови, штучного інтелекту, розвідки з відкритих джерел і фактчекінгу; засоби аналізу текстового, візуального та мережевого контенту; інструменти детекції, профілактики, реактивної відповіді й проактивного формування контрнаративів. Технології обробки природної мови та глибокого навчання дають змогу розпізнавати пропагандистські прийоми, об’єкти впливу й приховані смислові конструкції у текстовому контенті [144]. Їхня аналітична цінність полягає у здатності швидко опрацьовувати великі корпуси повідомлень, виявляти повторювані риторичні схеми та формувати масиви для подальшої експертної перевірки. Окремий напрям становлять системи мережевого

моніторингу, що картографують поширення повідомлень, виявляють скоординовану активність і поєднують аналіз відкритих даних з автоматизованим опрацюванням великих масивів контенту. У такому підході предметом аналізу стає сукупність зв'язків між обліковими записами, часовими інтервалами публікацій, повторюваними формулами та каналами перенесення меседжу між платформами. Превентивні методики інокуляції (prebunking) формують стійкість аудиторії через попереднє пояснення маніпулятивних технік, а медіаосвітні програми закріплюють навички критичного оцінювання інформації. Результативність інокуляційних втручань підтверджують експериментальні дослідження, розглянуті далі у підрозділі. Таким чином, вихідною передумовою типології є функціональна взаємодоповнюваність технологічних і освітніх засобів, які працюють на різних етапах появи, поширення та сприйняття деструктивного повідомлення.

Важливу складову протидії деструктивним впливам становлять фактчекінгові платформи та цифрові системи верифікації, серед яких Snopes, StopFake, VoxCheck, фактчекінгові підрозділи міжнародних медіа, дослідницька група Bellingcat, Google Fact Check Explorer та спеціалізовані засоби перевірки зображень і відео. Поєднання ручної експертизи з автоматизованим пошуком, аналізом метаданих і зіставленням відкритих джерел прискорює спростування інформаційних атак та підтримує довіру до перевірених повідомлень. Цифрова верифікація охоплює перевірку походження матеріалу, часу його створення або завантаження, географічної прив'язки, попередніх публікацій і відповідності візуального ряду заявленому контексту. Фактчекінг доповнює цю процедуру змістовним аналізом твердження, встановленням першоджерела та поясненням способу маніпуляції. Важливим напрямом протидії є формування контрнаративів, спрямованих на деконструкцію деструктивних меседжів і послідовне представлення власної інтерпретації подій. Тодд Гелмус і Христина Голинська, дослідники RAND – неприбуткової аналітичної організації у США, – показують, що українська відповідь на російську дезінформацію поєднувала спростування, пребанкінг, медіаграмотність і просування проукраїнських

наративів [145]. Контрнаратив у цій логіці виконує конструктивну функцію: він повертає повідомлення до перевіреного контексту, пояснює політичне значення події та пропонує аудиторії цілісну смислову альтернативу деструктивній інтерпретації. У даному дослідженні виокремлюємо чотири функціональні групи інструментів: автоматизоване виявлення й аналіз контенту; мережевий моніторинг і виявлення бот-активності; превентивну інокуляцію та медіаосвіту; фактчекінг і цифрову верифікацію. Великі мовні моделі та технології побудови ланцюжків міркувань розглядаємо як підходи всередині першої групи. Така типологія дає змогу зіставляти інструменти за їхньою функцією, способом застосування та місцем у загальній системі інформаційної стійкості. Вона також відокремлює засоби первинної автоматизованої селекції від процедур поглибленої перевірки та довгострокової підготовки аудиторії [146].

Першу групу становлять засоби автоматизованого виявлення й аналізу пропагандистського та дезінформаційного контенту. Їх застосування дає змогу працювати з інформаційними потоками, обсяг яких перевищує можливості ручного моніторингу, і швидше виділяти повідомлення, що потребують поглибленої перевірки. Об’єктом аналізу стають повторювані способи побудови повідомлень: емоційне нагнітання, категоричні узагальнення, підміна причинності, дискредитаційні означення, вибіркове використання фактів, сталі наративні конструкції. Накопичення таких ознак у різних каналах дозволяє виявляти формування інформаційної кампанії ще до того, як її основні тези закріпляться в масовому сприйнятті.

У 2019 році Альберто Баррон-Седеньйо, Джованні Да Сан Мартіно та Преслав Наков, дослідники Катарського інституту обчислювальних досліджень Університету Хамада бін Халіфи, а також Ісраа Джарадат з Техаського університету в Арлінгтоні, представили систему Proppy, яка моніторить новинні джерела, усуває дублікати, групує матеріали за подіями та ранжує їх за ймовірністю пропагандистського змісту [147]. Поєднання цих функцій дає аналітикові можливість бачити не окремий сумнівний матеріал, а ширшу конфігурацію інформаційного потоку: концентрацію повідомлень навколо

певної теми, синхронне повторення однакових інтерпретацій, різке збільшення кількості однотипного контенту. Дедуплікація зменшує інформаційний шум, подієва кластеризація показує щільність повідомлень навколо спільного сюжету, а ранжування допомагає визначати пріоритетність подальшої перевірки. Такий підхід особливо важливий у ситуаціях, коли інформаційний вплив здійснюється одночасно через різні медіа й платформи та створює видимість незалежного підтвердження однієї й тієї самої тези.

Автоматизований скринінг у цьому випадку виконує функцію раннього попередження. Він дозволяє відстежувати зміни в інформаційному середовищі й швидко визначати теми, навколо яких формується координоване або маніпулятивне просування. Однак машинне ранжування саме по собі не встановлює достовірність повідомлення і не пояснює його місце в ширшому контексті. Остаточна оцінка потребує зіставлення джерел, змісту, способу поширення та реакцій аудиторії. Автоматизована система в такій конфігурації допомагає визначити, куди спрямувати увагу аналітика, але не підмінює його висновок.

Одним із технологічних рішень для текстової класифікації є RoBERTa – трансформерна модель, яку додатково налаштовують на спеціалізованих масивах новинного контенту [148]. Її результативність значною мірою залежить від матеріалу, на якому проводилося навчання. Совітін Кунтур, дослідник факультету математики та інформаційних наук Варшавської політехніки, та співавтори у порівняльному дослідженні виявлення фейкових новин отримали для RoBERTa точність 86,16 % на FakeNewsNet і 99,99 % на ISOT [149]. Така різниця показує, наскільки обережно слід переносити показники, отримані на контрольованих наборах даних, на відкрите інформаційне середовище, де постійно змінюються теми, актори, мовні форми й способи маскування маніпуляції. Кіпріан-Октавіан Труїка та Елена-Сімона Апостол, дослідники комп’ютерних наук Політехнічного університету Бухареста, при цьому К.-О. Труїка також представляв Уппсальський університет у Швеції, пов’язують результативність трансформерних класифікаторів із контекстом, обсягом набору

даних і способом його підготовки [150].

Для практичного використання це означає, що алгоритмічний висновок завжди залежить від моделі даних, на якій він побудований. Особливої обережності потребують конфліктні інформаційні сюжети, іронія, нові події та повідомлення, у яких достовірні факти поєднуються з маніпулятивним висновком. Помилкове маркування такого контенту здатне впливати на його видимість, поширення та ставлення аудиторії до самої процедури перевірки. Тому автоматизовані фільтри доцільно поєднувати з регулярним оновленням навчальних матеріалів, зрозумілими критеріями оцінювання та експертним контролем. Прозорість тут безпосередньо пов’язана з довірою: користувач і аналітик повинні розуміти, наскільки впевнено система робить висновок і де проходять межі його застосування.

Окрему можливість для такої роботи створюють великі мовні моделі (Large Language Models, LLM), здатні оцінювати нові типи повідомлень без спеціального донавчання на кожній новій темі [151]. Для моніторингу інформаційного середовища це важливо через його постійну мінливість: можна уточнювати акторів, події, часові межі й критерії перевірки природною мовою. Водночас якість результату залежить від поставленого завдання, повноти контексту та здатності системи пояснити власний висновок.

Людмила Заволокіна та співавтори з Університету Цюриха – державного дослідницького університету Швейцарії – дослідили ClarifAI – інструмент, що поєднує аналіз новин за допомогою GPT-4 із візуальними маркерами та контекстними поясненнями [152]. Експеримент показав вищий рівень заявленого усвідомлення пропагандистських технік у версіях, де автоматична оцінка супроводжувалася маркерами й поясненнями: 82 % та 96 % відповідно [152]. Середній час роботи з матеріалом у повній версії збільшився приблизно на 49 секунд [152]. Отже, цифровий інструмент може змінювати сам спосіб взаємодії користувача з повідомленням, спонукаючи його довше затримувати увагу на аргументах і контексті.

У двопроцесній моделі Деніела Канемана повільніше аналітичне

опрацювання пов’язується з роботою Системи 2 [97]. Візуальна позначка або пояснення створюють додаткову паузу між отриманням емоційно насиченого повідомлення та його оцінюванням. Це зменшує роль автоматичної реакції й повертає користувача до перевірки фактів та аргументації. У цьому сенсі можливості LLM виходять за межі простого прискорення фактчекінгу: вони можуть підтримувати саму процедуру осмисленої перевірки, якщо остаточне рішення залишається за людиною.

Пояснюваність алгоритмічного висновку має значення і для довіри до верифікаційних інструментів. Система, покликана допомагати у виявленні маніпуляції, втрачає переконливість, якщо користувач отримує лише готову оцінку без можливості зрозуміти, як вона сформована. Для суспільно значущих повідомлень особливо важливо зберігати можливість відтворити логіку перевірки, відділити встановлений факт від машинної інтерпретації та визначити межі впевненості системи. Це утримує автоматизований аналіз у ролі інструмента підтримки рішення, а не автономного арбітра достовірності.

Для складних повідомлень, у яких достовірні факти поєднуються з хибним висновком або зміненим контекстом, важливою стає послідовність перевірки. Джейсон Вей та співавтори, дослідники Google Research, Brain Team, показали, що prompting із ланцюжком міркувань (Chain-of-Thought, CoT) покращує результати моделей у завданнях, які потребують послідовного логічного виведення [153]. У межах нашого аналізу цей принцип використовується для впорядкування самої процедури: спочатку виокремлюються заявлені факти, потім перевіряються їхні часові й просторові координати, після цього – причинні зв’язки й загальний висновок повідомлення. Така послідовність особливо ефективна там, де маніпуляція виникає не через вигадування факту, а через зміну зв’язку між кількома достовірними елементами.

Одним із різновидів такого впливу є часова деконтекстуалізація – перенесення події в інший часовий контекст, зміна послідовності епізодів або поєднання фактів із різних періодів. Для позначення цього прийому в роботі використовуємо авторську категорію «хронополітичне хакерство». Йдеться про

маніпулятивну зміну часових координат події, за якої окремі факти можуть залишатися достовірними, але їх поєднання створює інший причинно-наслідковий сенс. У такій ситуації перевірка має відновити реальну послідовність подій і виявити момент, у якому факт переходить у нав'язану інтерпретацію.

Послідовна декомпозиція корисна й для аналізу наративів загалом. Маніпулятивне повідомлення часто набуває переконливості саме тому, що правдиві елементи вбудовуються у схему, яка задає потрібне пояснення відповідальності, мотивів або наслідків. Розмежування фактологічного та інтерпретаційного рівнів дозволяє точніше визначити, де формується спрямований висновок. Для аудиторії така процедура має ще одну перевагу: вона показує не тільки підсумковий вердикт, а й шлях, яким його отримано. Саме тому автоматизований аналіз доцільно використовувати як інструмент підтримки експертного рішення, що підвищує швидкість перевірки й водночас зберігає можливість перевірити аргументацію.

Другу функціональну групу становлять системи моніторингу мережевого поширення та бот-активності. Вони аналізують скоординовану поведінку облікових записів, інтенсивність поширення повідомлень, структуру взаємодій і повторюваність цифрових сигналів. На відміну від текстового класифікатора, мережевий інструмент оцінює спосіб циркуляції контенту: синхронність публікацій, однакові посилання, шаблонні формулювання, аномальну частоту реакцій і взаємозв'язки між групами акаунтів. У політичному середовищі ці ознаки допомагають відрізнити органічне поширення повідомлення від штучно посиленої видимості та встановити вузли, через які наратив переходить між спільнотами. У 2019 році Обсерваторія соціальних медіа Університету Індіани – університетський дослідницький центр у Блумінгтоні, США, що вивчає інформаційні процеси в соціальних мережах, – представила безкоштовний відкритий інструмент BotSlayer для виявлення скоординованих кампаній у реальному часі [154]. Його практична цінність пов'язана з доступністю для дослідницьких груп, журналістів і громадських організацій, які отримують засіб

раннього виявлення різкого зростання активності навколо визначених тем. У серпні 2024 року Цзібін Ґун та співавтори, дослідники мультимодальної бот-детекції, представили BotSAI – модель виявлення ботів у Twitter/X, що інтегрує текстові характеристики, метадані користувачів і топологію гетерогенної мережі [155]. Її архітектура поєднує мережевий енкодер, механізм самоуваги та розподіл користувацьких ознак між інваріантним і специфічним підпросторами. Інваріантне представлення фіксує стійкі ознаки бот-поведінки, а специфічне – особливості конкретного типу акаунтів або набору даних. Така комбінація розширює аналіз від окремого профілю до його місця в мережі взаємодій. Хао Пен та співавтори, дослідники структурного аналізу соціальних мереж, запропонували UnDBot – пояснюваний метод навчання без учителя, побудований на теорії структурної інформації [156]. Він використовує розподіл типів публікацій, вплив публікацій і співвідношення підписок та підписників для формування зваженого багатореляційного графа й кластеризації спільнот ботів [156]. Автономний характер такого аналізу означає, що модель формує групи за структурною подібністю поведінки, а інтерпретовані метрики пояснюють підстави кластеризації. Це особливо важливо для швидкозмінних мереж, у яких заздалегідь розмічені приклади швидко втрачають репрезентативність. Антуан Вастель, фахівець із бот-детекції компанії Castle, у галузевому технічному матеріалі систематизує сигнали виявлення за чотирма групами: цифрові відбитки пристрою, поведінкові характеристики, репутаційні дані та контекстні сигнали [157]. Це комерційне технічне джерело відображає практику розробника, тоді як BotSAI та UnDBot представлені як академічні моделі. Зіставлення цих підходів показує зближення дослідницької та прикладної логіки навколо багатофакторного аналізу, у якому слабкі сигнали набувають значення через їхню сукупність. У даному дослідженні поєднання мережевих, поведінкових і контекстних ознак визначаємо як основу своєчасного розпізнавання координованого штучного поширення повідомлень.

Третю функціональну групу утворюють інструменти превентивної інокуляції (prebunking) та освітньої протидії. Автоматизовані детектори й

системи моніторингу переважно працюють із уже створеним контентом і фіксують його ознаки, канали та масштаби поширення. Превентивна інокуляція діє до контакту аудиторії з конкретною дезінформацією, ознайомлюючи її з типовими прийомами маніпуляції та способами їх розпізнавання. Її предметом є механізм впливу: апеляція до страху, хибна дилема, дискредитація джерела, конспірологічне пояснення, використання фальшивого експерта або штучне протиставлення соціальних груп. Освітні, медійні й симуляційні інтервенції моделюють інформаційну атаку у спрощеній формі, створюють навичку виявлення її конструктивних елементів і готують аудиторію до самостійної оцінки наступних повідомлень. Симуляційний формат дає змогу побачити маніпуляцію з позиції її конструювання, а короткі пояснювальні відео й інтерактивні вправи закріплюють впізнавання окремих технік у різних темах. Медіаграмотність у цій системі виконує довгострокову функцію, оскільки закріплює процедури перевірки джерела, контексту, авторства та візуальних доказів. Вона також формує звичку відкладати емоційну реакцію до завершення перевірки й зіставляти повідомлення з альтернативними джерелами. Пребанкінг і медіаосвіта відрізняються часовим горизонтом: перший інструмент орієнтований на конкретні прийоми або очікувані інформаційні хвилі, другий підтримує загальну компетентність аудиторії. У даному дослідженні превентивний напрям розглядаємо як доповнення до технологічної детекції: він переносить частину захисної функції з алгоритму на підготовленого користувача й підвищує стійкість інформаційного середовища до повторюваних технік впливу.

Теорія психологічної інокуляції, започаткована соціальним психологом Вільямом Макгвайром, виходить із того, що попередження про майбутню спробу переконання та ознайомлення з ослабленими аргументами маніпулятора стимулюють завчасне формування контраргументів. Сандер ван дер Лінден, професор соціальної психології Кембриджського університету й дослідник психології дезінформації, розглядає інокуляцію як спосіб підвищення психологічної стійкості аудиторії до маніпулятивних повідомлень [158]. У

сучасних пребанкінгових втручаннях цей принцип реалізується через попередження про характер загрози, демонстрацію типових прийомів і тренування розпізнавання маніпуляції. Перший елемент створює усвідомлення вразливості до впливу, другий подає ослаблений приклад маніпулятивного аргументу, третій закріплює спосіб його спростування. Завдяки цьому користувач засвоює переносиму навичку, яку застосовує до нових повідомлень зі схожою структурою. Практичні формати охоплюють короткі відео, інтерактивні ігри, навчальні картки, пояснення перед переглядом контенту та вправи з розпізнавання риторичних прийомів. Роберт Макфедран та співавтори з Verian Group – комерційної агенції прикладних соціальних досліджень у Лондоні – опублікували результати британського онлайн-експерименту в рецензованому журналі Scientific Reports [159]. Така характеристика джерела відокремлює інституційний статус виконавця від наукового статусу публікації, що пройшла рецензування. У фінальній вибірці з 2430 учасників інокуляційне навчання зменшило частоту реакцій «подобається/люблю» на дезінформаційні пости на 50,5 %, а загальну частоту реакцій – на 42,0 % порівняно з контрольною групою [159]. У цьому експерименті інокуляція ефективніше за попереджувальні мітки зменшувала позитивні реакції на дезінформаційні публікації [159]. Наведені показники відображають поведінкову реакцію учасників у змодельованій стрічці соціальної мережі й демонструють практичний ефект попереднього навчання. Ян Розенбек, Сандер ван дер Лінден і Томас Нюгрен, дослідники психології дезінформації та медіаграмотності, у кроскультурному дослідженні показали, що пребанкінгові втручання знижують сприйнятливість до дезінформації у різних культурних середовищах [87]. Кроскультурна відтворюваність посилює значення інокуляції як підходу, орієнтованого на універсальні прийоми маніпуляції, а локалізація прикладів забезпечує відповідність конкретному комунікативному контексту. Сукупність цих результатів дає підстави визначити інокуляцію як емпірично перевірений превентивний компонент системи протидії інформаційним впливам.

Четверту функціональну групу становлять фактчекінгові платформи та

цифрові системи верифікації. Автоматизовані інструменти й системи моніторингу формують потужний аналітичний ресурс, а фактчекінгові платформи залучають користувача до самостійної перевірки змісту, джерела й контексту повідомлення. Індивідуальна обізнаність, розпізнавання маніпулятивних технік і усвідомлене споживання контенту залишаються складниками системної протидії дезінформації. Фактчекінг перетворює результат перевірки на публічно доступне пояснення, у якому простежується шлях від первинного твердження до джерел, доказів і підсумкової оцінки. Цифрові інструменти доповнюють цей шлях технічними операціями: пошуком попередніх публікацій, аналізом метаданих, геолокацією, хронолокацією та виявленням ознак редагування. Один із найстаріших порталів перевірки фактів Snopes працює з 1994 року й використовує розгалужену систему рейтингових категорій [160]. Вона дає змогу розрізняти повністю хибні твердження, частково точні повідомлення, безпідставні чутки та автентичні матеріали з хибним підписом [160]. Категорія «Здебільшого правда» застосовується до тверджень із достовірним основним змістом і неточними другорядними деталями. Категорія «Безпідставне» використовується для повідомлень, які походять із чуток або спекуляцій і не мають переконливої доказової основи. Позначення «Неправильно підписане» стосується справжніх фотографій або відео, які супроводжуються хибним описом походження, контексту чи значення. Така деталізація показує, що інформаційна маніпуляція часто виникає через зміну контексту або пропорцій між достовірними й хибними елементами. У даному дослідженні градацію оцінок розглядаємо як спосіб пояснити аудиторії різні форми недостовірності без зведення перевірки до бінарної опозиції «правда/фейк».

Міжнародна мережа перевірки фактів (International Fact-Checking Network, IFCN), створена Інститутом Пойнтера у 2015 році, встановлює для підписантів вимоги щодо неупередженості, прозорості джерел і фінансування, відкритості методології та політики виправлень [161]. Інститут Пойнтера є американською неприбутковою освітньою організацією у сфері журналістики, а IFCN виконує

функцію професійної мережі та механізму оцінювання відповідності організацій її Кодексу принципів. Ці вимоги надають аудиторії критерії для оцінювання самої фактчекінгової організації: хто її фінансує, якими джерелами вона користується, як виправляє помилки та як відокремлює перевірку фактів від політичної позиції. У такий спосіб інституційна довіра формується через публічно описану процедуру. OSINT як підхід до роботи з відкритими джерелами створює методологічну основу для перевірки цифрових матеріалів, їх геолокації, хронолокації та зіставлення [162]. Відкритими джерелами виступають супутникові знімки, відео й фотографії з соціальних мереж, картографічні сервіси, реєстри, архіви вебсторінок і публічно доступні бази даних. Їхня доказова цінність визначається походженням, взаємним підтвердженням і прозорістю процедури перевірки. Bellingcat – незалежна міжнародна група відкритих розслідувань – застосовує ці процедури для документування подій, встановлення місця й часу зйомки та перевірки походження цифрових матеріалів. У проєкті TimeMap група систематизувала відкриті свідчення потенційної шкоди цивільному населенню в Україні, поєднуючи геолокацію, хронолокацію та архівування матеріалів [163]. Картографічне представлення пов’язує окремий цифровий доказ із просторовою й часовою послідовністю подій, завдяки чому сукупність матеріалів набуває аналітичної цілісності. Цей приклад показує, що цифрова верифікація виконує інформаційну, доказову й меморіальну функції: вона допомагає перевіряти актуальні повідомлення та зберігати верифіковані цифрові сліди для подальших розслідувань.

В Україні з 2014 року успішно функціонує платформа StopFake, яка декларує стратегію MAD (моніторинг, архівування, розвінчання) і працює за принципами Кодексу Міжнародної мережі перевірки фактів. Ключовим напрямом роботи StopFake є перевірка повідомлень про війну Росії проти України та спростування дезінформації, поширюваної російськими медіа [164]. З 2023 року організація концентрує роботу на спростуваннях, пов’язаних із російсько-українською війною, підтримує мережу вебсайтів чотирнадцятьма

мовами й проводить тренінги з перевірки фактів та протидії пропаганді. Така модель поєднує оперативне реагування на окремі фейки з накопиченням архіву повторюваних наративів, який дає змогу простежувати зміну аргументації та повторне використання старих сюжетів. Український проєкт VoxCheck, підписант Кодексу принципів IFCN, щомісяця додає близько ста спростувань до власної бази, яка налічує понад шість тисяч матеріалів [165]. Кількісне наповнення бази показує сталість фактчекінгової роботи й створює корпус для тематичного аналізу дезінформаційних повідомлень. У даному дослідженні StopFake і VoxCheck розглядаємо як приклади інституціоналізації українського фактчекінгу в умовах тривалої російської інформаційної агресії. Кемерон Мартел і Девід Ренд, дослідники цифрової поведінки та психології дезінформації, в експериментах за участю понад 14 000 респондентів у США показали, що попереджувальні мітки фактчекерів зменшували віру в хибні новинні заголовки та готовність ними ділитися, зокрема серед учасників із низькою довірою до перевіряльників [166]. Огляд у міжнародному рецензованому науковому журналі Nature засвідчує, що фактчекінг загалом зменшує віру в неправдиві твердження, а сила й тривалість ефекту визначаються форматом виправлення, темою та характеристиками аудиторії [167]. Наведені результати демонструють, що фактчекінг впливає на оцінку конкретного повідомлення й водночас працює через довіру до процедури перевірки. У даному дослідженні відкриту методологію, доступний архів перевірок і прозорі правила виправлень визначаємо як основу довіри до фактчекінгових організацій. У листопаді 2024 року на форумі «Dialogue on Fakes 2.0» було представлено Global Fact-Checking Network, просування якої пов’язане з ТАСС та АНО «Диалог» [168]. Reporters Without Borders – міжнародна неурядова організація із захисту свободи преси, що базується в Парижі, – характеризує GFCN як кремлівський інструмент, який імітує незалежний фактчекінг і декларує мережу з 55 експертів у 37 країнах [169]. Поширення імітаційних проєктів перетворює впізнавану форму фактчекінгу на засіб легітимації пропагандистського повідомлення. Відповіддю стає регулярна перевірка відповідності стандартам IFCN та EFCSN,

публічне пояснення цих стандартів і демонстрація повного ланцюга джерел. На рівні агрегованого фактчекінгу Google Fact Check Explorer надає єдиний пошуковий інтерфейс до матеріалів, розмічених за схемою ClaimReview [170]. Fact Check Markup Tool використовується для створення структурованої розмітки фактчекінгових сторінок [171]. Структурована розмітка допомагає машинним системам ідентифікувати предмет перевірки, автора оцінки та підсумковий вердикт. За офіційною документацією Google, підтримка ClaimReview зберігається у Fact Check Explorer, а його відображення як окремого елемента в основній пошуковій видачі поступово припиняється [172]. За офіційним описом розробників, браузерне розширення InVID & WeVerify поєднує виділення ключових кадрів із відео, перегляд метаданих, зворотний пошук зображень і форензичні інструменти; у межах проєкту vera.ai до нього інтегровано бета-модулі виявлення синтетичних зображень і клонованого голосу [173]. Воно підтримує робочий процес, у якому користувач переходить від первинного сигналу до порівняння ключових кадрів, джерел і технічних ознак матеріалу.

У сегменті виявлення синтетичних медіа хмарні сервіси доцільно розглядати передусім як засоби первинного скринінгу. Deepware Scanner – бета-сервіс для аналізу відео на ознаки синтетичної маніпуляції обличчя, доступний через вебінтерфейс, API та SDK [174]. Технічна форма доступу тут другорядна порівняно з функцією самого інструмента: він дозволяє швидко виділити матеріал, який потребує поглибленої перевірки. У середовищі високої швидкості поширення контенту така попередня оцінка скорочує часовий розрив між появою потенційно маніпулятивного відео та реакцією редакції, аналітичного центру або державної установи. Водночас результат сканування не встановлює достовірність події й не пояснює походження матеріалу. Для цього необхідне зіставлення файлу з первинним джерелом, метаданими та обставинами поширення. Саме таке розмежування важливе для збереження довіри до верифікації: автоматизований сигнал має запускати перевірку, а не підмінювати її готовим вердиктом.

Подібну функцію виконує Hive – комерційна платформа автоматизованого аналізу цифрового контенту, що пропонує засоби виявлення синтетичних зображень, відео, аудіо й тексту [175]. Система повертає оцінку впевненості, яку можна використовувати для визначення черговості подальшої роботи з матеріалами [175]. Для інформаційного моніторингу це особливо важливо під час масового надходження однотипного контенту, коли ручна перевірка кожного об’єкта стає практично неможливою. Оцінка впевненості допомагає розподіляти увагу аналітиків і швидше виділяти матеріали з вищим ризиком синтетичного втручання. Однак числовий показник сам по собі не відповідає на питання, хто поширює повідомлення, на яку аудиторію воно спрямоване і яку інтерпретацію події намагається закріпити. Через це автоматизована детекція набуває практичної цінності лише як частина ширшої процедури, де технічний сигнал поєднується з аналізом джерела, способу поширення та змісту повідомлення.

Інший тип завдань вирішує TinEye – комерційний сервіс зворотного пошуку зображень. За офіційним описом, він дає змогу знаходити ранні публікації, джерело зображення та його модифіковані версії [176]. Для аналізу інформаційного впливу така функція важлива у випадках, коли маніпуляція створюється не шляхом генерування фальшивого зображення, а через повторне використання справжньої фотографії з іншим підписом, датою або поясненням. Сам візуальний об’єкт може залишатися автентичним, тоді як зміна контексту формує хибне уявлення про подію. Пошук ранніх версій дозволяє відновити початковий зв’язок між зображенням, місцем, часом і обставинами його появи. Така процедура особливо корисна для перевірки контенту, який уже набув широкого поширення й почав використовуватися як візуальне підтвердження певного наративу. Відновлення первинного контексту в такому разі послаблює можливість маніпулятивно привласнювати достовірний візуальний матеріал і використовувати його для підтвердження іншої події або іншого причинного пояснення.

Для відеоматеріалів подібне завдання виконує YouTube Data Viewer, створений Amnesty International – міжнародною правозахисною організацією –

для оперативної перевірки відео у правозахисній роботі [177]. Інструмент відображає час завантаження ролика та генерує ключові кадри, придатні для зворотного пошуку [177]. Поєднання часових даних і візуальних фрагментів допомагає встановити, чи публікувався матеріал раніше, у якому контексті він з'явився та чи відповідає заявлена дата реальній послідовності поширення. Для дослідження інформаційних операцій така реконструкція дозволяє простежити момент, коли первинний матеріал отримує нове пояснення і починає працювати на інший наратив. Важливо й те, що основні кроки перевірки можна повторити: користувач бачить не тільки висновок, а й дані, на яких він побудований. Відтворюваність процедури зміцнює аргументацію фактчекера та зменшує залежність аудиторії від авторитету самого верифікатора.

У межах дослідження Deepware Scanner, Hive, TinEye та YouTube Data Viewer доцільно розглядати як різні ланки єдиної процедури цифрової верифікації. Перші два інструменти допомагають виявити ознаки можливого синтетичного втручання, тоді як зворотний пошук і аналіз часових даних відновлюють походження та контекст матеріалу. Така послідовність дозволяє перейти від первинного сигналу до перевіреного пояснення того, що саме було змінено: сам цифровий об'єкт, обставини його появи чи спосіб його інтерпретації. Для протидії інформаційно-психологічному впливу це принципово, оскільки достовірний файл може бути використаний у маніпулятивній конструкції так само ефективно, як і синтетичний. Верифікація має встановлювати не лише автентичність зображення або відео, а й відповідність між матеріалом, подією та смислом, який йому надають під час поширення. За такого підходу цифрові інструменти підтримують експертне рішення, а прозора процедура перевірки стає одним із механізмів збереження суспільної довіри в умовах інформаційного протиборства.

На підставі проведеного аналізу визначаємо поєднання автоматизованої детекції, мережевого моніторингу, превентивної підготовки аудиторії, фактчекінгу та цифрової верифікації як стійку модель протидії дезінформації. Її результативність забезпечує послідовний «каскад» методів: алгоритми

здійснюють первинне виявлення й сортування контенту, мережевий аналіз встановлює координоване поширення, фактчекери та OSINT-дослідники перевіряють твердження й цифрові докази, а інокуляційні та освітні інструменти підвищують здатність аудиторії самостійно розпізнавати маніпуляцію. Кожний рівень виконує окрему функцію й передає результат наступному: сигнал алгоритму стає предметом експертної перевірки, верифікований висновок – основою публічного пояснення, а накопичені приклади – матеріалом для превентивного навчання. Прозорі процедури, пояснюваність алгоритмічних висновків і фахова експертиза пов'язують ці рівні в єдину систему. Визначаємо, що довготривала стійкість формується через регулярне оновлення технологій, відкритість методології та включення користувача у процес критичного оцінювання. Саме така комбінована архітектура дає змогу реагувати на окремі фейки, виявляти скоординовані кампанії та формувати суспільну стійкість до деструктивних інформаційних впливів.

2.2. Соціальні медіа як механізм інформаційно-психологічного впливу на суспільну свідомість і поведінку

Упродовж останнього десятиліття соціальні медіа перетворилися з інструментів міжособистісного спілкування на важливі канали поширення політичної й суспільно значущої інформації та середовище інформаційно-психологічного впливу. За даними Reuters Institute Digital News Report 2025, підготовленого Інститутом Ройтерз з вивчення журналістики при Оксфордському університеті, у 48 досліджених медіаринках 44 % респондентів віком 18–24 роки назвали соціальні та відеоплатформи головним джерелом новин [178]. Український медіапростір характеризується глибокою інтеграцією соціальних мереж у виробництво й поширення новин. За результатами моніторингу Інституту масової інформації, української громадської організації з дослідження медіасередовища, у 40 % матеріалів десяти популярних українських онлайн-медіа джерелом інформації були соціальні мережі, а 57 % таких матеріалів посилалися на Telegram [179]. За результатами дослідження компанії

InMind, проведеного 2024 року за підтримки USAID та Internews, 84 % опитаних використовували соціальні мережі як основне джерело новин, а 73 % отримували новини через Telegram [180]. Поєднання цих показників дає підстави визначити Telegram одним із провідних каналів, що впливають на формування новинного порядку денного української аудиторії та онлайн-медіа. Соціальні платформи поєднують виробництво новин, емоційну взаємодію та алгоритмічну організацію видимості повідомлень. Їхня архітектура орієнтує поширення контенту на показники взаємодії, а морально-емоційна лексика пов'язана з інтенсивнішою дифузією повідомлень [181]. Незалежний експеримент Центру передового досвіду НАТО зі стратегічних комунікацій, міжнародної військової організації в Ризі, показав, що через чотири тижні понад 93 % придбаних неавтентичних взаємодій залишалися доступними, що засвідчує обмежену швидкість їх виявлення та видалення платформами [182]. Масштабність і швидкість поширення дезінформації розкриває дослідження Соруша Восугхі, Деба Роя і Сінана Арала, дослідників Массачусетського технологічного інституту, які проаналізували 126 тис. ланцюжків поширення новин у Twitter. Хибні новини досягали аудиторії у 1 500 користувачів приблизно в шість разів швидше, ніж правдиві [183]. Автори пов'язують таку динаміку з новизною хибних повідомлень, а у відповідях на них частіше виявлялися здивування й відраза [183]. Руне Карлсен і Торіл Олберг, норвезькі дослідники політичної комунікації, встановили, що подання новини у Facebook-контексті знижувало оцінку її достовірності порівняно з публікацією на сайті новинного медіа [184]. Виходячи з наведених даних, визначаємо три взаємопов'язані чинники впливу соціальних медіа. Першим є алгоритмічна організація видимості контенту. Другий пов'язаний з інституційною залежністю частини онлайн-медіа від соціальних платформ. Третій охоплює когнітивну сприйнятливість аудиторії до емоційного й швидкоплинного контенту.

Теоретичні підходи до вивчення впливу соціальних медіа поєднують напрацювання класичних теорій масової комунікації з аналізом алгоритмічно організованої мережевої публічності. Максвелл Маккомбс і Дональд Шоу,

американські дослідники політичної комунікації, показали, що медійна пріоритизація тем пов’язана з тим, які питання аудиторія вважає суспільно важливими [185]. У цифровому середовищі механізм встановлення порядку денного доповнюється алгоритмічною персоналізацією, яка впорядковує видимість тем у стрічці користувача. У даному дослідженні це розглядаємо як технологічне продовження класичної логіки agenda-setting. Роберт Ентман, американський дослідник політичної комунікації, визначає фреймінг як відбір і акцентування окремих аспектів реальності, що підвищує їхню помітність у комунікативному тексті [186]. У соціальних медіа фрейми підкріплюються візуальними й емоційними елементами, зокрема мемами, короткими відео та повторюваними образами, які спрямовують інтерпретацію подій. Елізабет Ноель-Нойман, німецька дослідниця громадської думки, у теорії «спіралі мовчання» пов’язує готовність людини публічно висловлювати позицію зі сприйняттям домінантної думки та страхом соціальної ізоляції [187]. У даному дослідженні швидкість публічних реакцій і їхня кількісна видимість у соціальних медіа розглядаються як чинники, що здатні посилювати сприйняття домінантності певної позиції. Українські дослідження конкретизують дію цих механізмів у воєнному середовищі. Катерина Балабанова, кандидатка педагогічних наук і доцентка Київського столичного університету імені Бориса Грінченка, на матеріалі опитування 505 респондентів проаналізувала зміни медіаспоживання переважно серед молодої університетської аудиторії у 2022–2024 роках [188]. Результати показують значну роль соціальних мереж у новинному споживанні, мобілізації та координації цієї групи. Д. Павленко, науковий співробітник Національної бібліотеки України імені В. І. Вернадського, розглядає соціальні медіа як середовище поширення достовірної інформації та інформаційних атак у воєнних умовах [189]. Виходячи з цього, визначаємо координовану бот-активність і таргетовані кампанії окремими напрямами аналізу ІПСО. На цій підставі соціальні медіа визначаємо середовищем, у якому класичні механізми медійного впливу поєднуються з алгоритмічною селекцією та координацією мережевої активності.

Порівняння соціальних платформ у межах дослідження будуємо за трьома групами параметрів: масштабом і структурою аудиторії, форматом споживання контенту та особливостями його поширення. Такий підхід дозволяє співвідносити кількість користувачів зі способом входження повідомлення у повсякденне інформаційне середовище, тривалістю контакту та механізмами повторного поширення. Для зіставлення масштабів використовуємо показник потенційного рекламного охоплення, що характеризує аудиторію, доступну рекламним інструментам платформи, окремо від кількості унікальних або щомісячно активних користувачів [190]. Якісна частина порівняння охоплює роль рекомендаційних систем, ступінь публічності комунікації, можливість сегментації аудиторії та доступність зовнішнього моніторингу. Поєднання цих характеристик визначає, який тип наративу найпростіше закріплюється на конкретній платформі та яким шляхом переходить від первинної публікації до повторюваної присутності в інформаційному полі.

За даними рекламних інструментів Google, на початку 2025 року потенційне рекламне охоплення YouTube в Україні становило 21,6 млн користувачів, що відповідало 56,4 % населення та 68,5 % інтернет-аудиторії країни [190]. YouTube вирізняється поєднанням широкого охоплення, тривалого аудіовізуального контакту й рекомендаційної послідовності перегляду. Псевдодокументальні відео, ток-шоу, інтерв’ю та авторські канали дають змогу вибудовувати розгорнуте пояснення подій, повторювати ключові оцінки й поєднувати фактичний матеріал з емоційним коментарем. Окреме відео задає інтерпретацію, наступні матеріали її уточнюють або підсилюють, а рекомендаційна система підтримує серійність контакту. Завдяки цьому наратив набуває форми послідовної картини причин, відповідальності та наслідків. Специфічний профіль YouTube пов’язуємо саме з можливістю тривалого й повторюваного занурення аудиторії в одну систему пояснення подій.

Потенційне рекламне охоплення Facebook в Україні на початку 2025 року відповідало 36,3 % населення, 43,8 % повнолітніх і 44,1 % інтернет-аудиторії [190]. Платформа поєднує персональні сторінки, тематичні групи, коментарі та

рекламну сегментацію, що створює умови для адаптації одного наративу до різних локальних середовищ. Повідомлення отримує додаткову переконливість, коли з'являється поряд із повсякденним контентом і підтримується реакціями знайомих користувачів або членів групи. Видимість лайків, коментарів і репостів формує соціальний контекст сприйняття, у якому популярність позиції може сприйматися як непряме підтвердження її прийнятності. Повторення однакових тез у кількох спільнотах здатне створювати враження незалежного виникнення схожих оцінок. Відповідно, профіль Facebook визначаємо через сегментоване поширення, групове підтвердження та вбудовування суспільно значущих наративів у звичну комунікацію користувачів.

На початку 2025 року рекламні інструменти технологічної корпорації Meta оцінювали потенційне охоплення Instagram в Україні у 12,0 млн користувачів, що відповідало 31,3 % населення [190]. Instagram як платформа візуального й короткого відеоконтенту стискає складні сюжети до образу, підпису, короткого ролика, мему або інфографіки. Наратив у такому середовищі часто працює через впізнаваний символ та емоційну реакцію, поєднуючи суспільно значущий зміст з особистим і розважальним контентом. WhatsApp як сервіс приватних повідомлень формує інший тип контакту: групове й персональне пересилання переносить повідомлення у коло знайомих, родини або професійних контактів, де довіра до відправника може впливати на сприйняття змісту. Закритість таких ланцюжків водночас ускладнює зовнішній моніторинг їхнього походження та масштабу. Отже, Instagram і WhatsApp демонструють два різні механізми – публічне візуальне кодування наративу та приватну горизонтальну ретрансляцію через міжособистісну довіру.

Рекламні інструменти TikTok на початку 2025 року показували 17,0 млн користувачів віком від 18 років в Україні. Це відповідало 53,6 % повнолітнього населення та 53,9 % інтернет-аудиторії [190]. Коротке відео, емоційна насиченість і безперервна рекомендаційна стрічка створюють іншу логіку впливу, ніж тривалий перегляд або групова дискусія. Поняттям «мікродозований інформаційно-психологічний вплив» у роботі позначаємо послідовність

коротких матеріалів, кожен із яких містить окремий образ, символ, музичний мотив або оцінку, а їхнє повторення поступово складається у цілісний наратив. Окреме відео може зберігати зовнішню аполітичність, обмежуючись образом, інтонацією або короткою оцінкою. Повторюваний контакт із подібними образами та оцінками створює накопичувальний ефект, у якому теза засвоюється разом зі способом емоційного ставлення до події або суспільної групи. Рекомендаційна система TikTok підтримує серійність такого контакту, орієнтуючись на попередню поведінку користувача та реакції на відео. Саме повторюваність коротких контактів визначає окремий профіль ризику цієї платформи.

Telegram у 2025 році перевищив показник в один мільярд активних користувачів [191]. В Україні його роль є особливою через поєднання месенджера, новинних каналів і середовища швидкої ретрансляції: 73 % опитаних у дослідженні InMind та Internews повідомили про отримання новин через Telegram [180]. Масові канали, боти, коментарі та відкритий API дозволяють поширювати повідомлення на великі аудиторії й автоматизувати окремі елементи взаємодії. Архітектура сервісу розмежовує звичайні хмарні чати й канали та окремий режим наскрізно зашифрованих secret chats [192]. Для аналізу важливішим є комунікаційний наслідок: в одному середовищі співіснують офіційні повідомлення, журналістські матеріали, анонімні канали й автоматизовані засоби поширення. Швидкість пересилання сприяє багаторазовому відтворенню повідомлення ще до завершення перевірки. Дослідження Telegram також фіксують присутність фейкового контенту, шахрайських схем та екстремістських спільнот [193]. Поєднання новинної функції, мережевого підсилення та швидкої ретрансляції визначає Telegram як окремий тип інформаційного середовища.

Вікові відмінності додатково змінюють спосіб контакту з платформним контентом. Для аналітичного зіставлення умовно виокремлюємо три сегменти: 16–24 роки, 25–49 років і 50+. У молодшій групі помітнішу роль відіграють короткі відео та візуальні повідомлення TikTok, Instagram і Telegram; для

аудиторії 25–49 років характерне поєднання відео, блогерського контенту й дискусійних спільнот YouTube, Instagram і Facebook; у сегменті 50+ окремої уваги потребують Facebook, YouTube і WhatsApp, де значущими є групові зв’язки, довірче пересилання та повторювані історичні й соціальні сюжети. Це групування є авторською аналітичною схемою, призначеною для опису переважних форматів контакту різних вікових груп із платформним контентом. Емпіричне дослідження американської аудиторії Facebook виявило виразний віковий ефект у поширенні посилань із низькодостовірних джерел, особливо серед користувачів віком понад 65 років [194]. Наведений результат використовуємо як додаткову підставу для окремого аналізу старшої аудиторії; американський віковий поріг у цьому випадку виконує лише орієнтувальну функцію для українського середовища. Межа 50+ у роботі виконує аналітичну функцію і допомагає зіставляти передусім характер платформ, форматів і довірчих зв’язків.

Порівняння показує специфічний профіль ризику кожної платформи для інформаційно-психологічного впливу. Ризик визначається відповідністю архітектури сервісу меті кампанії, формату повідомлення та способу взаємодії з аудиторією. YouTube створює умови для тривалого наративного занурення й серійного пояснення подій; Facebook – для сегментації та групового підтвердження; Instagram концентрує зміст у візуальних і коротких емоційних формах; WhatsApp переносить його в закриті ланцюжки міжособистісної довіри; TikTok підтримує повторюваний контакт із короткими фрагментами; Telegram поєднує новинне споживання, масові канали та швидке пересилання. Така диференціація переводить аналіз від простого порівняння чисельності аудиторій до питання про те, як конкретне середовище змінює форму наративу, швидкість його поширення, видимість підтримки та можливість зовнішньої перевірки. Саме ці характеристики визначають вибір платформи для різних етапів інформаційної кампанії та відповідні способи протидії.

Спроможність соціальних платформ протидіяти скоординованому поширенню дезінформації доцільно оцінювати на двох рівнях. Перший охоплює

демонтаж великих мереж, ідентифікованих корпоративними командами безпеки; другий – виявлення дрібносерійної або комерційно придбаної активності, яка швидко змінює акаунти, формат і тематику. Корпоративні звіти Google, Meta і TikTok характеризують передусім перший рівень, тоді як незалежні експерименти Центру передового досвіду НАТО зі стратегічних комунікацій дозволяють перевірити реакцію на другий. У бюлетені за І квартал 2025 року Google Threat Analysis Group, корпоративний підрозділ Google з аналізу загроз, повідомила про припинення 11 697 каналів, пов'язаних із КНР, 1 562 каналів, пов'язаних з Азербайджаном, і 1 263 каналів, пов'язаних із російською консалтинговою компанією [195]. Упродовж ІІ кварталу Google TAG зафіксувала нові хвилі, пов'язані з російською консалтинговою компанією, – 1 045, 507 і 392 канали [196]. Три значні хвилі каналів, пов'язаних із КНР, включали 1 545, 3 592 і 2 598 каналів [196]. Масштаб видалень показує здатність платформи ідентифікувати великі мережі, а повторне виникнення хвиль – їхню спроможність відновлювати активність. Для оцінки стійкості важливий також час, протягом якого така мережа встигає накопичувати аудиторію й повторювати повідомлення.

Meta з 2017 року публікує звіти про скоординовану неавтентичну поведінку. У корпоративному звіті за І квартал 2025 року компанія описала три операції, пов'язані з Китаєм, Іраном і Румунією, та повідомила, що їх видалили до формування значного органічного охоплення [197]. Раннє втручання обмежує перехід від штучно організованої мережі до самопідтримуваного поширення серед реальних користувачів. Водночас корпоративний звіт охоплює ті операції, які сама компанія виявила, атрибутувала й оприлюднила. У роботі цей звіт використовуємо як джерело про задекларовані практики виявлення й демонтажу мереж, зберігаючи розмежування між корпоративною звітністю та незалежною оцінкою стійкості платформи. Кількість видалених акаунтів характеризує масштаб корпоративного втручання, тоді як швидкість реагування на менш помітні форми маніпуляції потребує окремої оцінки.

Цю різницю показав незалежний експеримент Центру передового досвіду

НАТО зі стратегічних комунікацій 2024 року. На Facebook упродовж п’яти днів після повідомлення було видалено 6 % залучених у тесті акаунтів, а через чотири тижні доступними залишалися понад 93 % придбаних неавтентичних взаємодій [198]. Результат вказує на інший рівень проблеми, ніж корпоративні звіти про великі мережі. Платформа може успішно ліквідовувати встановлену операцію з чіткими зв’язками між акаунтами й водночас пропускати значну частину дрібносерійної активності. Для запуску інформаційної кампанії навіть такі взаємодії здатні збільшувати видимість матеріалу, створювати первинні реакції та імітувати інтерес аудиторії. Модерацію, відповідно, оцінюємо і за здатністю демонтувати відомі мережі, і за швидкістю очищення штучно створеної активності.

Подібний розрив простежується на TikTok. З травня 2024 року платформа веде регулярний корпоративний реєстр прихованих операцій впливу (Covert Influence Operations). У червні 2025 року TikTok повідомив про видалення 1 198 облікових записів, пов’язаних із такими операціями [199]. У межах Кодексу практик протидії дезінформації ЄС платформа також звітує про застосовані заходи та виявлені мережі [200]. Незалежний експеримент Центру передового досвіду НАТО зі стратегічних комунікацій показав, що через чотири тижні доступними залишалися 99,85 % придбаних неавтентичних взаємодій у TikTok, а частка видалених упродовж п’яти днів тестових акаунтів була близькою до нуля [198]. У межах експерименту це характеризує низьку результативність реагування саме на маломасштабну придбану активність. Отже, регулярний демонтаж встановлених операцій співіснує з можливістю дешевих і швидко відновлюваних схем підсилення, здатних дати короткому відео початкову видимість.

Після виходу X з Кодексу практик протидії дезінформації ЄС і зміни формату звітності зовнішнє зіставлення платформи дедалі більше спирається на незалежні дослідження. Експеримент Центру передового досвіду НАТО зі стратегічних комунікацій зафіксував, що X видалив близько половини залучених у тесті акаунтів упродовж п’яти днів, а через чотири тижні доступними

залишалися 61,9 % придбаних неавтентичних взаємодій [198]. Серед протестованих платформ X продемонстрував найвищу швидкість первинного видалення акаунтів [198]. Водночас більша частина створеної ними взаємодії зберігалася і після блокування частини профілів [198]. Це розмежовує нейтралізацію акаунта та усунення вже сформованих сигналів видимості: збережені реакції можуть і далі впливати на сприйняття популярності матеріалу.

Telegram формує окремий випадок через високу роль у новинному споживанні та іншу модель модерації. У матеріалах платформи щодо виконання Акта про цифрові послуги ЄС описано поєднання автоматизованих і ручних процедур та принцип застосування найменш обмежувального достатнього заходу [201]. Документ визначає порядок розгляду повідомлень, категорії обмежень і механізми реагування на незаконний контент [201]. Для нашого аналізу ця процедура важлива у зв’язку зі швидкою ретрансляцією через публічні канали, ботів, коментарі та приватне пересилання. Одне повідомлення може переходити між різними режимами комунікації, ускладнюючи оцінку масштабу поширення й моменту, коли втручання ще здатне помітно обмежити його циркуляцію. Загальне зіставлення платформ показує, що демонтаж встановлених мереж є лише одним компонентом інформаційної стійкості. Поряд із цим важливими залишаються швидкість реакції на дрібносерійну активність, очищення вже створених штучних взаємодій, прозорість процедур і можливість незалежної перевірки. Рішення платформ у цій сфері впливають на те, які сигнали масовості й суспільної підтримки залишаються видимими для користувача.

На платформах із рекомендаційним ранжуванням сигнали взаємодії входять до набору чинників, що визначають видимість контенту. Їхнє штучне стимулювання через координоване коментування, репости, лайки або ботоферми здатне збільшувати початкове охоплення й створювати умови для подальшого поширення. Незалежні експерименти з придбаною неавтентичною активністю показують, що значна частина таких сигналів зберігається на платформах упродовж тривалого часу [198]. Це дозволяє визначити початкове штучне

підсилення одним із механізмів запуску самопідтримуваної уваги, коли матеріал отримує додаткові органічні реакції після створення видимості інтересу. Telegram має іншу архітектуру, але поєднує високе новинне охоплення в Україні з каналами, ботами й швидкою ретрансляцією повідомлень. Тому у даному дослідженні визначаємо його одним із центральних середовищ інформаційно-психологічного впливу.

Архітектура платформ, алгоритмічне ранжування, персоналізація та соціальна структура зв'язків спрямовують інформаційні потоки й визначають послідовність контакту користувача з повідомленнями. Особливого значення набувають когнітивні евристики, емоційні реакції та поведінкові патерни цільової аудиторії. Вільям Брейді та співавтори, дослідники моральної психології й мережевої комунікації, встановили, що кожне додаткове морально-емоційне слово було пов'язане приблизно з 20 % більшою дифузією повідомлення у досліджених політичних дискусіях Twitter [181]. Під морально-емоційною лексикою автори розуміють слова, що поєднують моральну оцінку з емоційною реакцією. У практичному вимірі повідомлення, які апелюють до гніву, обурення або відчуття несправедливості, отримують більше передумов для поширення через реакції користувачів. Аналітичний огляд Detector Media, української медійної громадської організації, виокремлює мобілізацію, економічну втому, недовіру до політичної еліти та міфи про «занепад Заходу» серед системно експлуатованих тем [202]. У даному дослідженні їх розглядаємо як емоційні вузли, спрямовані на послаблення довіри й суспільної згуртованості. Типова конструкція «проблема – загроза – винний» поєднує опис події з персоналізованою негативною оцінкою та переводить емоційне напруження у ставлення до конкретної особи, групи або інституції.

Другий важливий пласт становлять когнітивні евристики, які спрощують обробку інформації та водночас можуть спрямовувати інтерпретацію повідомлень. Шанто Айєнгар і Кю С. Ган, американські дослідники політичної комунікації, експериментально показали, що партійні бренди медіа спрямовують вибір респондентів до ідеологічно співзвучних новин [203]. Цей механізм описує

селективну експозицію, за якої користувачі надають перевагу джерелам, узгодженим з їхніми поглядами. Алгоритмічна персоналізація здатна закріплювати такий вибір, зменшуючи частоту контакту з альтернативними інтерпретаціями. Підтверджувальне упередження позначає схильність шукати, відбирати й тлумачити свідчення на користь уже прийнятих переконань [204]. Окремо діє евристика доступності. Амос Тверські та Деніел Канеман, дослідники психології ухвалення рішень, показали, що оцінка частоти й імовірності події залежить від легкості пригадування її прикладів [205]. У соціальних мережах повторювана видимість драматичних постів, відео й повідомлень може зміщувати уявлення про поширеність явища. Прикладний KI-Textscanner, представлений науково-популярною редакцією MDR WISSEN, використовує 27 категорій когнітивних упереджень, логічних помилок і риторичних технік маніпуляції [206]. До них належать cherry-picking, навіювальні запитання, whataboutism, ad hominem, псевдодилема та емоційний сенсаціоналізм. Cherry-picking полягає у вибірковому підкресленні підтримувальних фактів. Навіювальне запитання містить наперед задану гіпотезу. Whataboutism переводить увагу на зустрічне звинувачення. Ad hominem спрямовує оцінку на особистість опонента. Псевдодилема звужує спектр рішень до двох крайнощів. Сенсаціоналізм посилює емоційну реакцію через перебільшення. У стрічках Telegram і TikTok повторення таких прийомів здатне створювати хибне відчуття масовості окремих випадків і підживлювати помилкові узагальнення. Далі розглянемо їхнє застосування у практиці російської інформаційної агресії.

1. Сценарій «чорної зими» поєднує евристику доступності та cherry-picking. Detector Media у вересні 2024 року зафіксував кампанію про нібито нестерпну зиму з повсюдними відключеннями електроенергії [207]. Окремі фото й відео перебоїв подавалися як свідчення загального колапсу. У даному дослідженні вибіркове представлення таких випадків класифікуємо як cherry-picking, а повторювану видимість драматичних прикладів як використання евристики доступності. Поєднання двох прийомів перетворює локальний або ситуативний факт на образ тотальної

загрози й закріплює його через багаторазове відтворення у стрічці.

2. EUvsDisinfo, проєкт Європейської служби зовнішніх дій з моніторингу дезінформації, визначає whataboutism як системну тактику переведення уваги на зустрічні звинувачення, зокрема через згадки про Ірак або Югославію [208]. У практиці російських каналів цей прийом використовується у відповідь на повідомлення про злочини проти цивільного населення. Замість розгляду факту дискусія переноситься на інший конфлікт або дії іншої держави. У даному дослідженні whataboutism розглядаємо як спосіб підтримання вже наявних переконань аудиторії та відведення моральної оцінки від первинної події.
3. Навіювальне запитання містить вбудовану гіпотезу й спрямовує інтерпретацію ще до подання доказів. Прикладом такої конструкції є формула «Чи не приховує влада справжні втрати?». Її граматична форма перетворює припущення про приховування на вихідну рамку подальшого обговорення. Коротке запитання легко відтворюється у заголовках, коментарях і Telegram-дописах, а повторення створює ефект попереднього налаштування сприйняття. У даному дослідженні цей прийом визначаємо як сугестивний праймінг, за якого аудиторія шукає підтвердження вже введеної гіпотези й оцінює наступні повідомлення крізь задану рамку.
4. Окремим прийомом є використання підроблених авторитетних підтверджень. Журналіст WIRED Девід Гілберт задокументував поширення сфабрикованих цитат знаменитостей, зокрема Тейлор Свіфт, у кампаніях з антиукраїнськими повідомленнями [209]. Впізнавана публічна постать виконує функцію джерела довіри, хоча сама цитата створена маніпуляторами. У даному дослідженні цей прийом визначаємо як псевдоавторитетну зовнішню валідацію повідомлення. Він дозволяє переносити довіру до особи на політичне твердження й зміцнювати його відповідність попереднім переконанням прихильної аудиторії.
5. Масштабне штучне насичення інформаційного середовища демонструє мережа Telegram-ботів. The Times у журналістському розслідуванні

повідомляє про понад 3 600 прокремлівських ботів, які з січня 2024 до квітня 2025 року опублікували понад 316 тис. повідомлень [210]. Основними темами були локальні проблеми, зокрема відключення електроенергії, ціни та стан інфраструктури, які системно пов'язували з критикою України й закликами до прийняття окупації. Виходячи з масштабу та тематичної повторюваності, у даному дослідженні цю практику розглядаємо як штучне насичення середовища однорідними інтерпретаціями. Воно посилює селективну експозицію, створює враження поширеності певної позиції та підвищує доступність повторюваних наративів у пам'яті аудиторії.

6. Хибна дихотомія у наративі «мир за будь-яку ціну» звужує політичний вибір до двох крайнощів: негайного миру на умовах Росії або нескінченної війни. Така конструкція відсуває інші варіанти, серед яких переговори на основі Статуту ООН, українська формула миру та міжнародні гарантії безпеки. EUvsDisinfo у червні 2024 року зафіксував дискредитацію Саміту миру у Швейцарії через твердження про його безрезультатність і виняткову реалістичність російських пропозицій [211]. Кремлівські ресурси акцентували увагу на державах, які не підтримали підсумкове комюніке, відсуваючи на другий план сам факт участі 92 держав у саміті [211]. У даному дослідженні таке вибіркове структурування контексту класифікуємо як поєднання псевдодилеми та cherry-picking, спрямоване на формування відчуття безальтернативності нав'язаного рішення.

Важливим когнітивним ефектом є «ефект припущеної правдивості» (implied truth effect), описаний у серії експериментів дослідників Массачусетського технологічного інституту, Єльського університету та Університету Торонто. Вони встановили, що додавання попереджень лише до частини фейкових новин підвищувало сприйняту правдивість матеріалів, які залишалися без попереджень [212]. Непозначений матеріал у такій системі отримує непряму позитивну оцінку, оскільки користувач може тлумачити відсутність маркера як ознаку перевіреності. Для українського інформаційного середовища цей результат

означає, що вибіркове маркування доцільно поєднувати з чітким поясненням меж перевірки та додатковими інструментами оцінювання достовірності. Такий комплексний підхід зменшує ймовірність сприйняття статусу непозначених матеріалів як підтвердження їхньої правдивості.

Поляризаційна динаміка може виникати і під час контакту з протилежними політичними позиціями. Крістофер Бейл та співавтори, дослідники Дьюкського університету, провели у Twitter експеримент, під час якого користувачі підписувалися на ботів із протилежними політичними поглядами. Після контакту з ліберальним ботом республіканці демонстрували посилення консервативних позицій, тоді як серед демократів показники залишалися близькими до вихідних [213]. Отже, результат мав асиметричний характер. У даному дослідженні використовуємо його для формулювання гіпотези про ризик поляризаційної контрреакції, коли пряме подання опозиційного наративу активує захист групової ідентичності. У воєнному контексті такий механізм може враховуватися під час аналізу цілеспрямованого поширення критичних або умиротворювальних закликів у спільнотах із домінантною проукраїнською позицією.

На рівні очікуваної поведінки соціальні медіа підтримують масштабування закликів до дії (call-to-action, CTA) завдяки низьким витратам на координацію та кросплатформному поширенню. У цьому сенсі цифрове інформаційне протиборство набуває окремих ознак асиметричного конфлікту: відносно обмежені ресурси можуть забезпечувати значний ефект завдяки точному спрямуванню повідомлень, алгоритмічному підсиленню та мережевому поширенню контенту. Detector Media у листопаді 2022 року зафіксував провокаційний флешмоб у Twitter і Viber із закликом масово вмикати світло, який підхопили проросійські майданчики [214]. Така конструкція переводить інформаційний сигнал у просту поведінкову інструкцію та дозволяє демонструвати її виконання як ознаку масової підтримки. Соціальні мережі й месенджери використовуються також для вербування та координації протиправних дій. За даними слідства, оприлюдненими Службою безпеки

України у повідомленні про підозру, жінку дистанційно завербували російські спецслужби, після чого вона стежила за Сергієм Стерненком і здійснила збройний напад [215]. Журналістський матеріал Центру публічних розслідувань описує судовий вирок підлітку на Миколаївщині та інші схеми завдань, що передавалися через Telegram [216]. Окремий кейс, описаний виданням The Record, стосується 43-річної жінки, яку, за даними українських правоохоронців, завербували через TikTok для збирання інформації про військові об'єкти [217]. На інституційному рівні Служба безпеки України запустила офіційний чатбот «Спали ФСБшника» для оперативного повідомлення про спроби вербування до терактів, диверсій і підпалів [218]. Цей інструмент поєднує раннє виявлення вербувальної комунікації з профілактичним інформуванням молоді. Проведений аналіз дає підстави визначити соціальні медіа багаторівневим механізмом інформаційно-психологічного впливу, у якому платформна архітектура поєднується з емоційними тригерами, когнітивними евристиками та низьковитратною координацією поведінки. На цій основі пропонуємо орієнтувати профілактичні заходи на одночасне підвищення прозорості платформ, медіаграмотності й раннього виявлення вербувальних комунікацій.

2.3. Специфіка застосування механізмів кібербезпеки у воєнних умовах

В умовах російської збройної агресії кібербезпека є невід'ємною складовою національної безпеки України, оскільки підтримує стійке функціонування державних інформаційних ресурсів, критичної інфраструктури, систем управління та економічних процесів. Потенціал кіберзагроз зростає разом із ширшим застосуванням штучного інтелекту в захисних і атакувальних діях. Всесвітній економічний форум (World Economic Forum, WEF) – міжнародна організація публічно-приватного співробітництва – у *Global Cybersecurity Outlook 2025* розглядає ШІ як один із чинників, що суттєво змінюють середовище кіберризиків [219]. У звіті Atlantic Council, американського аналітичного центру з питань міжнародної безпеки, запропоновано оцінювати кіберінциденти за їхніми наслідками для громадян, організацій і суспільства. Такий підхід посилює

міжвідомчу координацію та орієнтує державну політику на вимірювані результати кіберзахисту [220]. У воєнних умовах ця логіка має особливе значення, оскільки оцінювання кібербезпеки охоплює швидкість відновлення сервісів, масштаби порушення управлінських процесів і суспільні наслідки інциденту. У прогнозному матеріалі Swiss Cyber Institute, приватної освітньої та сертифікаційної організації у Цюриху, соціальну інженерію визначено одним із провідних напрямів кіберзагроз 2025 року, оскільки зловмисники дедалі активніше використовують когнітивні вразливості людини [221].

У даному дослідженні кібербезпеку визначаємо як стан захищеності та сукупність організаційних, правових і технологічних практик, що забезпечують стійке функціонування інформаційних систем, мереж і даних, управління кіберризиками, реагування на інциденти та відновлення після них. Таке розуміння узгоджується з українським законодавством, яке пов’язує кібербезпеку із захищеністю життєво важливих інтересів людини, суспільства й держави під час використання кіберпростору [88]. Базові цілі інформаційної безпеки утворюють конфіденційність, цілісність і доступність інформації. Конфіденційність обмежує доступ уповноваженими суб’єктами, цілісність забезпечує захист від неналежної модифікації або знищення, а доступність підтримує своєчасний і надійний доступ до інформаційних ресурсів [222]. Для подальшого аналізу виокремлюємо три взаємопов’язані рівні кібербезпеки: технологічний, що охоплює засоби захисту й контролю; організаційно-управлінський, до якого належать політики, стандарти, управління доступом та аудит; людський, що включає кібергігієну, підготовку персоналу і протидію соціальній інженерії. Така структура поєднує технічну надійність із процедурами управління та поведінкою користувачів, тому ефективність захисту визначається узгодженістю всіх трьох рівнів.

Розвиток штучного інтелекту змінює співвідношення можливостей захисту й атаки в кіберпросторі, а разом із ним – умови проведення інформаційних операцій. У матеріалі Kyivstar Business Hub зазначено, що ШІ вже використовується для аналізу поведінки користувачів у мережі, створення

персоналізованих повідомлень і підроблення голосу співрозмовника [223]. Той самий ресурс описує застосування машинного навчання для автоматизованого моніторингу трафіку й виявлення нетипової активності [223]. Отже, розвиток ШІ одночасно підвищує точність атак і швидкість їх виявлення. Для нашого дослідження принциповим є те, що персоналізація кібератаки дедалі тісніше зближується з механізмами інформаційно-психологічного впливу. Компрометація облікового запису, голосу, цифрової ідентичності або каналу зв'язку дає змогу звертатися до цільової аудиторії від імені суб'єкта, якому вона вже довіряє. У такій операції технічне проникнення виконує допоміжну функцію, тоді як основний ефект досягається через використання вже сформованих відносин довіри. Це зближує кібероперацію з логікою соціальної інженерії та наративного впливу, де результат залежить не лише від доступу до системи, а й від того, як цей доступ використовується для зміни сприйняття або поведінки людини.

Поширення ШІ водночас змінює темп протиборства. Всесвітній економічний форум у *Global Cybersecurity Outlook 2025* зазначає, що 66 % опитаних організацій очікували найбільшого впливу ШІ на кібербезпеку протягом наступного року, тоді як процедури попереднього оцінювання безпеки ШІ-інструментів мали 37 % респондентів [219]. Розрив між швидкістю впровадження технології та готовністю контролювати пов'язані з нею ризики особливо важливий для державних систем. В умовах війни перевагу отримує сторона, здатна швидше пройти шлях від виявлення уразливості або інформаційного сигналу до перевіреного рішення й реагування. У випадку успішного проникнення часовий фактор працює вже на користь атакуючої сторони: викрадені дані, контроль над каналом комунікації або доступ до облікових записів можуть бути використані раніше, ніж держава встановить характер інциденту й запропонує суспільству підтверджене пояснення. Виникає простір, у якому технічна невизначеність може бути доповнена дезінформацією, суперечливими версіями події або дискредитацією державних повідомлень. Здатність швидко виявити атаку і відновити контроль над інформаційним

середовищем за таких умов стає частиною протидії інформаційно-психологічному впливу.

Інший ризик пов’язаний із розвитком квантових обчислень. У *Global Cybersecurity Outlook 2025* окремо розглянуто модель *harvest now, decrypt later*, за якої зашифровані дані збираються заздалегідь із розрахунком на можливість розшифрувати їх після появи достатніх квантових обчислювальних потужностей [219]. Як засоби підготовки до такого сценарію розглядаються постквантова криптографія та квантове розподілення ключів (Quantum Key Distribution, QKD) [219]. Для держави, що перебуває у тривалому воєнному протистоянні, часовий горизонт захисту інформації не обмежується моментом її передавання. Службове листування, персональні дані, матеріали розвідки, внутрішні документи або відомості про мережі контактів можуть зберігати оперативну цінність протягом багатьох років. Якщо такі масиви згодом буде розшифровано, противник отримає матеріал не тільки для розвідувального аналізу. Вибіркове оприлюднення документів, поєднання достовірних даних із маніпулятивним контекстом, дискредитація конкретних осіб або точніше визначення вразливих аудиторій можуть перетворити давній витік на ресурс нової інформаційної операції. Саме через це постквантовий захист і QKD мають розглядатися в нашому дослідженні не як віддалена технічна перспектива, а як один із засобів збереження конфіденційності інформації, яка може бути використана у майбутніх операціях впливу.

Подальша автономізація систем ШІ посилює цю тенденцію. Штучний загальний інтелект (Artificial General Intelligence, AGI) у межах дослідження розглядаємо не як уже досягнутий технологічний стан і не як прогноз конкретного часу його появи, а як граничний сценарій розвитку автономності систем. Його аналітична цінність полягає в можливості поставити питання про те, що відбудеться з інформаційними операціями, якщо окремі функції, які сьогодні виконуються послідовно різними людьми й програмними засобами, дедалі більше об’єднуватимуться в одному автоматизованому циклі. Йдеться про пошук і систематизацію даних про аудиторію, виявлення її вразливостей,

генерування повідомлень, вибір каналів поширення, аналіз реакцій і коригування наступних дій. У межах запропонованої в дисертації моделі життєвого циклу СІО це означало б скорочення часу між когнітивним картографуванням, конструюванням наративу, його поширенням через визначені канали й платформи та адаптацією за результатами зворотного зв'язку. Принципова зміна полягала б не у появі нового механізму впливу, а в можливості значно швидше поєднувати вже відомі механізми в одному безперервному процесі.

Така перспектива дозволяє точніше визначити місце технологічного розвитку в інформаційній складовій сучасних воєн. ШІ розширює можливості аналізу й персоналізації, компрометація цифрової ідентичності дозволяє експлуатувати вже наявну довіру, а квантові обчислення змінюють часові межі захисту інформації. Подальше зростання автономності може прискорювати зв'язок між вивченням аудиторії та адаптацією впливу. Тому технологічна перевага в кіберпросторі набуває стратегічної ваги тоді, коли вона дозволяє стороні контролювати не тільки доступ до інформаційних ресурсів, а й умови, за яких інформація отримується, перевіряється, інтерпретується та використовується цільовою аудиторією.

На організаційному рівні архітектура нульової довіри переносить акцент із захисту мережевого периметра на постійну перевірку суб'єкта, пристрою та контексту кожного запиту до ресурсу. Доступ визначається ідентичністю, станом пристрою, характеристиками ресурсу та поточним рівнем ризику, а керування ним поєднує контекстну авторизацію, сегментацію ресурсів і безперервне оцінювання подій [224]. Українські дослідники А. Абібулаєв та А. Піскозуб розглядають практичне застосування цієї архітектури у хмарному середовищі, де динамічна перевірка доступу особливо важлива для розподілених систем [225]. Таким чином, сучасна кібербезпека формується як адаптивна система, у якій технологічні рішення підпорядковані управлінню ризиками, людському контролю та здатності організації безперервно перевіряти власну стійкість.

В умовах російсько-української війни кібероперації стали складовою комплексного впливу на державне управління, інформаційні ресурси та

критичну інфраструктуру. Державна служба спеціального зв'язку та захисту інформації України (Держспецзв'язку), державний орган у сфері захисту інформації та кібербезпеки, фіксує випадки координації російської кіберактивності з ракетними ударами та іншими воєнними діями [226]. Таке поєднання змінює функцію кіберудару: порушення роботи систем стає частиною ширшого тиску, у якому одночасно ускладнюються управління, доступ до інформації та комунікація з населенням. Кібероперація в цьому разі може створювати умови для подальшого поширення дезінформації, особливо коли держава змушена відновлювати канали зв'язку й одночасно пояснювати причини технічного збою.

Використання кіберінструментів як засобу політичного тиску простежувалося ще під час Євромайдану 2013–2014 років. Гліб Пахаренко, український фахівець із кібербезпеки, у безпосередньому описі подій аналізує атаки на державні й громадські інформаційні ресурси в умовах гострої політичної кризи [227]. Для подальшого розвитку російської агресії важливим стало поєднання технічного порушення з інформаційною невизначеністю: атакований ресурс тимчасово втрачає функціональність, а суспільство отримує обмежений доступ до офіційної інформації саме в момент підвищеної потреби в ній.

Інший масштаб продемонструвала атака NotPetya у червні 2017 року. У лютому 2018 року адміністрація президента США назвала її найбільш руйнівною і дорогою кібератакою на той момент та поклала відповідальність за операцію на російських військових [228]. Для України наслідки виходили далеко за межі ураження окремих комп'ютерних систем: порушення роботи державних установ, банків, транспортних, енергетичних і приватних компаній показало залежність повсякденного функціонування суспільства від цілісності цифрової інфраструктури.

За телеметрією міжнародної компанії з кібербезпеки ESET, уже представленої раніше в дослідженні, понад 75 % зафіксованих компанією випадків зараження NotPetya припадали на Україну [229]. Подальше поширення

шкідливого програмного забезпечення за межі держави продемонструвало ще одну особливість сучасного кіберпротиборства: операція, спрямована насамперед проти українського середовища, здатна спричиняти транскордонні економічні та інфраструктурні наслідки. Кіберстійкість України за таких умов стає пов'язаною зі стійкістю інформаційних і технологічних систем держав-партнерів.

Напередодні повномасштабного вторгнення кіберактивність набула виразно демонстративного характеру. 14 січня 2022 року Департамент кіберполіції Національної поліції України, спеціалізований підрозділ з протидії кіберзлочинності, повідомив про атаку на понад 70 державних сайтів, серед яких були ресурси Кабінету Міністрів України, Міністерства освіти і науки, Міністерства закордонних справ та інших органів влади [230]. Масовість одночасного порушення доступу створювала ефект, який перевищував технічну шкоду окремому ресурсу. Для громадянина видима недоступність великої кількості державних сайтів могла сприйматися як ознака загальної вразливості державної цифрової системи саме в період різкого зростання воєнної загрози.

Майже одночасно Microsoft Threat Intelligence – аналітичний підрозділ корпорації Microsoft з дослідження кіберзагроз – виявила у системах українських організацій WhisperGate [231]. Програма імітувала ransomware, однак була орієнтована на знищення даних і виведення систем із ладу [231]. Публічно видимі атаки на вебресурси й приховане деструктивне проникнення виконували різні функції одного тиску: перші демонстрували вразливість, друге створювало реальну загрозу втрати інформації та порушення внутрішніх процесів.

Ще чіткіше зв'язок між кібероперацією та воєнними діями проявився 24 лютого 2022 року. Приблизно за годину до початку повномасштабного вторгнення було здійснено атаку на супутникову мережу Viasat, яку використовували, зокрема, українські військові [232]. Наслідки одночасно відчули тисячі цивільних і комерційних користувачів у Європі [232]. Порушення зв'язку в момент початку бойових дій мало безпосередню оперативну функцію, але водночас розширювало простір невизначеності, у якому ускладнювалися

передавання інформації, координація та перевірка повідомлень.

У 2023–2024 роках російська кіберактивність дедалі більше поєднувала деструктивні дії з прихованим проникненням, розвідкою та тривалим закріпленням у системах [226]. Така зміна важлива для інформаційного протиборства, оскільки отримані під час проникнення відомості можуть використовуватися пізніше: для підготовки наступної атаки, персоналізованої соціальної інженерії, дискредитації посадових осіб або побудови повідомлень на основі реальних внутрішніх даних. Кіберрозвідка в такій конфігурації створює інформаційну базу для точнішого вибору цілей і способів впливу.

У грудні 2024 року масштабна кібератака призвела до зупинення роботи державних реєстрів і суттєво ускладнила надання адміністративних послуг [233]. Тут зв’язок між технічним інцидентом і суспільним сприйняттям проявляється особливо безпосередньо. Для громадянина цифрова держава існує через можливість отримати документ, підтвердити право, зареєструвати дію або скористатися сервісом. Тривала недоступність таких функцій переносить наслідок кібератаки з технологічної інфраструктури у сферу щоденної взаємодії людини з державою. У межах наведеного кейсу довіра до надійності державних цифрових сервісів стає одним із супутніх об’єктів кібертиску.

Масштаб операційного навантаження характеризують дані CERT-UA – урядової команди реагування на комп’ютерні надзвичайні події України, що діє в системі Держспецзв’язку. У 2024 році команда опрацювала 4315 кіберінцидентів, що на 69,8 % перевищило показник попереднього року [234]. Показник відображає середовище постійного тиску, у якому захист уже не може будуватися навколо реагування на поодинокий інцидент. Державна система має одночасно виявляти нові проникнення, відновлювати ресурси, накопичувати інформацію про способи атак і підтримувати безперервність критичних сервісів.

Паралельно розширюється внутрішня технологічна й професійна база кіберзахисту. В огляді ринку, підготовленому галузевою IT Ukraine Association спільно з European Business Association за підтримки USAID, обсяг українського ринку кібербезпеки у 2024 році оцінено приблизно у 138 млн дол. США, а за

вісім років він зріс приблизно вчетверо [235]. Для нашого аналізу цей показник характеризує формування внутрішньої спроможності підтримувати захист і відновлення в умовах тривалого воєнного навантаження. Розширення ринку відбувається одночасно зі збільшенням кількості інцидентів, тобто розвиток національної кіберекосистеми значною мірою формується безпосередньо під тиском війни.

Сукупність наведених кейсів дозволяє перейти від хронології російських атак до їх функціонального аналізу. Для предмета цього дослідження принциповим є те, яким способом кібероперація впливає на спроможність держави діяти, комунікувати й підтримувати довіру, а також які можливості вона створює для подальших інформаційних операцій. На цій підставі виокремлюємо чотири взаємопов’язані тактики: порушення доступності сервісів, деструктивний вплив на дані й системи, приховане проникнення та кібершпигунство, компрометацію користувачів через соціальну інженерію.

1. Порушення доступності державних і суспільно значущих сервісів реалізується насамперед через масштабні DDoS-атаки. Глобальна статистика NETSCOUT фіксує 8 911 312 таких атак у другому півріччі 2024 року, що на 12,75 % перевищує показник першого півріччя. Ця динаміка характеризує загальне поширення інструменту, тоді як у російсько-українській війні DDoS-атаки використовуються для тимчасового порушення доступності державних ресурсів, мереж зв’язку та інших критичних сервісів [236]. Автоматизація та сервіси DDoS-for-hire знижують поріг входу для операторів і дають змогу масштабувати атаки, змінювати їхню географію та швидко перебудовувати параметри трафіку [236]. Політичний ефект цієї тактики виникає через видиму недоступність державних ресурсів, яка створює відчуття некерованості та посилює тиск у кризовий момент. У разі синхронізації з кінетичними ударами DDoS-атака ускладнює інформування населення, роботу органів влади та координацію реагування, тому короткочасне технічне порушення може отримувати ширший воєнно-політичний результат.

2. Деструктивні операції із застосуванням wiper-програм спрямовуються на знищення даних і порушення функціонування систем. ESET зафіксувала розгортання HermeticWiper, IsaacWiper та CaddyWiper у лютому–березні 2022 року, а також застосування Industroyer2 проти енергетичної інфраструктури України [237]. Спільною рисою цих операцій є орієнтація на незворотну втрату доступності або цілісності даних, що відрізняє їх від класичного вимагання викупу. У воєнних умовах технічна шкода доповнюється психологічним впливом, оскільки демонструє здатність противника проникати до систем, пов’язаних із життєзабезпеченням держави. Відновлення після таких інцидентів охоплює перевірку резервних копій, очищення інфраструктури, відновлення довірених конфігурацій і повторну верифікацію облікових записів. Через це wiper-операції одночасно виснажують технічні ресурси та відволікають фахівців від інших напрямів захисту.
3. Приховане проникнення та кібершпигунство використовують фішингові повідомлення, викрадення облікових даних і троянські програми віддаленого доступу. Такі засоби дають змогу отримувати документи, службове листування та інші дані зі скомпрометованих пристроїв, створюючи канал для подальшого розвідувального використання. Угруповання UAC-0010, яке CERT-UA пов’язує з ФСБ РФ, здійснює тривалі кампанії проти українських державних органів [238]. Інші кампанії, зокрема активність, пов’язана з GhostWriter, демонструють залучення союзних Росії державних кіберсуб’єктів. У звіті Держспецзв’язку за друге півріччя 2023 року окремо виділено активність військових кіберпідрозділів противника, які діяли проти державного сектору й оборонних цілей [239]. Специфіка цієї тактики полягає в тривалому прихованому перебуванні в системі, накопиченні інформації та створенні умов для подальших операцій. Здобуті відомості можуть використовуватися для підготовки деструктивної атаки, вибору персоналізованих фішингових повідомлень або дискредитації посадових

осіб. Тому протидія кібершпигунству поєднує технічне виявлення проникнення з контролем привілеїв, захистом службового листування та аналізом аномальної поведінки користувачів.

4. Соціальна інженерія використовується для компрометації облікових записів і отримання доступу до службових комунікацій. Викрадені дані та захоплені канали зв'язку надалі можуть забезпечувати інформаційно-психологічний вплив. З огляду на активне використання військовими месенджера Signal російські спецслужби застосовують фішингові ресурси, що імітують вебсайти підрозділів Сил оборони України й пропонують приєднатися до груп у цьому сервісі. Після сканування підробленого QR-коду до облікового запису Signal може бути прив'язаний пристрій, контрольований зловмисником. Це відкриває доступ до подальшого листування та службових контактів користувача [240]. Подібні методи використовуються також для компрометації облікових записів у WhatsApp, Telegram та інших месенджерах. Успішне захоплення каналу комунікації дає змогу імітувати довіреного співрозмовника, збирати відомості про структуру підрозділу та поширювати повідомлення від імені реального користувача. Узагальнюючи наведені приклади, визначаємо кібероперації інструментом одночасного впливу на технічну стійкість і суспільне сприйняття. Порушення роботи сервісів, витоки даних і компрометація каналів зв'язку створюють відчуття вразливості держави та посилюють інформаційно-психологічний тиск.

Правовий та інституційний контур кібербезпеки України розвивається відповідно до досвіду повномасштабної війни й потреби узгодити дії державних органів, операторів критичної інфраструктури та команд реагування. Науковий аналіз стану кібербезпеки України в умовах воєнного стану також пов'язує ефективність протидії кіберзагрозам з узгодженою взаємодією суб'єктів забезпечення кібербезпеки [241]. Закон України № 4336-IX від 27 березня 2025 року оновив правові засади захисту державних інформаційних ресурсів та об'єктів критичної інформаційної інфраструктури [242]. Він конкретизував

повноваження Держспецзв'язку щодо координації реагування на кіберінциденти, обміну інформацією про загрози та оцінювання стану кіберзахисту державних ресурсів і критичної інформаційної інфраструктури [242]. Закон запровадив оцінювання стану кіберзахисту, аудит інформаційної безпеки та обов'язки щодо повідомлення про кіберінциденти. Ці механізми формують спільні вимоги до контролю захищеності державних ресурсів і критичної інфраструктури. Закон № 4336-IX наблизив українські механізми управління кіберризиками та повідомлення про інциденти до окремих вимог Директиви NIS2. Подальша гармонізація охоплює секторні вимоги, нагляд і відповідальність керівництва [243]. Директива NIS2 поширює вимоги з управління кіберризиками та повідомлення про значні інциденти на ширше коло суттєвих і важливих суб'єктів. Вона також закріплює відповідальність органів управління за затвердження заходів кібербезпеки та нагляд за їх виконанням [243]. Гармонізація кібербезпекового законодавства входить до ширшого процесу європейської інтеграції України та реалізації реформ у цифровому секторі. Реалізацію стандартів NIS2 пов'язуємо з модернізацією інформаційних систем, підготовкою фахівців, розвитком моніторингу та спроможністю безперервного реагування на інциденти. Окремим напрямом інституціоналізації військових кіберспроможностей є проєкт Закону № 12349 про Кіберсили Збройних Сил України, зареєстрований 19 грудня 2024 року. Верховна Рада прийняла його за основу 9 жовтня 2025 року, а станом на серпень 2026 року законопроєкт був підготовлений до розгляду в другому читанні й перебував на відповідній стадії парламентської процедури [244]. У законопроєкті Кіберсили визначено як спеціалізований компонент Збройних Сил, орієнтований на кібероборону, кіберрозвідку та проведення операцій у кіберпросторі в межах повноважень сектору оборони [244]. Досвід США і Польщі демонструє дві моделі інституціоналізації військових кіберспроможностей: об'єднане бойове командування та спеціалізований компонент збройних сил. В обох випадках організаційне відокремлення кіберфункцій забезпечує концентрацію кадрового потенціалу, вироблення спільних процедур і постійне планування операцій у

кіберпросторі. Українські дослідники С. Вдовенко та Ю. Даник у рецензованій статті про системи кібербезпеки й кібероборони провідних держав окремо характеризують освітню та наукову інфраструктуру США [245]. За їхньою оцінкою, наприкінці 2019 року органи управління й підрозділи видів Збройних сил США, залучені до виконання завдань кібероборони, налічували близько 50 тис. військовослужбовців і працівників [245]. У лютому 2022 року Польща офіційно сформувала Війська оборони кіберпростору (Wojska Obrony Cyberprzestrzeni) як спеціалізований компонент збройних сил [246]. Перспективний напрям розвитку військових кіберспроможностей України пов'язуємо з обміном інформацією про загрози, спільними навчаннями та сумісністю процедур із партнерами НАТО і ЄС. Формування Кіберсил також пов'язуємо з розвитком спеціалізованої підготовки, професійного відбору та науково-технічного забезпечення, інтегрованих із загальною системою кіберосвіти й підготовки кадрів сектору безпеки та оборони. У межах наведеного аналізу визначаємо специфіку кібербезпеки у воєнних умовах через поєднання технічного захисту, безперервного реагування, правової координації та військових кіберспроможностей. Її результативність виявляється у здатності держави підтримувати функціонування критичних сервісів, обмежувати розвідувальні й деструктивні можливості противника та зберігати суспільну довіру під час комплексного воєнного тиску.

Висновки до розділу 2

У цьому розділі цифрове середовище розглянуто як простір, де деструктивні наративи, алгоритмічні системи, соціальні медіа, автоматизовані інструменти виявлення дезінформації та кібербезпекові практики взаємодіють у межах єдиного механізму інформаційно-психологічного протиборства.

1. Встановлено, що новітні комунікативні технології змінюють саму конфігурацію інформаційної війни. Вплив на суспільну свідомість у цифровому середовищі здійснюється через поєднання смислової конструкції, каналу поширення, алгоритмічного підсилення, емоційного

резонансу та поведінкової реакції аудиторії. За таких умов інформаційна операція вже не може бути пояснена лише змістом повідомлення, оскільки її результат залежить від того, як платформа ранжує контент, кому його показує, у який момент підсилює і в якій аудиторній спільноті закріплює. У цьому полягає принципове уточнення механізму впливу: цифрова інфраструктура стає активним елементом інформаційної війни, а не зовнішнім каналом передавання повідомлень.

2. Обґрунтовано, що деструктивні наративи в сучасному інформаційному середовищі функціонують як повторювані схеми політичного тлумачення реальності. Їхня функціональна роль полягає в упорядкуванні для аудиторії складних подій, заданні емоційної оцінки, посиленні недовіри до інституцій і формуванні бажаних для ініціатора поведінкових орієнтирів. Саме тому протидія дезінформації не може обмежуватися спростуванням окремих фейків після їхнього поширення. Ефективнішими є ті інструменти, які працюють із логікою наративу: виявляють смислові повтори, фіксують джерела поширення, пояснюють маніпулятивні прийоми, попереджають аудиторію про типові схеми обману й формують здатність розпізнавати деструктивний вплив до моменту його закріплення.
3. Систематизація інструментів виявлення та подолання деструктивних впливів дозволила розмежувати кілька рівнів інформаційного захисту. Автоматизована детекція, OSINT-моніторинг, аналіз бот-мереж, фактчекінг, дебанкінг, пребанкінг, цифрова верифікація, контрнаративи й медіаграмотність виконують різні функції, але мають працювати як взаємопов’язані елементи. Автоматизовані системи швидко фіксують аномалії й технічні ознаки координованої активності; фактчекінг повертає аудиторію до перевірюваного факту; пребанкінг формує попередню стійкість до типових маніпуляцій; контрнаративи відновлюють смислову цілісність там, де противник намагається нав’язати викривлене пояснення подій. Така типологія уточнює прикладний інструментарій протидії деструктивним впливам і показує, що захист суспільної свідомості

потребує одночасної роботи з фактами, смислами, технологіями та аудиторними вразливостями.

4. Соціальні медіа обґрунтовано як один із провідних механізмів інформаційно-психологічного впливу на суспільну свідомість і поведінку. Їхня роль визначається здатністю поєднувати персоналізоване поширення повідомлень, емоційне підсилення конфліктних тем, алгоритмічне формування порядку денного, створення цифрових ехо-камер та імітацію масової підтримки через бот-мережі й астротурфінг. У такій конфігурації соціальні медіа впливають на аудиторію не тільки через інформацію, яку вона отримує, а й через відчуття соціального підтвердження, групової належності, загрози або морального обурення. Саме тому політичний ефект соціальних медіа має оцінюватися через зміну сприйняття, довіри, емоційної мобілізації та готовності громадян підтримувати або відкидати певні рішення.
5. Аргументовано асиметрію можливостей цифрового інформаційного впливу: його масштаб і результативність не перебувають у прямій залежності від обсягу залучених ресурсів. Алгоритмічне підсилення, персоналізація, повторюваність і мережеве поширення дають змогу окремим повідомленням та координованим кампаніям досягати значного охоплення й закріплюватися в інформаційному середовищі. Деструктивний вплив може досягати значного ефекту навіть за відносно обмежених ресурсів, якщо повідомлення потрапляє в аудиторію з високою емоційною вразливістю та багаторазово підсилюється платформною логікою рекомендацій. Повторюваність, візуальна простота, короткий формат, емоційна насиченість і можливість миттєвого поширення перетворюють окремі меседжі на стійкі інтерпретаційні схеми. У цьому проявляється нова якість цифрового інформаційно-психологічного впливу: він діє не лінійно, а мережево, через взаємне підсилення контенту, аудиторії, алгоритму й політичного контексту.

6. Розкрито специфіку кібербезпеки як складника інформаційної безпеки держави у воєнних умовах. Кібератаки на державні реєстри, системи зв'язку, медійні ресурси, цифрові сервіси та критичну інфраструктуру створюють не тільки технічні порушення, а й політико-психологічні наслідки: втрату довіри, паніку, відчуття безпорадності, сумнів у спроможності держави та інформаційну дезорієнтацію. Через це кіберзахист повинен розглядатися в одній системі зі стратегічними комунікаціями, аналітичним моніторингом і протидією інформаційно-психологічним операціям. Технічна стійкість цифрової інфраструктури створює умови для збереження інформаційної орієнтації суспільства, тоді як порушення доступності, цілісності або достовірності даних може ставати чинником політичного й психологічного тиску.
7. Встановлено взаємозв'язок між механізмами ведення інформаційної війни в умовах поширення новітніх комунікативних технологій, роллю соціальних медіа в інформаційно-психологічному впливі та специфікою застосування механізмів кібербезпеки у воєнних умовах. Показано, що провідні наративи поширюються через цифрові платформи, підсилюються алгоритмами, адаптуються до вразливостей цільових аудиторій і підтримуються координованою мережевою активністю. Водночас інформаційно-психологічний вплив може поєднуватися з кіберзагрозами, що дає підстави розглядати механізми впливу на суспільну свідомість як взаємодію смислового, технологічного, психологічного та безпекового рівнів.

РОЗДІЛ 3. ІНФОРМАЦІЙНИЙ СУПРОВІД ПРОТИДІЇ РОСІЙСЬКІЙ ЗБРОЙНІЙ АГРЕСІЇ ПРОТИ УКРАЇНИ

3.1. Політико-правові засади забезпечення безпеки інформаційного простору України у воєнних умовах

Безпеку інформаційного простору в умовах російської збройної агресії визначаємо як здатність держави забезпечувати стійкість інституцій, суспільну довіру, захищеність публічних комунікацій та узгодженість дій державних інституцій під тиском цілеспрямованого ворожого впливу. Практичне значення цього визначення розкривається через спроможність своєчасно переходити від виявлення загрози до правомірного рішення, його виконання та оцінювання наслідків. Правова форма і процедурна відтворюваність надають такому реагуванню передбачуваності, а суспільне пояснення підтримує легітимність обмежувальних заходів. Одним із показових етапів стала санкційна практика 2017 року щодо російських соціальних мереж і цифрових сервісів. У межах нашого аналізу цей кейс розглядаємо як перехід до сприйняття цифрової платформи як потенційної інфраструктури ворожого впливу. Аналітичний матеріал міжнародної правозахисної організації Freedom House 2019 року розглядав доцільність збереження санкцій проти російських технологічних компаній і порушував питання їхньої ефективності та впливу на цифрові права [247]. Пропонуємо розглядати пролонгацію санкцій як окремий етап оцінювання їхньої ефективності, пропорційності та актуальності.

Поєднання оперативності реагування, правової визначеності та суспільної довіри спирається на конституційні гарантії свободи вираження поглядів і доступу до інформації. Стаття 34 Конституції України гарантує свободу думки і слова, вільне вираження поглядів і переконань, а також право збирати, зберігати, використовувати й поширювати інформацію. Водночас ця стаття допускає встановлені законом обмеження в інтересах національної безпеки, територіальної цілісності, громадського порядку та захисту прав інших осіб. Стаття 64 Конституції України допускає встановлення окремих обмежень прав і

свобод в умовах воєнного або надзвичайного стану із зазначенням строку їх дії та визначає права, які зберігають абсолютний захист [248]. Захист інформаційного простору набуває легітимності за умови нормативної визначеності, процедурної відтворюваності та контрольованого застосування винятків.

Закон України «Про правовий режим воєнного стану» визначає воєнний стан як спеціальний правовий режим, що запроваджується у разі збройної агресії або загрози нападу та передбачає надання органам державної влади, військовому командуванню і військовим адміністраціям повноважень, необхідних для відвернення загрози й забезпечення національної безпеки [249]. Виходячи з передбаченого законом розширення повноважень органів державної влади, визначаємо своєчасність, міжвідомчу узгодженість і перевірюваність рішень як критерії їхньої результативності в інформаційній сфері. Такий підхід пов'язує оперативність воєнного управління з можливістю встановити правову підставу, компетентного суб'єкта, строк і мету кожного обмеження.

Процедурні рамки обмеження доступу до інформації встановлює Закон України «Про доступ до публічної інформації». Обмеження доступу допускається за сукупності трьох умов: воно переслідує визначену законом мету, розголошення може завдати істотної шкоди охоронюваному інтересу, а ця шкода переважає суспільний інтерес в отриманні інформації [250]. Ця процедура дає змогу обґрунтовувати необхідність обмежень і відмежовувати їх від довільного розширення державного втручання. У воєнних умовах трискладовий тест зберігає значення як інструмент індивідуалізації рішення, оскільки пов'язує його з конкретною інформацією, конкретною шкодою та актуальним суспільним інтересом.

Закон України «Про інформацію» визначає загальні засади інформаційних відносин, права їхніх учасників та принципи інформаційної діяльності. Його предмет охоплює документовану або публічно оголошену інформацію незалежно від форми її подання, що забезпечує базову нормативну єдність для паперових, аудіовізуальних і електронних форм даних [251]. Спеціальні

повноваження щодо цифрових платформ, медіасервісів і технічної інфраструктури водночас потребують опори на профільні нормативні акти. У такий спосіб загальний закон визначає принципи інформаційних відносин, а спеціальне законодавство конкретизує засоби реагування.

Закон України «Про медіа» систематизував правові засади діяльності суб'єктів у сфері аудіовізуальних, друкованих та онлайн-медіа [252]. Він деталізував статус суб'єктів у сфері медіа, повноваження Національної ради України з питань телебачення і радіомовлення та процедури застосування заходів реагування. Для безпеки інформаційного простору значення цього акта полягає у переході до постійного регуляторного режиму, в якому компетенції, адресати та наслідки порушень визначаються наперед. Така формалізація підвищує передбачуваність рішень і створює правову основу для реагування на загрози в сучасному медійному середовищі.

Баланс безпеки та прав і свобод у воєнний час є ресурсом стійкості. Легітимність процедур визначає, чи зможе держава утримати довіру громадян тоді, коли обмеження інформаційних прав стають відчутними. У цьому сенсі правові запобіжники не послаблюють безпеку, а роблять її стійкішою, звужуючи простір для делегітимації державних рішень. Українська правова рамка допускає обмеження за наявності законної мети, установленої процедури та можливості контролю. Конституційна допустимість обмежень і трискладовий тест доступу до інформації тому виступають взаємопов'язаними орієнтирами правомірного реагування.

Правова еволюція захисту інформаційного простору охоплює перехід від загальних засад інформаційних відносин до організаційно-технічних процедур. Закон України «Про захист інформації в інформаційно-комунікаційних системах» визначає комплексну систему захисту інформації як взаємопов'язану сукупність організаційних та інженерно-технічних заходів, засобів і методів захисту інформації [253]. Ця конструкція переводить безпекову вимогу в площину проєктування систем, розподілу відповідальності, застосування технічних засобів і перевірки їхньої дієвості. Закон сформував ранню

нормативну основу організаційного й технічного захисту інформаційних систем; окреме законодавче оформлення кібербезпеки відбулося пізніше.

Після початку російської збройної агресії у 2014 році важливого значення набули спеціальні обмежувальні заходи безпекової політики. У межах цього дослідження санкції розглядаємо як спеціальні обмежувальні заходи, правові підстави та порядок застосування яких визначено Законом України «Про санкції». Закон закріплює принципи законності, прозорості, об'єктивності, відповідності меті та ефективності застосування санкцій [254]. Виходячи з цих принципів, визначаємо доказовість і контрольованість процедури як умови суспільної легітимності санкцій. У медійно-цифровому середовищі ця вимога має особливу вагу, оскільки наслідки рішення безпосередньо впливають на доступ до інформації та політичну комунікацію.

Закон України «Про національну безпеку України» закріпив загальні засади функціонування сектору безпеки і оборони та пов'язав захист державного суверенітету, територіальної цілісності, демократичного конституційного ладу й інших національних інтересів у цілісну систему [255]. У цій системі безпека інформаційного простору набуває міжсекторального характеру, оскільки залежить від політичних рішень, правового регулювання, захисту інфраструктури та стратегічних комунікацій. Такий підхід дає підстави оцінювати інформаційні обмеження через їхній внесок у захист конкретного національного інтересу, а не через абстрактне посилання на безпеку.

У 2017–2018 роках законодавче оформлення кібербезпеки та сектору національної безпеки уточнило місце інформаційної сфери в загальній системі державної безпеки. Закон України «Про основні засади забезпечення кібербезпеки України» орієнтує кібербезпекову політику на захищеність життєво важливих інтересів людини, суспільства й держави під час використання кіберпростору [88]. У запропонованій нами структурі кібербезпеку визначаємо функціональною підсистемою захисту інформаційного простору, що забезпечує стійкість цифрової інфраструктури та даних. Це розмежування зберігає самостійність технічних завдань кіберзахисту й водночас показує їхній

вплив на доступність державних сервісів, достовірність інформації та безперервність публічної комунікації.

Доктрина інформаційної безпеки 2017 року окреслила актуальні загрози національним інтересам та напрями державної політики в інформаційній сфері [256]. Її значення полягало в систематизації російського інформаційного впливу, визначенні завдань державних органів і поєднанні безпекового, комунікаційного та інституційного вимірів. Доктрина створила стратегічну основу для переходу від реагування на окремі інформаційні прояви до формування узгоджених напрямів державної політики. Для практичної реалізації такого підходу вирішальним стає переведення стратегічних пріоритетів у компетенції, процедури й вимірювані завдання.

Стратегія інформаційної безпеки 2021 року визначила стратегічні цілі, напрями державної політики та механізми їх досягнення в умовах інформаційної агресії [257]. Документ пов’язав захист інформаційного простору зі стратегічними комунікаціями, розвитком інформаційного суспільства, підвищенням медіаграмотності та інституційною координацією. Стратегічні документи таким чином поєднують загальні нормативні засади з визначенням загроз, цілей, завдань та інституційних механізмів державної політики. Пропонуємо оцінювати їх виконання через регулярний моніторинг результатів, актуальності загроз і відповідності застосованих інструментів поставленим цілям.

Міжвідомчу координацію визначаємо центральною умовою перетворення стратегічних орієнтирів на виконувані рішення. Її зміст охоплює встановлення суб’єкта ініціювання, порядку підготовки матеріалів, способу обміну даними, відповідального виконавця та процедури оцінювання результату. За такої організації стратегічний документ задає спільну логіку дій, а законодавство визначає межі компетенції кожного органу. Це забезпечує послідовність державної політики й скорочує ризик суперечливих рішень у ситуаціях, що потребують швидкого реагування.

Санкційний і медіарегуляторний механізми розрізняються правовими

підставами, компетентними суб'єктами, адресатами та процедурами застосування. Закон України «Про санкції» регулює спеціальні обмежувальні заходи, спрямовані на захист національних інтересів і безпеки [254]. Закон України «Про медіа» встановлює постійний порядок функціонування медійної сфери та компетенцію Національної ради щодо нагляду й реагування [252]. Розмежування компетенцій регулятора та органів сектору безпеки визначаємо умовою процедурної узгодженості рішень. Процедурна непрозорість створює умови для політичної інтерпретації санкцій і ускладнює їх суспільне обґрунтування.

Одним із перших масштабних кейсів застосування санкцій у цифровій сфері стало рішення травня 2017 року. Указ Президента України № 133/2017 увів у дію рішення Ради національної безпеки і оборони України щодо застосування персональних спеціальних економічних та інших обмежувальних заходів. У додатках до рішення серед адресатів санкцій зазначено російські компанії та сервіси, пов'язані з «ВКонтакте», «Одноклассники», «Яндекс» і Mail.ru [258]. У межах нашого аналізу рішення 2017 року розглядаємо як застосування санкцій до цифрової інфраструктури, яку держава віднесла до безпекових ризиків. Масштаб наслідків для повсякденних цифрових практик громадян водночас підвищив значення публічного пояснення мети й строку таких заходів.

Міжнародна правозахисна організація Human Rights Watch, яка здійснює моніторинг дотримання прав людини в різних країнах, критично оцінила блокування російських вебкомпаній як захід, що створював ризики для свободи вираження поглядів і доступу до інформації [259]. Ця позиція не усуває безпекового контексту рішення, проте нагадує про необхідність індивідуалізації обмежень і перевірки їхньої пропорційності. Для української практики така зовнішня оцінка важлива як тест спроможності аргументувати зв'язок між конкретною платформою, конкретною загрозою та обсягом втручання.

Комісар Ради Європи з прав людини, незалежна інституція Ради Європи з моніторингу та захисту прав людини, у 2017 році наголосив на небезпеці довільного блокування інтернет-ресурсів для свободи вираження поглядів [260].

У політико-правовому вимірі ця позиція акцентує на якості закону, доступності процедур оскарження та передбачуваності правових наслідків. Відтак безпекова ефективність цифрового обмеження має оцінюватися разом із точністю визначення адресата та можливістю перегляду рішення.

Наступним резонансним етапом стало застосування санкцій до медійних активів у лютому 2021 року. Указ Президента України № 43/2021 увів у дію рішення РНБО щодо застосування санкцій, яке стосувалося Тараса Козака та пов'язаних із ним телеканалів «112 Україна», ZIK і NewsOne [261]. Кейс показав, що санкційний механізм може безпосередньо впливати на структуру телевізійного мовлення та доступ аудиторії до медіаконтенту. Тому його правова й суспільна оцінка залежить від переконливого встановлення зв'язку між адресатами заходів і загрозою національній безпеці.

У публічному обґрунтуванні рішення щодо телеканалів ішлося про джерела їх фінансування та зв'язки власника з окупованими територіями. Human Rights Watch розглянула цей випадок як складну проблему співвідношення національної безпеки та свободи медіа й звернула увагу на застосування санкційного механізму без попереднього судового рішення [262]. Цей аргумент підсилює вимогу до перевірюваної доказової бази й доступного механізму правового захисту. У межах нашого аналізу саме процедурна повнота визначає, чи буде швидке безпекове рішення сприйняте як правомірне й пропорційне.

Представник ОБСЄ з питань свободи медіа, інституція Організації з безпеки і співробітництва в Європі, що здійснює раннє попередження та підтримує дотримання зобов'язань у сфері свободи вираження, обговорив рішення з постійним представником України при ОБСЄ та наголосив на необхідності дотримання міжнародних стандартів свободи вираження [263]. Комунікація з міжнародними інституціями в такій ситуації виконує подвійну функцію: дає змогу представити безпекові підстави рішення й водночас виявити процедурні аспекти, які потребують додаткового обґрунтування.

Кейс серпня 2021 року був критично оцінений Представницею ОБСЄ з питань свободи медіа Терезою Рібейро, яка 25 серпня 2021 року висловила

занепокоєння практикою застосування санкцій, що негативно впливають на роботу медіа та журналістів [264]. Ця оцінка конкретизувала міжнародну вимогу до розмежування протидії ворожому інформаційному впливу та захисту професійної журналістської діяльності. Для політико-правового дизайну відповідний сигнал означає потребу в адресності заходу, чіткому викладенні підстав і процедурі перегляду.

Указ Президента України № 376/2021 увів у дію рішення РНБО від 20 серпня 2021 року про застосування персональних спеціальних економічних та інших обмежувальних заходів. У додатках до рішення зазначено осіб та пов'язані з ними активи, щодо яких було застосовано санкції [265]. Персональний характер таких заходів загострює питання правової підстави, встановлення індивідуального зв'язку із загрозою та можливості оскарження. В інформаційній сфері ці елементи особливо важливі, оскільки персональні санкції легко стають предметом політичної інтерпретації.

У звіті Freedom on the Net 2021, підготовленому міжнародною правозахисною організацією Freedom House, персональні санкції й блокування ресурсів розглядалися серед чинників погіршення свободи інтернету в Україні [266]. Оцінка відображала зовнішнє сприйняття української практики та показувала, що безпекова мета сама по собі не знімає питань щодо способу застосування обмежень. Виходячи з цього, персональні санкції в інформаційній сфері мають спиратися на чіткі правові підстави, перевірювану доказову базу та публічне пояснення зв'язку між адресатом санкцій і конкретною загрозою.

Безпосередньо напередодні повномасштабного вторгнення показовим став кейс телеканалу «НАШ» та пов'язаних структур. Рішення РНБО від 11.02.2022 було введене в дію Указом Президента № 52/2022 [267]. У цьому випадку санкційне рішення набуло додаткового значення через близькість до початку великої війни й тому розглядалося як елемент превентивного захисту інформаційного простору.

Ширший політичний контекст російського втручання напередодні повномасштабного вторгнення відображено в повідомленні уряду Великої

Британії від 22 січня 2022 року про виявлений план Кремля щодо формування проросійського керівництва в Україні [268]. Цей матеріал не встановлює причинного зв'язку із санкційним рішенням щодо телеканалу «НАШ», однак підтверджує масштаб зовнішньополітичної та інформаційної загрози, у середовищі якої українська держава ухвалювала безпекові рішення.

Після 24 лютого 2022 року правові механізми протидії російській пропаганді розвивалися одночасно в Україні та європейських державах. Дослідження Андрея Ріхтера, автора публікації Європейської аудіовізуальної обсерваторії – спеціалізованої структури Ради Європи у сфері аудіовізуальних медіа, аналізує формування правових механізмів обмеження поширення російських і білоруських аудіовізуальних медіа, пов'язаних із пропагандою війни [269]. Для України така синхронізація з європейською практикою підвищує значення правової визначеності, цільового характеру й пропорційності обмежень. Спільність безпекової проблеми водночас не скасовує потреби враховувати національну компетенцію та процедури кожної правової системи.

Офіційне повідомлення від 27 грудня 2025 року засвідчує синхронізацію частини українських санкцій із Великою Британією та застосування обмежень відповідно до резолюцій Ради Безпеки ООН [270]. Така практика демонструє включення української санкційної політики до ширших міжнародних режимів і посилює потребу в сумісності критеріїв, доказів та процедур. Синхронізацію розглядаємо як інструмент зовнішньої легітимації, який доповнює, але не замінює внутрішнє правове обґрунтування кожного рішення.

У січні 2026 року санкції було застосовано до російських спортивних пропагандистів і діячів шоу-бізнесу, залучених до підтримки агресії [271]. Цей кейс засвідчує розширення кола адресатів інформаційних санкцій за межі традиційних медіаорганізацій. Для оцінювання таких рішень пропонуємо враховувати конкретну роль особи у виробництві, легітимації або поширенні пропагандистського впливу, а також очікуваний практичний ефект установленого обмеження.

Регламент Ради Європейського Союзу 2022/350 від 1 березня 2022 року

встановив обмеження на мовлення та поширення контенту RT і Sputnik у Європейському Союзі [272]. Заходи були адресовані визначеним державним медіа Росії та прямо пов’язані з їхньою роллю в підтримці агресії проти України. Рішення мало адресний і тимчасовий характер та поширювалося на визначених суб’єктів, пов’язаних із російською державною пропагандою. Європейський досвід у цьому випадку показує можливість поєднання жорсткого обмеження з конкретизацією адресатів, предмета й безпекової мети.

Перехід від санкційної практики до організаційно-технологічного забезпечення розкриває інший рівень безпеки інформаційного простору. Його стійкість залежить від надійності інформаційно-комунікаційних систем, узгодженості стандартів захисту, безперервності обміну даними та здатності суб’єктів оперативно реагувати на інциденти. Цей рівень забезпечує матеріальну основу для виконання політичних рішень і підтримує функціонування державних комунікацій у воєнних умовах.

Комплексна система захисту інформації охоплює взаємопов’язані організаційні та інженерно-технічні заходи, засоби й методи [253]. Її практична дієвість визначається узгодженням вимог безпеки з архітектурою системи, розподілом відповідальності та регулярною перевіркою захисних механізмів. У контексті державного управління така система підтримує конфіденційність, цілісність і доступність інформаційних ресурсів, від яких залежать управлінські рішення та публічні сервіси. Організаційний компонент при цьому має таку саму вагу, як технічний, оскільки встановлює порядок дій і відповідальність суб’єктів.

Законодавчу рамку кібербезпеки формує Закон України «Про основні засади забезпечення кібербезпеки України», який визначає суб’єктів національної системи кібербезпеки, їхні основні завдання та напрями взаємодії [88]. Стратегія кібербезпеки України, введена в дію Указом Президента України № 447/2021, визначила пріоритети розвитку кіберстійкості, захисту критичної інформаційної інфраструктури та координації суб’єктів [273]. У запропонованій нами моделі технічний і комунікаційний рівні поєднуються через наслідки кіберінцидентів для доступності інформації, довіри до державних сервісів і

спроможності інституцій підтримувати безперервну комунікацію. Організацію протидії визначаємо через поєднання інструментів, процедур міжвідомчої взаємодії та критеріїв результативності.

Антон Русакевич, аспірант Національного технічного університету «Дніпровська політехніка», розглядає інформаційну безпеку в умовах воєнного стану у зв'язку із захистом інформаційних прав громадян [274]. Його підхід акцентує на нормативній визначеності діяльності органів влади, дотриманні встановлених законом меж обмеження прав і підтриманні правових гарантій у надзвичайному безпековому середовищі. Для нашого аналізу ця позиція підтверджує, що процедурна якість є складником результативності інформаційної політики, оскільки визначає передбачуваність дій держави та можливість їх правової оцінки.

Галина Красноступ, кандидат юридичних наук, старший науковий співробітник і провідний науковий співробітник наукової лабораторії інформаційного права та інформаційної безпеки Державної наукової установи «Інститут інформації, безпеки і права Національної академії правових наук України», аналізує правові засади оновлення Стратегії інформаційної безпеки у відповідь на російське інформаційне маніпулювання та втручання [275]. Дослідниця пов'язує ефективність правового реагування з точністю визначення загроз і відповідністю інструментів характеру втручання. Цей підхід підтримує висновок про необхідність регулярного уточнення категорій загроз та процедур їх нейтралізації відповідно до зміни інформаційного середовища.

Ірина Лопатченко – кандидат наук з державного управління, Аліна Помаза-Пономаренко – доктор наук з державного управління, старший дослідник, Юрій Батир – кандидат економічних наук, доцент; усі троє представляють Навчально-науково-виробничий центр Національного університету цивільного захисту України у Харкові. У спільній статті вони розглядають державне регулювання інформаційної безпеки в умовах воєнного стану та звертають увагу на правові, організаційні й координаційні складники відповідної політики [276]. Їхня позиція підкреслює значення узгодження повноважень і міжвідомчих процедур

для практичної реалізації нормативних приписів. Зіставлення наведених наукових підходів дає підстави визначити процедурну узгодженість норм і повноважень як центральну умову їх практичної дієвості.

На підставі проведеного аналізу визначаємо чотири взаємопов'язані проблемні позиції політико-правового та організаційного забезпечення. Перша стосується розмежування санкційних, медіарегуляторних і кримінально-правових механізмів, адже нечіткість критеріїв вибору інструменту послаблює передбачуваність рішення. Друга пов'язана з фрагментованим обміном даними, який здатний формувати різні оцінки загрози та ускладнювати синхронізацію рішень. Третю проблемну позицію пов'язуємо з потребою уніфікованих метрик результативності, які дали б змогу зіставляти ефекти різних інструментів. Четверта позиція має комунікаційний характер: послідовне публічне пояснення правових підстав і мети рішення зменшує можливості для його маніпулятивного переосмислення. Разом ці позиції окреслюють напрями, у яких нормативна база має поєднуватися з процедурою виконання та оцінювання.

Європейський вимір формує нормативно-ціннісне середовище, з яким Україна узгоджує власну політику в контексті європейської інтеграції. Комісар Ради Європи з прав людини наголошував на ризиках широкого інтернет-блокування та значенні правової визначеності для захисту свободи вираження [260]. Регламент Ради ЄС щодо RT і Sputnik водночас показав можливість адресного обмеження діяльності визначених суб'єктів, пов'язаних із державною пропагандою Росії [272]. Зіставлення цих підходів дає підстави визначити адресність, пропорційність, обмеженість у часі та можливість перегляду як базові критерії демократично легітимного втручання.

Пріоритети оптимізації визначаємо за критеріями здійсненності, ризику та очікуваного ефекту. На правовому рівні пропонуємо деталізувати процедури застосування обмежень, компетенцію суб'єктів, вимоги до доказової бази, строк дії та порядок перегляду. На організаційному рівні обмін даними доцільно будувати не лише між державними органами, а й із тими групами, яких безпосередньо стосується рішення. Для законодавчих рішень в економічній

сфері це означає залучення профільних парламентських комітетів, представників галузевих об’єднань, промисловців і підприємців до отримання фактичних даних і зворотного зв’язку. У такому розумінні інформаційне забезпечення стратегічних комунікацій починається з якості інформації, на якій ґрунтується рішення, і завершується зрозумілим поясненням його мотивів та наслідків. На інформаційно-технологічному рівні пріоритетом залишаються сумісність даних, фіксація походження доказів і можливість відтворити аналітичний шлях до рішення.

В умовах тривалої російської збройної агресії окремого значення набуває довгострокова стійкість правового режиму та регулярний перегляд тимчасових обмежень. Пропонуємо передбачати для таких заходів визначений строк, критерії перегляду та процедуру припинення після зникнення відповідних безпекових підстав. Регулярний перегляд доцільно пов’язати з оцінюванням результатів, актуальності загрози та пропорційності подальшого застосування заходу. Проведений аналіз дає підстави визначити політико-правову основу безпеки інформаційного простору через поєднання конституційної допустимості обмежень, спеціального законодавства, стратегічних документів, санкційних і медіарегуляторних процедур та організаційно-технологічного захисту. Системна дієвість цих складників залежить від правової визначеності, процедурної відтворюваності й демократичної стійкості. Саме така конфігурація дає змогу державі оперативно протидіяти ворожому впливу, зберігати суспільну довіру та підтримувати відповідність безпекової політики європейським правовим стандартам.

3.2. Основні гуманітарні складники антиукраїнських інформаційно-пропагандистських операцій

Гуманітарний вимір російської агресії спрямований на трансформацію ідентичності, колективної пам’яті та ціннісних орієнтирів українського суспільства й доповнює військово-політичний контроль над територією. Гуманітарна агресія спрямована на руйнування національної та громадянської

ідентичності й послаблення культурної суб'єктності суспільства [277]. У межах дослідження гуманітарну безпеку визначаємо як стан суспільства, за якого зберігаються базові права людини, культурна спадщина та функціонування освіти, культури й соціальної сфери, а відповідна інфраструктура має спроможність протидіяти цілеспрямованому інформаційному та пропагандистському впливу. Гуманітарні загрози російсько-української війни проявляються на глобальному, регіональному й національному рівнях [278].

До основних сфер гуманітарного впливу відносимо мову, культуру, освіту, релігію, історичну пам'ять і символічний простір. У цих сферах Росія намагається змінювати структуру колективних уявлень про минуле, нормалізувати вигідні їй політичні ідентичності та звужувати уявлення про можливі моделі майбутнього. Виходячи з наведених ознак, визначаємо три взаємопов'язані домінанти гуманітарного впливу: доктрину «руського міра», ревізіоністське переозначення історичної пам'яті та культурної спадщини, а також мовно-цифрову інфраструктуру поширення наративів [279].

Доктрина «руського міра» (рос. «русский мир», англ. Russkiy Mir) поєднує уявлення про особливу цивілізацію, засновану на російській мові, культурі й православ'ї, з неоімперським баченням природних кордонів російського політичного впливу. О. Гордійчук, А. Галапсіс і М. Козловець простежують еволюцію доктрини «руського міра» від інструмента культурного впливу до неоімперської ідеології [280]. У межах цієї доктрини заперечення історичної суб'єктності України використовується для легітимації претензій Росії на політичний і культурний контроль [280]. Отже, мовно-культурна близькість перетворюється на аргумент для втручання у внутрішні справи сусідніх держав.

Ревізіоністська робота з історичною пам'яттю та культурною спадщиною виконує функцію зовнішньополітичного й внутрішнього мобілізаційного інструмента. Д. Шульц і К. Джаспарро аналізують використання історії та культурної спадщини Росією в інформаційній війні й формулюють рекомендації для НАТО [281]. Російські кампанії переосмислюють роль СРСР у Другій світовій війні, використовують статус радянських пам'ятників і маркують

опонентів як «неонацистів», делегітимізуючи суверенітет України та країн Балтії [281]. Коли деколонізаційні рішення подаються як «наруга над історією», вони стають приводом для інформаційних атак і делегітимації політики пам'яті. Виходячи з наведеного, об'єктом впливу визначаємо також інтерпретацію ключових історичних подій, довкола яких формується колективна ідентичність.

Цифрово-мовний компонент цієї стратегії забезпечує її щоденну присутність у комунікативних практиках. Євгенія Шишкіна, дослідниця Національного технічного університету «Харківський політехнічний інститут», аналізує інформаційні технології російської пропаганди у 2014–2022 роках [282]. Вона реконструює пропагандистську систему як поєднання масового продукування російськомовного контенту, політичної новомови (newspeak), фабрик тролів, ботомереж і використання ефекту «фільтр-бульбашки» [282]. За умов інформаційної ізоляції такі повідомлення можуть закріплюватися як самоочевидні інтерпретації в окремих сегментах аудиторії [282]. Таким чином, мовна й цифрова інфраструктура забезпечує масштабування гуманітарних наративів і їхнє повсякденне відтворення.

Матеріальний вимір цієї експансії виразно простежується на прикладі Фонду «Русский мир», який у дослідженні Українського інституту та групи MZ Hub описується як центральний інструмент гуманітарного впливу Росії [283]. Формально позиціонуючись як недержавна організація, Фонд фактично контролюється державною владою, фінансується з федерального бюджету й діє у взаємодії з міністерствами та адміністрацією президента [283]. Через мережу культурних центрів, мовних курсів, освітніх і медійних проєктів реалізується модель культурного впливу, прив'язана до реваншистського тлумачення російської цивілізації та лояльності до зовнішньополітичних рішень Кремля [283]. У програмних документах Фонду концепт «руського міра» пов'язується з православ'ям, а Російська православна церква описується як духовне ядро цього простору [283]. Отже, гуманітарна інфраструктура Фонду надає доктрині організаційної форми й забезпечує її присутність за межами Росії.

У дослідженні «Гібридна війна: вплив Російської православної церкви на

українські медіа» (Hybrid War: The Influence of the Russian Orthodox Church on the Ukrainian Media) РПЦ розглянуто як канал трансляції політичних меседжів Кремля мовою традиційних цінностей і захисту віруючих [284]. Через релігійні медіа й публічну комунікацію РПЦ транслює політизовані повідомлення про захист віруючих і особливий статус російського православ'я [284]. На окупованих територіях окупаційна влада нав'язує реєстрацію та підпорядкування релігійних громад структурам, пов'язаним із РПЦ, одночасно обмежуючи діяльність незалежних громад [285]. У межах наведених даних визначаємо цю практику як релігійне переформатування окупованого простору, спрямоване на витіснення громад, незалежних від РПЦ та окупаційної адміністрації. Структури РПЦ використовуються як канали політичного й медійного впливу Росії [284]. Це посилює значення безпекової оцінки їхньої діяльності в Україні.

Релігійне виправдання війни виразно простежується у публічній риториці патріарха Кирила. Архієпископ Борис Ґудзяк, автор експертної публікації Atlantic Council про церковне виправдання російської агресії, характеризує патріарха Кирила як одного з провідних релігійних ідеологів війни проти України, який наділяє агресію метафізичним і релігійним сенсом [286]. Така інтерпретація не лише легітимує насильство в очах частини вірян, а й наділяє його статусом священного обов'язку, що ускладнює будь-які спроби мирного врегулювання. Документовані руйнування культових споруд, викрадення й убивства релігійних діячів та обмеження діяльності громад, незалежних від РПЦ, дають підстави розглядати релігійний примус як складник політики зміни ідентичності [285].

На тлі такого інституційного й ідеологічного оформлення важливо простежити закріплення концепту «руського міра» в сучасному міжнародно-політичному дискурсі. Концепт поєднує мовно-культурний простір, геополітичні претензії та консервативно-релігійну ідеологію, протиставлену ліберальному міжнародному порядку. Александер Меєнберґер, дослідник Університету Санкт-Галлена, простежує історичну еволюцію концепту

«руського міра» [287]. У 1990-х роках концепт тяжів до ідеї культурної спільноти російськомовних. Надалі концепт набув консервативного й православно забарвленого змісту, став інструментом геополітики Росії та почав використовуватися для легітимації її впливу [287]. Таке трактування створює ідеологічну основу для претензій Росії на втручання у справи держав, які вона зараховує до ширшої російської спільноти.

Витоки сучасної версії «руського міра» пов'язуються з інтелектуальними дискусіями другої половини 1990-х років у середовищі російських політтехнологів та публічних інтелектуалів, які шукали спосіб компенсувати наслідки розпаду СРСР. Саме тоді оформлюється уявлення про «другу Росію» поза державним кордоном – розгалужену мережу російськомовних спільнот, що мисляться як ресурс відновлення могутності держави та гуманітарна основа для нової політики «збирання» простору.

Фундаментальне значення для формування концептуального підґрунтя сучасної російської експансії мали розробки Петра Щедровицького – одного з провідних інтелектуальних лідерів Московського методологічного гуртка та спадкоємця методологічної школи Г. Щедровицького. Саме він на межі 1990–2000-х років запропонував розглядати російськомовні спільноти за кордоном не як традиційну діаспору, а як «спільноту співвітчизників», що за своїм масштабом є співмірною з населенням самої РФ і становить ключовий ресурс зовнішньополітичного впливу. Ця концепція «Російського світу» як глобальної мережевої структури стала теоретичним базисом для подальшої інструменталізації гуманітарної сфери у воєнних цілях. Важливо констатувати, що ключові фігури, відповідальні за підготовку та реалізацію агресії проти України, є безпосередніми вихованцями методологічних студій П. Щедровицького, де відпрацьовувалися технології програмування реальності та маніпулятивного управління великими соціальними системами. Зокрема, Сергій Кірієнко (перший заступник керівника Адміністрації Президента РФ), якого вважають одним із головних архітекторів доктрини інформаційно-смислової агресії та ідеологічного виправдання окупації українських територій, послідовно

впроваджує методологічні принципи у практику державного управління та пропаганди. Разом із ним до кола ідеологів, що трансформували теорію «методологів» у прикладну зброю гібридної війни, належать такі високопоставлені функціонери в російській владі, як Антон Вайно та Владислав Сурков, чиї стратегії базуються на алгоритмах конструювання штучних ідентичностей та управлінні конфліктами через інформаційне домінування. Ці інтелектуальні конструкції сформували одну з ідеологічних передумов претензій Росії на культурний і політичний контроль над сусідніми державами.

У публічній політиці подальша інституціоналізація концепту відбувалася через законодавчі та організаційні механізми. Юріє Ротарі, автор дослідження про динамічне використання концепту «руського міра» у зовнішній політиці РФ, простежує його інституціоналізацію [288]. Ухвалення Федерального закону РФ «Про державну політику Російської Федерації щодо співвітчизників за кордоном» 1999 року стало відправною точкою для перетворення «руського міра» з культурної метафори на інструмент зовнішньої політики [288]. У публічній риториці Володимира Путіна належність до «руського міра» пов’язувалася з проголошеною духовною та культурною самоідентифікацією [288]. Приналежність до «руського міра» пов’язується передусім із проголошеною духовною й культурною самоідентифікацією, що виходить за межі громадянства.

У 2007 році було створено Фонд «Русский мир» як інституційний механізм поширення концепту [288]. Через мережу культурних центрів, мовних курсів та освітніх проєктів Фонд розширював російську гуманітарну присутність за кордоном [283]. У звіті наведено вислів виконавчого директора Фонду Володимира Кочина, який пов’язує поширення російської мови з політичною присутністю Росії [283]. Після початку повномасштабної агресії концепт отримав подальше офіційне закріплення в Концепції зовнішньої політики РФ 2023 року [288]. Отже, «руський мір» пройшов шлях від інтелектуального конструкту до офіційної ідеологеми, підкріпленої гуманітарними, церковними й квазідипломатичними інституціями.

Структура гуманітарної агресії Росії проявляється в доктринальних та інституційних рішеннях і у виразній адресності цільових груп. У межах дослідження до основних цільових груп відносимо мешканців тимчасово окупованих територій, внутрішньо переміщених осіб, дітей і молодь, релігійні громади, національні меншини та українців, які перебувають за кордоном. Спільним для цих груп є досвід розриву усталених соціальних зв'язків, часткової втрати звичних каналів взаємодії з українською державою й вимушене перенесення значної частини життя в цифрові простори – від месенджерів і локальних чатів до сегментованих спільнот у соціальних мережах. Виходячи з цих умов, можемо припустити підвищену сприйнятливість окремих груп до повідомлень, що апелюють до безпеки, турботи й відновлення справедливості. Громадянська мережа ОПОРА – українська громадська організація, що проводить дослідження медіаспоживання та соціальної згуртованості, – виявила істотні вікові й соціально-демографічні відмінності у використанні цифрових каналів [289]. Уразливість соціальних зв'язків і бар'єри згуртованості для окремих груп зафіксовано в окремому дослідженні ОПОРИ [290].

Найбільш концентровано логіка адресної роботи проявляється на тимчасово окупованих територіях, де поряд із військовим контролем вибудовується режим цифрового підкорення: перехоплення телерадіомовлення, переведення мобільного зв'язку на російських операторів, обмеження доступу до українських онлайн-ресурсів і паралельне розгортання мережі формально регіональних медіа та Telegram-каналів, які де-факто координуються з російських центрів управління. Atlantic Council – аналітичний центр у Вашингтоні – виявив мережу з 3634 автоматизованих акаунтів, що поширювали проросійські повідомлення в Telegram-каналах, орієнтованих на населення окупованих територій [291]. Такий інформаційний режим здатний нормалізувати образ окупаційної адміністрації як головного постачальника безпеки, соціальної допомоги й відбудови. Отже, цифрова інфраструктура окупації поєднує обмеження доступу до українського інформаційного простору з імітацією локальної суспільної підтримки.

Діти та підлітки в цій конфігурації становлять окрему зону вразливості,

оскільки для них змінюється інформаційний фон і базові інститути соціалізації. Освітній процес на окупованих територіях цілеспрямовано вбудовується в логіку «руського міра»: перехід шкіл на російські стандарти, запровадження єдиних підручників історії, спецкурсів на кшталт «історії краю» чи «духовної і моральної культури Росії» формує для молодшого покоління картину світу, в якій українська державність виглядає випадковою, а російська присутність – природною й історично виправданою. Центр громадянської освіти «Альменда» – українська неурядова організація, що документує порушення прав дітей на тимчасово окупованих територіях, – у звіті про освітню політику окупантів та мережу так званих оздоровчих таборів демонструє, що навчальні плани, позакласні заходи та організовані поїздки до РФ або на інші окуповані території утворюють єдиний цикл [292]. Залежність дітей-сиріт, дітей з інвалідністю та дітей із сімей у складних життєвих обставинах від опікунських інституцій посилює ризик тривалого індоктринаційного впливу. Таким чином, вплив на дітей спрямовується на довготривале закріплення нових мовних, символічних і політичних орієнтирів.

На контрольованій Україною території молоді люди опиняються під іншим типом тиску: їхня повсякденність не визначається окупаційною владою, однак значна частина новинного споживання перемістилася до цифрових платформ. Серед молодших респондентів соціальні мережі та месенджери посідають провідне місце в отриманні новин, хоча традиційні медіа зберігають окрему роль [289]. Висока частка новинного споживання через соціальні мережі підвищує ризик поширення у блогерських і розважальних форматах повідомлень, що експлуатують втому від війни, недовіру та невизначеність майбутнього. Отже, стійкість молоді залежить від поєднання доступу до достовірної інформації з розвитком навичок критичної оцінки цифрового контенту.

Внутрішньо переміщені особи й ширше – люди, що втратили житло, роботу й локальні спільноти, – опиняються в подібній ситуації з іншим набором ризиків. Якісне дослідження Громадянської мережі ОПОРА, побудоване на 19 експертних інтерв’ю та 18 фокус-групах, виявило бар’єри соціальної

згуртованості для п’яти досліджуваних груп [290]. Обмежені канали участі та локалізований інформаційний обмін можуть підвищувати сприйнятливість ВПО до наративів про несправедливий розподіл ресурсів і другорядність окремих регіонів. Тому комунікація з цією групою має поєднувати доступ до інформації з реальними механізмами участі у прийнятті рішень.

Релігійні громади стають ще одним об’єктом системного впливу, оскільки в умовах війни саме вони часто виконують роль інфраструктури підтримки, взаємодопомоги та сенсового орієнтира. У звіті «Віра під російським терором» (Faith Under Russian Terror), підготовленому Mission Eurasia та Інститутом релігійної свободи, задокументовано переслідування релігійних громад на окупованих територіях [285]. Звіт документує примусове припинення або перереєстрацію діяльності та тиск на релігійні громади, незалежні від РПЦ й окупаційної адміністрації [285]. У такій конфігурації доступ до богослужіння, пастирської опіки й базових гуманітарних послуг починає залежати від прийняття наративів, які транслюють «канонічні» церковні структури й які збігаються з політичними завданнями Росії – від заперечення української суб’єктності до нормалізації окупаційного режиму. Отже, контроль над релігійним середовищем використовується для зміни інституційної та символічної структури окупованих громад.

Українці, які вимушено опинилися за кордоном, стають адресатами іншого типу впливу. Учасники фокус-груп і опитані експерти описували ізоляцію, страх конфлікту, втрату соціального капіталу та бар’єри участі українців за кордоном у суспільному житті України [290]. Опитані експерти й учасники фокус-груп критично оцінювали частину державних підходів до взаємодії з українцями за кордоном [290]. Соціальна дистанція може бути використана для поширення наративів відчуження та послаблення зв’язку цієї групи з українським політичним простором. Тому підтримання політичного й культурного зв’язку з українцями за кордоном визначаємо окремим напрямом гуманітарної стійкості.

Прийняття Стратегії інформаційної безпеки засвідчило інституціоналізацію частини гуманітарної відповіді України на російський інформаційний вплив

[257]. Стратегія інформаційної безпеки визначає завдання у сферах медіаграмотності, підтримки української мови й культури та зміцнення національної ідентичності [257]. У сукупності ці напрями формують гуманітарний складник безпекової політики. Відповідь на російські інформаційні операції поєднує обмеження ворожих ресурсів і спростування дезінформації з відтворенням українських цінностей в освітніх, культурних, медійних та меморіальних практиках.

У перспективі повоєнного перехідного періоду В. Філатов, дослідник інформаційного права Університету митної справи та фінансів, пов’язує розвиток інформаційного законодавства з чотирма напрямами перехідного правосуддя: встановленням істини, відповідальністю, відшкодуванням шкоди та інституційними реформами [293]. Такий підхід розширює часовий горизонт гуманітарної політики від реагування на поточні операції до відновлення інституційної довіри та суспільної цілісності після війни.

Аналітичний звіт «Український медіаландшафт 2022–2024» (Ukrainian Media Landscape 2022–2024) простежує зміни українського медіаландшафту під впливом повномасштабної війни, зокрема трансформацію редакційних практик, регіональних медіа та цифрових каналів [294]. Соціальні мережі й месенджери посідають важливе місце в новинному споживанні українців, особливо серед молодших вікових груп [289]. Detector Media – українська громадська організація, що досліджує медіа та медіаграмотність, – у п’ятій хвилі Індексу медіаграмотності порівнює практики різних груп населення [295]. На підставі виявлених відмінностей пропонуємо диференціювати освітні й комунікаційні програми за віком, рівнем освіти та медіапрактиками аудиторій.

Формування єдиного гуманітарного простору відбувається в умовах фрагментованого медіаполя. Звіт про інформаційне середовище України показує співіснування традиційних медіа з нетрадиційними каналами, блогерами й мережевими спільнотами, де анонімність ускладнює перевірку походження інформації [296]. Нетрадиційні канали створюють додаткові можливості для поширення деструктивних повідомлень під виглядом особистої думки або

альтернативного погляду. Тому пропонуємо спрямовувати інструменти гуманітарної протидії також у середовища, де формуються повсякденні інтерпретації війни, окупації, втрат і майбутнього.

Важливою складовою гуманітарної стійкості є діяльність громадянського суспільства, спрямована на документування російських злочинів, пояснення механізмів маніпуляції та підтримку локальних інформаційних і освітніх ініціатив. Політика пам'яті й культурна дипломатія підтримують українську інтерпретацію минулого та сучасності для внутрішньої й зовнішньої аудиторій. Разом ці напрями доповнюють державну політику горизонтальними практиками солідарності та суспільної самоорганізації.

Гуманітарна відповідь, спрямована всередину країни, доповнюється інфраструктурою міжнародного партнерства. У спільному звіті Detector Media, Kosciuszko Institute та Civic Resilience Initiative, підготовленому за підтримки Open Information Partnership, порівняно підходи України, Польщі й Литви до протидії дезінформації [297]. Звіт визначає спільні складники стійкості: усвідомлення загрози, багатовимірний підхід, міжсекторальну взаємодію, незалежні медіа та медіаграмотність [297]. Партнерські рамки з Польщею, Литвою та іншими державами регіону охоплюють регуляторні, культурні, освітні й комунікаційні рішення, що зміцнюють гуманітарний вимір безпеки.

Отже, гуманітарна складова російської агресії поєднує доктрину «руського міра», ревізію історичної пам'яті, мовно-цифрову інфраструктуру та адресний вплив на групи, чия повсякденність порушена війною. Взаємодія цих елементів забезпечує тривале відтворення потрібних Росії інтерпретацій ідентичності, минулого й політичного майбутнього. Виходячи з проведеного аналізу, визначаємо адресність та інституційну вбудованість ключовими ознаками гуманітарних інформаційно-пропагандистських операцій. Виявлені механізми впливу водночас окреслюють напрями державної, суспільної та міжнародної протидії, які конкретизуються в наступному підрозділі.

3.3. Основні інструменти російської гуманітарної агресії проти України та протидія їхньому впливу на суспільну свідомість і поведінку

Доктринальні засади «руського міра» та ревізіоністські концепції історичної пам’яті задають ідеологічні вектори атаки, а інструментарій забезпечує їх переведення у практики впливу. Інструменти гуманітарної агресії визначаємо як сукупність цифрових, медійних, організаційних, символічних і примусових практик, спрямованих на зміну ідентичності, пам’яті, довіри та поведінки цільових аудиторій. Ворожий інструментарій функціонує як взаємопов’язана екосистема тиску, у якій окремі засоби підсилюють один одного й забезпечують тривалу присутність агресивних наративів у повсякденних комунікаціях.

Ця екосистема охоплює когнітивні вразливості користувачів у глобальному цифровому просторі та екзистенційні потреби людей у зоні бойових дій і на тимчасово окупованих територіях. Росія поєднує штучно сконструйований інформаційний шум із нав’язуванням окупаційних адміністративних і комунікаційних практик. На тимчасово окупованих територіях така логіка виявляється у перехопленні телерадіомовлення, переведенні мобільного зв’язку на російських операторів, обмеженні доступу до українських онлайн-ресурсів і розгортанні формально регіональних медіа та Telegram-каналів.

Цифрово-комунікаційний компонент забезпечує щоденну присутність російських наративів через масове продукування російськомовного контенту, політичну новомову (newspeak), мережі тролів і ботів та ефект інформаційної бульбашки. Поєднання цих практик надає координованій кампанії вигляду природного суспільного резонансу. У локальних чатах і спільнотах автоматизовані акаунти формують видимість повсякденного консенсусу на користь окупаційного режиму та витісняють альтернативні джерела інформації.

У частині сучасних бот-мереж кількісний спам доповнюється інформаційним затопленням і варіативним генеруванням повідомлень. Координовані проросійські мережі акаунтів поряд із переконуванням використовують перевантаження інформаційного середовища та імітацію масової підтримки. Надмірна кількість штучно сформованих позицій,

замаскованих під голоси реальних громадян, послаблює здатність аудиторії оцінювати достовірність інформації, підвищуючи ризик апатії та поширеної недовіри до джерел.

Розширення можливостей генеративного штучного інтелекту та великих мовних моделей підвищило варіативність автоматизованих повідомлень і зменшило ефективність детекції, заснованої лише на пошуку повних текстових збігів. Автоматизовані акаунти можуть підтримувати правдоподібну історію активності, чергувати політичні й нейтральні дописи та адаптувати час публікацій до цільового регіону. У звіті про еволюцію Operation Overload ці практики розглянуто як частину ускладнення російської цифрової інфраструктури впливу [298].

Найбільш репрезентативний приклад такої цифрової окупації подано у спільному дослідженні OpenMinds і Digital Forensic Research Lab Атлантичної ради за липень 2025 року [291]. Дослідники ідентифікували 3 634 автоматизовані акаунти, активність яких була зосереджена на тимчасово окупованих територіях України. Характер роботи мережі створював ефект локальної підтримки окупаційної влади та видимість поширеності проросійських позицій [291].

Механіка операції передбачала локалізацію повідомлень за допомогою топонімів, побутових тем і мовних маркерів цільових громад. Українські позиції витіснялися масовим потоком координованих коментарів, частина яких мала стилістичні ознаки автоматизованого генерування [291]. У результаті формувалися контрольовані локальні інформаційні середовища з переважанням штучно посилених проросійських оцінок.

Паралельно бот-мережі взаємодіють із псевдоновинними ресурсами. Французька служба VIGINUM у лютому 2024 року описала мережу Portal Kombat, що складалася щонайменше зі 193 сайтів, які автоматизовано збирали й поширювали проросійські матеріали, імітуючи локальні новинні ресурси [119]. У межах запропонованої аналітичної реконструкції бот-акаунти та псевдоновинні сайти можуть утворювати цикл взаємного цитування, який підсилює видимість суспільної підтримки. Домінування однотипних коментарів

створює уявлення про переважання певної позиції та підвищує ризик самоцензури опонентів. Отже, бот-мережі функціонують як інструмент масштабного маніпулювання видимістю суспільних позицій у цифровому середовищі; їхній вплив спрямовується на зміну переконань, послаблення суб'єктності та зниження готовності до опору.

Одним із комплексних інструментів гуманітарної агресії є спеціальні інформаційні операції, які поєднують цифрові, психологічні та організаційні засоби впливу. Окремі операції можуть мати короткостроковий тактичний характер із чітко визначеними часовими межами та цілями: формування емоційного фону перед дипломатичними переговорами, дискредитація міжнародної допомоги або маніпулятивна підготовка аудиторії до певної політичної події. Частина СІО розгортається як тривалі процеси з циклічною зміною інтенсивності, каналів і зовнішньої форми.

У межах авторського узагальнення розглянутих кейсів виокремлюємо такі стратегічні цілі російських СІО, що зберігаються протягом усього періоду російської агресії проти України:

1. Дестабілізація і деморалізація населення України, насамперед у громадах, наближених до зони бойових дій, через поширення панічних настроїв, незахищеності та невизначеності.
2. Руйнування національної єдності через загострення міжетнічних, міжконфесійних, мовних і регіональних суперечностей.
3. Зниження довіри до державних інституцій і політичного керівництва через маніпулятивне використання теми корупції, перебільшення її масштабів і представлення окремих випадків як універсальної характеристики держави, а також через провокування протестних настроїв і закликів до зміни державного керівництва.
4. Дискредитація військового керівництва та підрив довіри до командування Сил оборони України через дезінформацію про втрати, сумніви у досяжності воєнних цілей і нав'язування переговорів на умовах територіальних поступок.

5. Систематичне поширення закликів і практичних порад щодо уникнення мобілізації.
6. Формування очікувань неминучого економічного занепаду України.
7. Формування зневіри в тривалості міжнародної підтримки України.

Наведені напрями показують, що операційна логіка СІО спрямована на послаблення стійкості держави через взаємопов'язаний вплив на довіру, мотивацію й поведінку. Кристофер Пол і Майкл Швілле розглядають еволюцію інформаційних сил через аналогію з інституціоналізацією сил спеціальних операцій [117]. У межах нашого аналізу кінцеву результативність СІО доцільно оцінювати за змінами установок і поведінки, доповнюючи ці показники даними про охоплення та інтенсивність поширення.

Telegram і TikTok стали важливими каналами поширення проросійських наративів в українському інформаційному просторі. Telegram забезпечує мережеве поширення через анонімні канали та пов'язані спільноти, тоді як TikTok підсилює короткий відеоконтент через алгоритмічні рекомендації. Після початку повномасштабного вторгнення ці практики стали помітною частиною російських інформаційних операцій. Вибіркові приклади дозволяють простежити їхню прикладну організацію.

1. Створення фейкових каналів, що імітують сторінки українських військових підрозділів, військових керівників, громадських і волонтерських організацій.
2. Розгортання псевдоукраїнських новинних каналів у Telegram для просування маніпулятивних наративів і дезінформації. У публікації автора, оприлюдненій за матеріалами конференції 12–13 грудня 2023 року, наведено такі показники аудиторії: Telegram-канал «Легитимный» – 1,073 млн підписників, канал Анатолія Шарія – 1,178 млн, канал Діани Панченко – 0,229 млн [299].
3. Просування каналів проросійських авторів українського походження, які позиціонують власний контент як об'єктивне висвітлення подій і використовують сформовану раніше українську аудиторію.

4. Клонування у TikTok акаунтів українських військовослужбовців і наповнення їх відеороликами, націленими на загострення суперечностей між бійцями та командирами й між різними підрозділами Сил оборони України.
5. Масове коментування та підтримка проросійських ресурсів за допомогою ботів. Показовим прикладом організаційного оформлення такого середовища є Telegram-канал «Цифровая Армия России», який у власному описі закликає долучатися до «цифрового спротиву»; існування ресурсу перевірено 5 серпня 2026 року [300].

Спеціальні інформаційні операції можуть мати внутрішній, зовнішній або окупаційний вектор. У багатьох випадках вони узгоджуються зі спільним стратегічним наративом і оперативним задумом. Кінцева мета CIO полягає в управлінні установками та поведінковими реакціями цільових аудиторій. Цю операційну логіку простежимо на прикладах кампанії «Doppelgänger» і російської кампанії проти мобілізації в Україні.

Показовим прикладом технологічно складної транскордонної операції стала кампанія «Doppelgänger». Її значення визначають масштаб охоплення та застосування цифрової мімікрії, спрямованої на підрив процедур верифікації інформації. Ознаки активності мережі простежуються щонайменше з травня 2022 року; у вересні 2022 року EU DisinfoLab оприлюднила результати її викриття [301]. Початкова механіка ґрунтувалася на реєстрації візуально схожих доменів і відтворенні дизайну відомих медіа. У 2023 році французька служба VIGINUM, що діє при Генеральному секретаріаті з питань оборони та національної безпеки, описала технічні характеристики кампанії RRN і пов’язаних мереж [302]. Подальша еволюція операції охопила ширше коло країн і поєднала клоновані ресурси, рекламну інфраструктуру, мережі акаунтів та адаптований контент. У звіті Психологічної оборонної агенції Швеції 2025 року цей розвиток проаналізовано як розширення спроможностей Social Design Agency за межі початкової моделі Doppelgänger [303].

Окремим прикладом гуманітарного впливу у Франції є кампанія Operation

Overload. У її межах проросійські актори масово надсилали редакціям і фактчекерам сфабриковані матеріали, змушуючи їх витрачати ресурси на перевірку [304]. Частина підроблених матеріалів пов'язувала поширення клопів з українськими біженцями. Французький уряд публічно пов'язував штучне роздмухування цієї теми з російською дезінформаційною активністю [305]. У межах наведеного кейсу виокремлюємо три взаємопов'язані цілі:

1. Дегуманізація українців у свідомості європейської аудиторії через асоціативний ряд «біженець – джерело небезпеки, хвороб і хаосу».
2. Створення інформаційних передумов для посилення скепсису щодо підтримки України у французькому суспільстві.
3. Дискредитація Франції як господаря міжнародного заходу в ширшому контексті інформаційних атак напередодні Олімпійських ігор 2024 року [304].

На зовнішньому рівні кампанія використовувала локальні соціальні вразливості для посилення суперечностей усередині європейських суспільств. Маніпуляції навколо міграції, бюджетних витрат і суспільної безпеки створювали фон, на якому підтримка України подавалася як джерело внутрішніх проблем.

В українському інформаційному просторі такі матеріали можуть посилювати відчуття міжнародної ізоляції та зневіру у стійкості зовнішньої підтримки. Імітація західних медіа надає деструктивним тезам видимість зовнішнього підтвердження та підриває довіру до обраного державою курсу.

У 2025 році кампанія Operation Overload продовжила практику цілеспрямованого впливу на медіа. Зловмисники перевантажували редакції та фактчекінгові організації запитами на перевірку сфабрикованого контенту, перетворюючи процедуру верифікації на об'єкт атаки [298]. У кампанії Doppelgänger операційна логіка спиралася на три взаємопов'язані механізми:

1. Інституційна мімікрія. Мережа відтворювала дизайн медіа й окремих офіційних ресурсів, використовуючи їхню репутацію для підвищення правдоподібності повідомлень [306].

2. Гібридна інфраструктура. За даними Meta, витрати на одну з рекламних хвиль перевищили 100 000 доларів [307]. Масштаб фінансування сам по собі не визначає його державне походження.
3. Адаптивний таргетинг. Наративи пристосовувалися до локальних соціально-економічних і політичних суперечностей цільових країн.

У вересні 2024 року Міністерство юстиції США оголосило про судові заходи щодо вилучення 32 доменів, пов'язаних із російськими операціями впливу [306]. Кейс підтверджує, що протидія потребує роботи з доменами, рекламною інфраструктурою та мережею розповсюдження. Цільовий гуманітарний ефект кампанії був спрямований на послаблення довіри до медіа та процедур суспільної верифікації інформації. Масштаб і технологічна складність операції водночас характеризують насамперед її спроможність підтримувати інформаційний тиск і самі по собі не засвідчують досягнення відповідних змін у суспільних установках.

Застосування запропонованої моделі життєвого циклу CIO до кампанії «Doppelgänger» дає змогу простежити, як окремі елементи операції складалися в послідовний механізм інформаційного впливу. Вихідною точкою стало використання локальних суспільних суперечностей і тем, здатних послаблювати підтримку України в європейських державах [302]. На цій основі формувалися повідомлення про політичні, економічні та безпекові наслідки такої підтримки [302]. Їх поширення забезпечувалося через клонування відомих медіа, візуально подібні домени та цифрові платформи [301]. Подальший розвиток кампанії засвідчив розширення її інструментарію, мережевої інфраструктури та способів адаптації контенту до різних цільових середовищ [303]. Для порівняння, в окремій кампанії Operation Overload об'єктом впливу стали редакції та фактчекінгові організації, ресурси яких перевантажувалися запитами на перевірку сфабрикованих матеріалів [298]. У проаналізованій динаміці Doppelgänger простежується зв'язок між початковим визначенням уразливостей аудиторії, конструюванням відповідних наративів, інфраструктурою їх поширення та подальшою адаптацією операції. Застосування моделі до цього

кейсу дає змогу розмежувати операційну спроможність СІО, її цільовий когнітивний вплив та емпірично підтверджені політичні наслідки.

Кампанія проти мобілізації є однією з найбільш тривалих російських інформаційних кампаній, спрямованих на внутрішню стійкість України. Для аналітичного впорядкування матеріалу пропонуємо умовно виділити три етапи, кожен із яких відображає зміну провідних наративів і каналів.

Перший етап – примусова деморалізація від лютого 2022 року до початку 2023 року. Основний наратив поєднував образ неминучої поразки із закликами складати зброю та повідомленнями про відсутність навчання, спорядження й належного командування. Високий рівень суспільної мобілізації обмежив ефективність цієї моделі й стимулював перехід до персоналізованіших емоційних сюжетів.

Другий етап – демонізація територіальних центрів комплектування у 2023–2024 роках. Окремі конфліктні відео масштабувалися й подавалися як універсальна характеристика мобілізаційної системи. Центр протидії дезінформації зафіксував поширення наративів про соціальну несправедливість мобілізації, наратив про нібито намір влади воювати до останнього українця та відсутність майбутнього в України [308].

Третій етап – юридичний і мережевий саботаж у 2024–2025 роках. У медіапросторі діяли блогери й псевдоюридичні коментатори, які повторювали подібні аргументи про нібито нелегітимність мобілізаційних процедур [309]. Псевдоправові конструкції надавали ухиленню вигляду захисту прав і переводили страх перед службою в площину недовіри до держави.

Окремі фейки адаптувалися до регіонального контексту. Центр протидії дезінформації 3 липня 2025 року спростував повідомлення про нібито мобілізацію громадян Молдови в Одесі та області [310]. Цей кейс підтверджує локалізацію повідомлень, але сам по собі не доводить використання штучного інтелекту.

Операційна логіка кампанії спирається на три психосоціальні тригери: відчуття соціальної несправедливості, стигматизацію військової служби та

делегітимізацію держави. Перший тригер протиставляє різні соціальні групи; другий змінює образ військовослужбовця із захисника на жертву обставин; третій подає законні державні процедури як прояв диктатури. Їх поєднання створює умови для залучення неусвідомлених ретрансляторів ворожих наративів.

У межах наведених матеріалів кампанію проти мобілізації визначаємо як операцію, що безпосередньо спрямована на поведінковий результат – зниження готовності громадян виконувати оборонний обов'язок і послаблення суспільної підтримки комплектування Сил оборони. Її стійкість пов'язана з експлуатацією екзистенційного страху, реальних конфліктів і недовіри до інституцій. Отже, інформаційний вплив здатний уражати державний механізм через ерозію соціального контракту.

У розглянутих кейсах операційна логіка агресора поєднує технологічну мімікрію, рефлексивне управління й експлуатацію алгоритмічних вразливостей цифрових платформ. Особливу загрозу становить адаптивна трансформація СІО – від створення окремих фейків до соціальної інженерії, алгоритмічного підсилення та залучення неусвідомлених ретрансляторів. Демократична відкритість і доступність цифрової комунікації в таких умовах перетворюються на канали впливу проти держави та суспільства.

Для аналітичного опису цілеспрямованого руйнування та переозначення символічного простору виокремлюємо три взаємопов'язані напрями: символічне усунення, символічне заміщення та культурну апропріацію. Через візуальне середовище окупаційна влада прагне змінити повсякденні маркери належності, представити російську присутність як природну й витіснити український культурний код.

Перший напрям – символічне усунення – охоплює демонтаж українських пам'ятників, меморіальних дощок, державних символів і топонімів. У Маріуполі окупанти демонтували пам'ятник жертвам Голодомору, що є конкретним прикладом усунення українських меморіальних маркерів [311]. Заміна українських назв і вивісок, повернення радянської топоніміки та вилучення

української мови з публічного простору формують нову систему щоденних символічних орієнтирів.

Друга стадія – символічна окупація – передбачає агресивне насичення простору маркерами російської імперської ідентичності. Це встановлення пам'ятників постатям, які часто не мають органічного стосунку до конкретної місцевості, але виконують роль «ідеологічних стовпів» – Олександру Невському, Пушкіну, Сталіну [312]. Використання мілітарної символіки «Z» і «V» у монументальному мистецтві, графіті та оформленні будівель перетворює публічний простір на постійне нагадування про присутність окупаційної влади.

Третій напрям – культурна апропріація та реінтерпретація – полягає у привласненні української спадщини та її включенні до російського історичного міфу. Офіс Генерального прокурора повідомив про вивезення окупантами понад 10 тисяч експонатів із музею в Херсоні [313]. Фізичне вилучення колекцій поєднується з переозначенням пам'яток і викресленням українського періоду їхньої історії, що позбавляє громади матеріальних джерел пам'яті.

Гуманітарний вплив руйнації символічного простору проявляється в ерозії колективної пам'яті, відчуженні людини від власного дому та візуальній легітимізації окупації. Зміна топонімічного й архітектурного ландшафту створює відчуття втрати звичного середовища, а постійна присутність російських символів нормалізує владу окупанта. ЮНЕСКО верифікує пошкодження культурних об'єктів України, що дає документальну основу для оцінювання масштабів втрат [314]. У сукупності меморіальна агресія спрямована на позбавлення українців права на власну історію та перетворення тимчасово окупованого простору на середовище імперської ідеології.

Гуманітарна складова антиукраїнських інформаційно-пропагандистських операцій є структурним елементом сучасної війни. Українська держава й суспільство поступово сформували контур протидії, закріплений у Стратегії інформаційної безпеки та документах із національної стійкості. Водночас між нормативними цілями й практичними спроможностями зберігаються системні розриви, які визначають подальші напрями політики.

На нормативно-інституційному рівні гуманітарний захист має поєднувати обмеження ворожого контенту з довгостроковими завданнями відновлення символічного простору, підтримки локальних спільнот, роботи з травмою та формування інклюзивних наративів. Інформаційна політика в перехідний період повинна підтримувати документування злочинів, пошук правди, меморіалізацію та інституційні реформи, оскільки саме ці процедури формують основу суспільної довіри після тривалого насильства.

У секторі традиційних медіа відбулися помітні структурні зміни. Дослідження «Ukrainian Media Landscape 2022–2024» описує трансформацію телевізійного й радіосередовища, зменшення присутності відкрито проросійських майданчиків і посилення ролі суспільного мовника [294]. Ці зміни підвищують контрольованість видимого сегмента інформаційного простору, але не охоплюють усі канали споживання контенту.

Цифрове середовище зберігає асиметричні можливості для операцій впливу. Звіт «Research on Information Environment: Ukraine» показує значну роль Telegram, месенджерів і координованої активності в українському інформаційному середовищі [296]. Саме тут поєднуються висока емоційна насиченість, швидке мережеве поширення та обмежена прозорість відповідальності. Гуманітарна протидія потребує постійної присутності у цих середовищах і створення привабливих альтернативних майданчиків для різних аудиторій.

Окремим викликом є нерівномірність гуманітарного захисту різних груп і територій. Мешканці прифронтових громад, внутрішньо переміщені особи, українці за кордоном і релігійні громади на окупованих територіях мають різний доступ до якісного контенту, освітніх і культурних програм, психологічної підтримки та суспільного діалогу. Ефективність політики доцільно оцінювати за змінами інформаційних практик, охопленням вразливих груп, довірою до якісних медіа та здатністю гуманітарних інституцій відновлювати відчуття гідності й перспективи майбутнього.

Перспективні напрями посилення гуманітарної безпеки випливають із цих

розривів. На нормативному рівні пріоритетом є узгодження інформаційної політики із завданнями перехідного правосуддя та повоєнної реконструкції. На локальному рівні необхідні сталі програми документування досвіду окупації, депортацій і спротиву, підтримка культурних інституцій і повернення громадам права формулювати власні наративи.

В інформаційному середовищі першочергового значення набуває системна робота в месенджерах, напівформальних спільнотах і мережах лідерів думок. Технічне маркування та блокування ворожого контенту має доповнюватися створенням альтернативних платформ, де досвід війни й окупації артикулюється голосами самих громад. Такий підхід перетворює гуманітарну протидію з реакції на окремі фейки на довготривалу політику підтримання ідентичності та суспільної згуртованості.

У міжнародному вимірі важливим напрямом є інституціоналізація українського досвіду в регіональних форматах. У звіті «Resilience to Disinformation: Lublin Triangle Perspective» Люблінський трикутник розглянуто як простір кооперації України, Польщі та Литви у протидії дезінформації й зміцненні суспільної стійкості [297]. Така взаємодія дозволяє поєднувати практичний досвід України з демократичними стандартами захисту прав людини та закріплювати українське розуміння російської агресії у ширшому європейському дискурсі.

Таким чином, гуманітарний вимір інформаційної безпеки є одним із центральних складників безпекової системи України. Поєднання правових рамок, інституційних механізмів, локальних практик, цифрової присутності та міжнародної кооперації визначає здатність суспільства витримувати поточний тиск російських інформаційно-пропагандистських операцій і формувати передумови стійкого гуманітарного розвитку після завершення війни.

3.4. Перспективи впровадження технологій штучного інтелекту в систему стратегічних комунікацій та інформаційного захисту держави

На сучасному етапі розвитку цифрового інформаційного середовища зростає потреба в переосмисленні принципів державної комунікації. Цифрові технології дедалі активніше визначають добір, структурування й поширення змістів у системі стратегічних комунікацій (Strategic Communications, StratCom). Упровадження штучного інтелекту посилює динамічність цього середовища, оскільки алгоритмічні системи здатні автоматизувати аналіз великих масивів даних, адаптацію повідомлень і розподіл контенту відповідно до заданих цілей та параметрів. Класична лінійна модель «адресант – повідомлення – адресат» недостатньо відображає багаторівневу й алгоритмічно опосередковану взаємодію в цифровому середовищі. Видимість повідомлення залежить від архітектури платформи, параметрів ранжування, поведінкових сигналів користувачів і способів модерації контенту. Унаслідок цього стратегічні комунікації охоплюють роботу з повідомленнями, даними, каналами поширення та умовами, за яких аудиторія отримує й інтерпретує інформацію. Алгоритми соціальних мереж і пошукових систем істотно впливають на видимість, послідовність та пріоритетність контенту для конкретного користувача. У сучасному інструментарії гуманітарної агресії ШІ посилює персоналізацію, масштабування та замикання користувачів в інформаційних екосистемах, орієнтованих на вплив на сприйняття й поведінку.

Традиційні моделі державної комунікації значною мірою спиралися на контроль над основними каналами поширення інформації та централізоване формування повідомлень. Цифрове середовище дедалі більше фрагментується між платформами, спільнотами й персоналізованими потоками контенту, тому однакове повідомлення отримує різну видимість і значення для окремих сегментів аудиторії. AJP-10 виходить із необхідності системного розуміння

складного й динамічного інформаційного середовища та узгодження комунікаційних спроможностей для досягнення стратегічних цілей [85]. У цьому документі стратегічні комунікації розглядаються як скоординоване застосування комунікаційних спроможностей, дій і повідомлень на основі розуміння інформаційного середовища [85]. Стратегія інформаційної безпеки України визначає стратегічні комунікації як скоординоване використання комунікаційних спроможностей держави для просування її цілей [257]. ШІ розширює можливості прогнозного аналізу аудиторій, тестування варіантів повідомлень і виявлення змін у структурі інформаційних потоків; використання цих можливостей в операціях впливу потребує окремої верифікації за матеріалами про конкретні кампанії. Виходячи з цих змін, вважаємо за доцільне розвивати в державних структурах сценарне моделювання інформаційних загроз із використанням прогнозної аналітики та перевірених поведінкових даних. Таке моделювання має допомагати визначати можливі реакції аудиторій, оцінювати ризики поляризації та заздалегідь готувати пояснювальні повідомлення, зберігаючи експертний і правовий контроль над застосуванням алгоритмів. Одним із наслідків цифрової трансформації є посилення залежності видимості контенту від алгоритмічного ранжування платформ. Воно може знижувати доступність альтернативних позицій, підсилювати вже сформовані уподобання та підтримувати ефект інформаційної бульбашки. Дослідник стратегічних комунікацій Луї Брук розглядає ШІ як чинник організаційної перебудови сучасного StratCom і пов’язує його застосування з переходом до швидшого аналізу середовища та адаптації комунікаційних рішень [315]. На цій підставі архітектуру державного наративу визначаємо як поєднання змісту, каналів, процедур перевірки й алгоритмічних умов видимості, за яких достовірні пояснення подій стають своєчасними та доступними для відповідних аудиторій. ШІ-системи можуть скорочувати час аналізу й підготовки рішень у циклі OODA, однак остаточна оцінка політичних наслідків і відповідальність за дію залишаються за людиною. У такій моделі державні комунікаційні структури набувають рис технологічних організацій, де аналітика даних, тестування гіпотез

і швидке коригування повідомлень поєднуються з нормативними обмеженнями та суспільною підзвітністю. Великі мовні моделі й семантичний аналіз можуть підтримувати підготовку сценаріїв пребанкінгу, але зміст таких інтервенцій має проходити експертну перевірку та емпіричне оцінювання. Це дозволяє змістити частину зусиль із реактивного спростування на попереднє пояснення типових прийомів маніпуляції та підвищення стійкості аудиторій.

Перспективи трансформації стратегічних комунікацій пов'язані зі зміною самого інформаційного середовища. Невілл Болт та Еліна Ланге-Йонатамішвілі у звіті Центру передового досвіду НАТО зі стратегічних комунікацій «The NextGen Information Environment» аналізують технологічні й соціальні зміни, які визначатимуть умови комунікації в найближчі роки [316]. У межах наведених положень можемо сформулювати висновок про поступовий перехід від прямого переконання до створення умов, у яких аудиторія здатна орієнтуватися між конкуруючими потоками інформації. Для опису технологічного складника цього процесу використовуємо авторську робочу категорію «алгоритмічна координація видимості та пріоритетності контенту». Вона охоплює узгодження аналітичних систем, каналів поширення й правил ранжування, завдяки яким перевірені повідомлення можуть своєчасно досягати потрібних аудиторій. Така координація має підпорядковуватися прозорим цілям, правовим нормам і процедурі людського нагляду, оскільки технічне підвищення видимості не повинно підміняти автономію користувача. Інформаційний захист у цій логіці вбудовується в доступну й зрозумілу цифрову взаємодію держави з громадянами та підтримує можливість перевірити походження повідомлення, його зміст і підстави для поширення.

Інтеграція ШІ в систему стратегічних комунікацій потребує одночасного врахування інформаційних і технічних ризиків. Національний інститут стандартів і технологій США (National Institute of Standards and Technology, NIST) у «AI Risk Management Framework 1.0» визначає надійний ШІ через такі взаємопов'язані характеристики, як валідність і надійність, безпечність, захищеність і стійкість, підзвітність і прозорість, пояснюваність, захист

приватності та керування шкідливими упередженнями [317]. Застосовуючи підхід NIST до стратегічних комунікацій, вважаємо за доцільне включити перевірку походження даних, стійкості моделей до маніпулятивного втручання, пояснюваності результатів і можливості аудиту до базових вимог державних ШІ-систем. Окремим ризиком є навмисне спотворення навчальних даних або контексту запиту, яке може змінити класифікацію загрози, пріоритетність повідомлень чи рекомендації системи. Технічний захист моделі має поєднувати контроль доступу, журналювання операцій, перевірку цілісності даних і регулярне тестування на вразливості. У сфері StratCom ці процедури повинні доповнювати змістову верифікацію, оскільки формально коректна модель може відтворювати неточні або політично небезпечні висновки. Поєднання стратегічних комунікацій із кібербезпекою створює умови для контролю походження контенту, цілісності моделей і автоматизованої перевірки інформаційних продуктів.

Трансформація стратегічних комунікацій безпосередньо пов’язана з розвитком концепції когнітивної війни. У звіті головного наукового співробітника НАТО «Cognitive Warfare» (2025), підготовленому під редакцією Джанет Блатні, розглядаються можливості технологічного впливу на когнітивні процеси й використання вразливостей людського сприйняття [56]. ШІ підвищує точність сегментації аудиторій і персоналізації повідомлень на основі цифрових поведінкових даних, однак реальна результативність такого впливу залежить від контексту, якості даних і організаційної спроможності суб’єкта операції. У межах дисертації когнітивний захист визначаємо як сукупність інституційних, технологічних і освітніх заходів, спрямованих на збереження здатності громадян критично сприймати інформацію, оцінювати її походження та ухвалювати рішення без прихованого маніпулятивного примусу. Центром такого захисту є процеси сприйняття, оцінювання та ухвалення рішень, на які спрямовуються сучасні операції когнітивного впливу [56]. Відповідно, державна система має відстежувати зміни не лише в обсягах поширення контенту, а й у способах його інтерпретації різними групами населення. Практична реалізація цього підходу

передбачає поєднання моніторингу інформаційного середовища, дослідження вразливостей, медіаграмотності та своєчасної державної комунікації.

В Україні вже існують окремі технологічні та інституційні компоненти, які можуть бути поєднані в систему швидшого виявлення й аналізу інформаційних загроз. Для опису такого узгодження використовуємо авторську робочу категорію «алгоритмічна оркестрація». Під нею розуміємо скоординовану роботу аналітичних платформ, моделей ШІ, державних комунікаційних каналів і фахівців, за якої автоматизована система допомагає виявити зміну інформаційного середовища, а інтерпретація загрози й рішення про реагування залишаються в межах визначеної інституційної відповідальності. Йдеться про організаційний принцип, а не про створення єдиного централізованого алгоритму управління комунікацією.

Підсумки Міністерства цифрової трансформації України за 2025 рік описують «агентивну державу» як напрям розвитку цифрових послуг, у якому ШІ-асистенти допомагають користувачеві виконувати окремі сервісні дії [318]. Для стратегічних комунікацій важлива сама зміна інтерфейсу між громадянином і державою. Персоналізований цифровий сервіс здатний швидше пояснювати процедуру, спрямовувати користувача до перевіреної інформації та зменшувати простір для маніпуляцій навколо складних адміністративних питань. Водночас така взаємодія потребує чітко встановлених меж використання персональних даних, прозорих правил автоматизованої відповіді та можливості перейти до взаємодії з людиною.

Аналітичний рівень цієї системи може будуватися на інструментах, здатних працювати з великими масивами повідомлень і виявляти зміну наративів. Національний кластер з інформаційної стійкості, започаткований 2023 року як майданчик взаємодії державних органів, громадського сектору та технологічних компаній, представив серед таких рішень Mantis Analytics [319]. Платформа орієнтована на аналіз інформаційного поля та динаміки наративів [319]. Для стратегічних комунікацій важливий перехід від підрахунку окремих згадок до спостереження за тим, як тема змінюється, з якими повідомленнями поєднується

і в яких сегментах інформаційного середовища отримує поширення. Такий аналіз дозволяє раніше помічати момент, коли окреме повідомлення починає формувати стійкішу інтерпретацію подій. Точність конкретних модулів і межі їх застосування при цьому мають встановлюватися за технічною документацією та результатами незалежного тестування.

Інший ресурс формує оборонний технологічний сектор. BRAVE1 – український кластер підтримки розробок у сфері оборонних технологій – створює середовище для появи рішень, частина яких може використовуватися для аналізу даних, підвищення ситуаційної обізнаності та роботи в кібер- й інформаційному просторі. В офіційному повідомленні РНБО від 26 квітня 2023 року діяльність BRAVE1 прямо пов’язано з розвитком спроможностей для розвідувальних і наступальних операцій у кібер- та інформаційному просторі [320]. Для нашого дослідження важливо розмежовувати технологічну доступність інструмента та його придатність для стратегічних комунікацій. Використання оборонної розробки для аналізу суспільного інформаційного середовища потребує окремої перевірки функцій, режиму доступу до даних і наслідків для прав громадян.

Комерційні аналітичні системи утворюють ще один рівень цієї екосистеми. Платформа Cyabra спеціалізується на аналізі автентичності облікових записів, виявленні координованого підсилення контенту та картографуванні бот-мереж [321]. Такі функції допомагають відділяти органічну активність аудиторії від штучно створеної видимості підтримки або обурення. Для державної комунікації це принципово, оскільки помилкова оцінка координованої кампанії як реальної суспільної реакції здатна впливати на вибір теми, тональність повідомлень і пріоритети реагування. Разом із тим приватна платформа має постачати аналітичний сигнал, а право визначати зміст допустимої публічної дискусії залишається поза межами її функцій. Взаємодія держави з такими системами потребує процедур тестування, аудиту й перевірки отриманих висновків.

Масштаб державних цифрових каналів створює окрему можливість для поширення перевіреної інформації. Станом на 24 грудня 2025 року застосунок

«Дія» мав понад 23 млн користувачів [322]. Така аудиторія робить державний сервіс потенційно важливим каналом кризової та пояснювальної комунікації, але сама кількість користувачів не забезпечує стійкості до дезінформації. Вирішальними залишаються довіра до джерела, своєчасність повідомлення, зрозумілість пояснення та відокремлення сервісної функції від прихованого впливу на переконання. ШІ-асистент може допомагати громадянину знаходити перевірену інформацію й розуміти адміністративні процедури, якщо межі такої допомоги є прозорими й підконтрольними користувачеві.

Якуб Каленський і Роман Осадчук у дослідженні Європейського центру передового досвіду з протидії гібридним загрозам описують українську модель протидії російській дезінформації через метафору «вулик проти мамонта» [323]. Її сильна сторона полягає в мережевій взаємодії державних установ, громадських ініціатив, медіа, фактчекерів і технологічних команд, здатних швидко обмінюватися інформацією та розподіляти завдання [323]. Саме в такій структурі «алгоритмічна оркестрація» може мати практичний сенс: аналітичні системи прискорюють виявлення й передачу сигналу, тоді як різні учасники зберігають власну компетенцію, способи перевірки та відповідальність. Результатом має бути швидша координація без перетворення інформаційного захисту на централізоване алгоритмічне управління суспільною дискусією.

Алгоритмічну пильність доцільно розглядати як перспективний напрям розвитку, у межах якого цифрові системи допомагають своєчасно помічати зміни в інформаційному середовищі, а рішення про реагування залишаються за відповідальними інституціями. Україна вже має окремі компоненти такого підходу: інструменти моніторингу, оборонні технологічні розробки, державні цифрові сервіси й мережі громадської взаємодії. Їх поєднання ще не утворює цілісного «когнітивного щита», але створює основу для подальшої інтеграції. Інформаційний захист має поєднувати законні обмеження протиправної діяльності, виявлення аномалій, швидке поширення перевірених пояснень і розвиток когнітивної стійкості громадян. Український досвід може використовуватися в міжнародному обміні практиками протидії операціям

впливу, особливо в частині гнучкої взаємодії державних і недержавних учасників. У звіті OpenAI «Disrupting malicious uses of AI» від 25 лютого 2026 року показано, що суб'єкти загроз використовують мовні моделі як один з елементів ширших операційних процесів [324]. Серед таких функцій названо пошук інформації, підготовку й переклад контенту, а також допоміжну автоматизацію окремих завдань [324]. Для російських операцій це означає можливість швидше створювати варіанти повідомлень, адаптувати їх до різних мов і аудиторій та підтримувати постійний темп публікацій. Генеративний ШІ знижує часові витрати на виробництво контенту, проте результативність кампанії й надалі залежить від організаційної інфраструктури, каналів поширення, знання цільової аудиторії та здатності координувати дії.

Трансформація загроз простежується у «Microsoft Digital Defense Report 2025», де взаємозв'язок ШІ, соціальної інженерії та кіберзлочинності розглядається як один із чинників ускладнення цифрового середовища [325]. ШІ може посилювати фішингові й інші маніпулятивні повідомлення завдяки мовній адаптації, персоналізації та використанню викрадених або відкритих даних [325]. Така персоналізація підвищує правдоподібність звернення й може спонукати адресата відкрити шкідливе посилання, передати облікові дані або виконати іншу потрібну зловмиснику дію. Після компрометації цифрового середовища отримані дані можуть використовуватися для точнішого інформаційно-психологічного впливу. Отже, кібероперації й комунікаційні маніпуляції утворюють взаємопов'язаний ланцюг: технічний доступ забезпечує дані та канали, а інформаційний вплив перетворює їх на поведінковий ефект. Протидія цьому поєднанню потребує узгодженої роботи кіберзахисту, стратегічних комунікацій і систем управління інцидентами.

Системні ризики, пов'язані з масштабним поширенням генеративних моделей, посідають помітне місце у доповіді Всесвітнього економічного форуму «The Global Risks Report 2026». У ній мізінформація та дезінформація посідають друге місце у дворічному горизонті та четверте – у десятирічному [326]. Така оцінка пов'язує інформаційні порушення з поляризацією, ослабленням довіри й

ускладненням колективного реагування на інші глобальні ризики. У воєнно-політичному контексті генеративний ШІ підвищує швидкість створення різних версій повідомлення та полегшує їх адаптацію до локальних суперечностей. Вікторас Даукшас і Лайма Венцлаускене у дослідженні «The Collage of the Kremlin's Communication Strategy» описують російську комунікаційну стратегію як гнучке поєднання різних каналів, тем і форматів, що можуть комбінуватися відповідно до обставин [327]. Модель «колажу» пояснює, чому окремі суперечливі повідомлення здатні працювати на спільну політичну мету без єдиної послідовної картини світу. ШІ може підсилювати цю практику, прискорюючи підготовку варіативного контенту та його мовну адаптацію, хоча джерело не визначає алгоритм як центральний вузол такої системи. У результаті технологічна автоматизація підвищує адаптивність і потенційне охоплення вже сформованої комунікаційної стратегії.

У контексті технологічної інфраструктури таких операцій досвід виявлення та нейтралізації мереж на кшталт «Doppelgänger» у попередні періоди (2023–2024 рр.) став точкою відліку для розуміння процесів повної автоматизації доменного та контентного виробництва. У звітах 2026 року простежується подальше зростання ролі персоналізації та автоматизації в операціях впливу. Їхньою мішенню стає увага, емоційне сприйняття й здатність аудиторії оцінювати суперечливі повідомлення. Аналіз поведінкових і психографічних даних дає змогу формувати різні версії одного наративу для вузьких груп, підбираючи звичну лексику, темп і емоційний тон. У звіті НАТО про когнітивну війну технологічний вплив розглядається в контексті процесів сприйняття, інтерпретації та ухвалення рішень [56]. Для позначення кумулятивного ефекту тривалого перебування в перенасиченому суперечливому середовищі використовуємо авторську категорію «семантичне виснаження». Вона описує зниження готовності перевіряти інформацію, розрізняти джерела й підтримувати послідовну картину подій унаслідок постійної зміни версій та емоційних стимулів. За певних соціальних умов цей стан може сприяти апатії, поляризації або радикалізації, але характер і масштаб наслідків потребують емпіричної

перевірки для кожної аудиторії. Відповідно, система протидії має аналізувати не тільки поширення окремих фейків, а й накопичувальний вплив інформаційного середовища на здатність громадян орієнтуватися в подіях.

Перспективним напрямом інформаційного захисту є протидія семантичному отруєнню (semantic poisoning), яке в межах дослідження визначаємо як поступове спотворення контекстів, зв'язків і значень, що використовуються аудиторією для інтерпретації політичної реальності. Зафіксовані OpenAI операції демонструють використання мовних моделей для масового виробництва варіативного контенту та допоміжних завдань у ширших кампаніях впливу [324]. Небезпека полягає у накопиченні невеликих зміщень у лексиці, причинних зв'язках і емоційній оцінці подій, які окремо можуть не виглядати як дезінформація. Це вимагає від національної системи StratCom переходу до моделі «наративного моніторингу» нового покоління, яка була б здатною відстежувати не лише ключові слова, а й ледь помітні зміни в семантичній та емоційній структурі суспільного діалогу, що часто сигналізують про підготовку масштабного зсуву громадської думки перед важливою політичною подією. Дослідження Центру передового досвіду НАТО зі стратегічних комунікацій оцінює можливості великих мовних моделей у роботі з офіційними мовами ЄС, які мають менше цифрових ресурсів [328]. Отримані результати підтверджують потребу тестувати моделі окремо для кожної мови й комунікаційного завдання, оскільки якість відповідей залежить від обсягу та структури навчальних даних [328]. Синтетичний текст стає складніше виявляти лише за мовними ознаками, тому семантичний аналіз має доповнюватися перевіркою метаданих, походження контенту, мережевої поведінки й цифрових маркерів. Національні мовні ресурси можуть підвищити якість українськомовного аналізу, однак вони є одним компонентом багаторівневої системи верифікації.

Одним із перспективних напрямів розвитку української системи стратегічних комунікацій є створення національної великої мовної моделі. Її доцільність визначається завданнями, для яких критично важливими є

українська мова, національний суспільно-політичний контекст, законодавча термінологія та робота з даними державних систем. Використання зовнішніх моделей у таких сценаріях пов’язане з питаннями юрисдикції обробки інформації, доступності сервісу, захисту чутливих даних і точності відтворення локального контексту. Конкретний рівень кожного ризику залежить від архітектури розгортання та умов використання моделі. Через це національна LLM має розглядатися не як універсальна заміна зовнішніх систем, а як спеціалізований компонент для завдань, де контроль над даними й українським мовним контекстом має підвищене значення.

Дмитро Овчаренко, технічний директор Центру штучного інтелекту Міністерства цифрової трансформації України, пов’язує створення національної LLM із потребою якісніше опрацьовувати українську мову, локальний контекст і завдання державних сервісів [329]. Для такого проєкту принциповими є склад і походження навчальних даних. Нерівномірне представлення історичних подій, суспільних груп або правових понять може відтворюватися у відповідях моделі й непомітно впливати на пояснення політично чутливих питань. Власні мовні ресурси дають державі ширші можливості контролювати якість корпусів, встановлювати процедури їх оновлення й перевіряти систематичні помилки. Водночас контроль над навчальними даними не гарантує нейтральності моделі, а створює можливість зробити процедуру її формування більш прозорою та підзвітною.

Для узагальнення цієї спроможності використовуємо поняття «семантичний суверенітет». Воно означає здатність держави й суспільства підтримувати власні мовні ресурси, дані та моделі, необхідні для інтерпретації національно значущої інформації, і водночас перевіряти принципи, за якими ці системи формують відповіді. Йдеться про контроль над критично важливою інфраструктурою смислової обробки інформації, а не про ізоляцію українського інформаційного середовища від зовнішніх джерел або моделей. Практично семантичний суверенітет передбачає можливість працювати з чутливими даними у визначеному правовому режимі, контролювати оновлення системи, зберігати

журнали її роботи й незалежно оцінювати результати.

Воєнний досвід України створює значний масив матеріалів про дезінформаційні кампанії, кібероперації та кризові комунікації. Використання таких даних для навчання або тестування моделей потребує правового очищення, анонімізації, визначення режимів доступу та етичного контролю. Особливої обережності потребують матеріали, що містять персональні дані, службову інформацію або відомості, за якими можна відновити структуру роботи державних чи військових організацій. Національна модель матиме перевагу лише тоді, коли доступ до більш релевантних даних поєднуватиметься з вищим рівнем їх захисту й контролю за способами використання.

Семантичний суверенітет водночас передбачає міжнародну сумісність. AJP-10 пов’язує ефективність стратегічних комунікацій із координацією, взаємодією та спільним розумінням інформаційного середовища [85]. Для ШІ-систем це означає можливість передавати партнерам перевірені індикатори загроз, порівнювати результати аналізу та використовувати узгоджені способи опису операцій впливу. Спільність форматів при цьому не потребує централізації даних: національні інституції можуть зберігати контроль над власними масивами інформації й передавати лише ті елементи, які потрібні для спільної оцінки транскордонної кампанії.

Дослідники RAND Corporation аналізують можливість істотного впливу ШІ на майбутні воєнні змагання та процеси ухвалення рішень [330]. Для стратегічних комунікацій із цього випливає потреба завчасно формувати спільний понятійний апарат, за допомогою якого різні системи та аналітичні групи однаково інтерпретуватимуть основні характеристики інформаційної загрози. Вважаємо за доцільне використовувати узгоджені словники індикаторів, типології наративів і правила опису операцій впливу. Разом із самим індикатором мають передаватися відомості про джерело, час фіксації, рівень упевненості й можливі альтернативні пояснення. Такий порядок дозволяє партнеру перевірити логіку висновку замість механічного прийняття автоматизованої оцінки.

Практичним прикладом багатосторонньої технологічної координації є Талліннський механізм підтримки цивільної кіберстійкості України. За даними Міністерства цифрової трансформації України, він об'єднує тринадцять держав і мобілізував 241,7 млн євро допомоги на два роки [331]. Офіс управління проєктами механізму узгоджує українські потреби з можливостями держав-партнерів та координує реалізацію відповідних проєктів [331]. Для майбутньої інтеграції ШІ цей досвід важливий як уже діюча модель, у якій міжнародна підтримка організовується навколо визначених національних потреб. Подальше включення ШІ-рішень до подібних програм доцільно пов'язувати зі спільними критеріями безпеки, правилами роботи з даними, незалежним тестуванням та вимірюваними результатами.

Таким чином, розвиток національної LLM і міжнародна технологічна взаємодія утворюють взаємодоповнювальні напрями. Власна модель дозволяє посилити контроль над мовними ресурсами, чутливими даними та локальним контекстом, а взаємосумісність забезпечує можливість зіставляти результати й координувати реагування з партнерами. У межах запропонованого підходу до семантичного суверенітету ці завдання поєднуються через принцип контрольованої відкритості: критично важливі дані та моделі залишаються під національною відповідальністю, тоді як стандарти опису загроз, процедури перевірки й окремі індикатори можуть бути спільними.

Юридична інтеграція ШІ в систему стратегічних комунікацій потребує узгодження національного регулювання з європейськими нормами. Регламент (ЄС) 2024/1689, що встановлює гармонізовані правила у сфері штучного інтелекту, був ухвалений 13 червня 2024 року та опублікований в Офіційному журналі Європейського Союзу 12 липня 2024 року [332]. Рамкова конвенція Ради Європи про штучний інтелект, права людини, демократію та верховенство права відкрилася для підписання 5 вересня 2024 року [333]. Обидва документи формують важливі орієнтири для цивільного застосування ШІ, але їхня сфера дії має окремі виключення щодо національної оборони й національної безпеки. Тому цивільні комунікаційні сервіси держави та оборонні системи потребують

розмежованих режимів оцінювання, контролю доступу й підзвітності. Пропонуємо ініціювати постійний міжвідомчий діалог між органами, відповідальними за цифрову трансформацію, інформаційну безпеку, оборону, захист персональних даних і права людини. Його завданням має стати вироблення узгоджених правил для систем подвійного призначення, які можуть застосовуватися і в державних сервісах, і в безпековому секторі.

У системі інформаційної безпеки України необхідною складовою стратегічних комунікацій є нормативне й етичне регулювання використання штучного інтелекту. Для цивільних систем окремі застосування можуть належати до категорій високого ризику за EU AI Act, тоді як системи, призначені виключно для військових, оборонних або національно-безпекових цілей, мають окремий правовий режим [332]. Аналітичний матеріал Європейського парламенту узагальнює ризик-орієнтовану структуру регулювання цивільних ШІ-систем [334]. Вимоги до високоризикових систем охоплюють управління ризиками, якість даних, технічну документацію, прозорість, реєстрацію подій і людський нагляд [332]. Вважаємо необхідним розробити національну методику оцінювання ризиків ШІ для цивільних систем стратегічних комунікацій, узгоджену з EU AI Act і вимогами захисту чутливої інформації. Методика має визначати критерії допустимості даних, процедури тестування, підстави для зупинення системи та порядок оскарження автоматизованого результату. Людина повинна зберігати відповідальність за політично значущі повідомлення, оцінювання загроз і рішення, що можуть впливати на права громадян. Автоматизована рекомендація набуває практичного значення лише після перевірки її фактичної основи, контексту й можливих побічних наслідків.

Рамкова конвенція Ради Європи про штучний інтелект встановлює вимогу забезпечувати відповідність діяльності впродовж життєвого циклу ШІ принципам прав людини, демократії та верховенства права [333]. Для стратегічних комунікацій цей орієнтир означає збереження автономії сприйняття й ухвалення рішень громадянином. Державні системи можуть допомагати виявляти маніпуляції, пояснювати складні події та забезпечувати доступ до

перевіреної інформації, але їхня архітектура не повинна передбачати прихований примус або непомітну зміну політичної поведінки. Демократична перевага полягає у здатності підвищувати якість суспільної орієнтації через прозорість джерел, відкритість критеріїв і можливість перевірки. Тому оцінювання ШІ-систем має охоплювати не тільки точність, а й вплив на свободу думки, плюралізм, недискримінацію та доступ до альтернативних пояснень. Когнітивна стійкість у такій моделі формується завдяки підтриманню критичного мислення, а не технологічному керуванню переконаннями.

Окремим етичним і технічним викликом залишається алгоритмічна упередженість (algorithmic bias). Моделі можуть відтворювати нерівномірність навчальних даних, помилки маркування та приховані припущення, закладені під час розроблення. У системах аналізу інформаційного середовища це здатне створити викривлену картину настроїв, помилково визначити групу як джерело загрози або пропустити новий тип маніпуляції. Моніторинг соціальної напруги за допомогою ШІ розглядається як перспективний напрям, реалізація якого має супроводжуватися оцінюванням алгоритмічної упередженості. Дорожня карта впровадження має передбачати незалежний аудит даних і моделей, тестування на різних групах, публічне документування обмежень та механізм виправлення помилок. У січні 2024 року Міністерство цифрової трансформації України оприлюднило рекомендації щодо відповідального використання ШІ в медіа, приділивши увагу прозорості, перевірці інформації та позначенню згенерованого матеріалу [335]. Цей документ підтверджує формування нормативно-етичних орієнтирів, але не засвідчує завершеного впровадження єдиної системи маркування. Прозоре позначення синтетичного контенту може підтримувати довіру до державної комунікації за умови, що маркер є зрозумілим, технічно стійким і не замінює перевірку фактичного змісту.

Виходячи з проведеного аналізу, визначаємо авторську послідовність упровадження ШІ в систему стратегічних комунікацій та інформаційного захисту України. Перший етап має охопити нормативне розмежування цивільних і оборонних застосувань, створення методики оцінювання ризиків та

формування захищеної обчислювальної інфраструктури. Другий етап передбачає розроблення й незалежне тестування національної великої мовної моделі, придатної для українськомовного семантичного аналізу, державних сервісів і роботи з перевіреними корпусами. Третій етап може включати застосування ШІ в «Дії» та інших цифрових сервісах лише для чітко визначених сценаріїв із вимогами приватності, точності, журналювання та можливості оскарження результату. Четвертий етап пов'язаний із міжнародною сумісністю: необхідно погодити формати даних, рівні доступу, правила передачі індикаторів і процедури спільної перевірки інформаційних загроз. П'ятий етап може передбачати використання проактивних агентних систем у межах обмежених функцій, де кожна дія реєструється, має визначеного відповідального суб'єкта й допускає людське втручання. Семантичний суверенітет у цій послідовності означає здатність України контролювати критично важливі мовні ресурси, дані та моделі, зберігаючи міжнародну взаємосумісність і відкритість до незалежної оцінки. Наявні цифрові сервіси, аналітичні платформи, технологічні кластери та партнерські механізми становлять окремі компоненти майбутньої системи, а їх інтеграція потребує єдиних стандартів, стабільного фінансування, фахових кадрів і демократичного нагляду. За таких умов ШІ може посилити швидкість виявлення загроз, якість пояснювальних повідомлень і здатність держави підтримувати когнітивну стійкість суспільства без підміни людської відповідальності автоматизованим рішенням.

Висновки до розділу 3

1. Виходячи з проведеного аналізу, визначаємо політико-правову основу захисту інформаційного простору України як поєднання конституційно допустимих обмежень, спеціального законодавства, стратегічних документів, санкційних і медіарегуляторних процедур та організаційно-технологічного захисту. Її дієвість забезпечують правова визначеність, адресність і пропорційність втручання, процедурна відтворюваність, міжвідомча координація, фіксація доказового ланцюжка та регулярний

перегляд тимчасових обмежень. Така конфігурація дає змогу поєднувати оперативну протидію ворожому впливу із захистом прав людини, суспільною довірою та європейськими правовими стандартами. У такий спосіб конкретизовано авторський підхід до захисту інформаційного простору як узгодженої системи правових, інституційних і технологічних механізмів.

2. Удосконалено підхід до аналізу гуманітарних складників антиукраїнських інформаційно-пропагандистських операцій. У межах цього підходу визначаємо, що гуманітарна складова російської агресії поєднує доктрину «руського міра», ревізіоністське переозначення історичної пам’яті й культурної спадщини та мовно-цифрову інфраструктуру поширення наративів. Її адресність проявляється у диференційованому впливі на мешканців тимчасово окупованих територій, дітей і молодь, внутрішньо переміщених осіб, релігійні громади та українців за кордоном. Інституційна вбудованість і тривала присутність цих практик у повсякденній комунікації спрямовані на зміну ідентичності, пам’яті, довіри й уявлень про політичне майбутнє України. Ревізіоністські інтерпретації історії та культурної спадщини використовуються для делегітимації української державності й переозначення колективної пам’яті. Поширення цих наративів у цифровому просторі призвело до формування викривленої реальності, у якій маніпуляція пам’яттю стає інструментом легітимізації насильства. Результатом цього процесу є спроба агресора зруйнувати ціннісний фундамент українського суспільства, замістивши його сконструйованими образами «штучності» держави. Доходимо висновку, що ефективність такої деструктивної діяльності залежить не лише від змісту повідомлень, а й від системності їхнього впровадження в інформаційну мережу на всіх рівнях комунікації.
3. Систематизовано цифрові, медійні, організаційні, символічні та примусові інструменти російської гуманітарної агресії. Їхня операційна логіка поєднує цифрову окупацію, координовану неавтентичну активність,

псевдоновинні мережі, технологічну мімікрію, спеціальні інформаційні операції, кампанії поведінкового впливу та переозначення символічного простору. Кейс-аналіз бот-мереж, Portal Kombat, «Doppelgänger», Operation Overload і кампанії проти мобілізації показав адаптацію змісту й каналів до локальних вразливостей. У межах авторського підходу протидію цим практикам визначаємо через узгодження правових, інституційних, локальних, цифрових і міжнародних механізмів із довгостроковим відновленням гуманітарного простору. Така систематизація конкретизує політичну природу російської гуманітарної агресії як взаємопов'язаної сукупності практик впливу на ідентичність, поведінку та суспільну згуртованість.

4. Обґрунтовано поетапне впровадження штучного інтелекту в систему стратегічних комунікацій та інформаційного захисту України. Визначена послідовність охоплює нормативне розмежування цивільних і оборонних застосувань, інтеграцію аналітичних інструментів у чинні процеси, розвиток національних мовних ресурсів і моделей, міжнародну взаємосумісність та обмежене використання проактивних агентних систем. Національну велику мовну модель розглянуто як спеціалізований компонент для завдань, де особливого значення набувають українська мова, локальний суспільно-політичний контекст і контроль над чутливими даними. Поняття «семантичний суверенітет» використано для позначення здатності держави й суспільства підтримувати власні мовні ресурси, дані та моделі, перевіряти принципи їхньої роботи й водночас зберігати міжнародну взаємосумісність. Аналітичні платформи, державні цифрові канали, технологічні кластери та партнерські механізми розглянуто як окремі компоненти системи, інтеграція яких потребує незалежного тестування, правового й етичного контролю, захисту даних, реєстрації автоматизованих дій та збереження відповідальності за людиною. Такий підхід дозволяє використовувати швидкість машинного аналізу без передачі алгоритмам права визначати зміст суспільно значущої

комунікації.

Узагальнення результатів розділу показує, що захист інформаційного простору потребує узгодження політико-правових, організаційних, гуманітарних, комунікаційних і технологічних механізмів. Стратегічні комунікації забезпечують зв’язок між аналізом загроз, публічним поясненням державних рішень, відповідальним використанням технологій штучного інтелекту та підтриманням когнітивної стійкості суспільства. Автоматизований моніторинг і прогнозна аналітика посилюють цю систему настільки, наскільки їхні результати залишаються перевірюваними, а рішення – інституційно та персонально підзвітними.

ВИСНОВКИ

У дисертації досягнуто мету комплексного політологічного дослідження інформаційної складової сучасних воєн, провідних наративів та механізмів впливу на суспільну свідомість. Отримані результати охоплюють теоретико-методологічний, операційний, цифровий, гуманітарний, політико-правовий і технологічний рівні інформаційного протиборства. Їх поєднання дало змогу визначити інформаційну складову сучасних воєн як самостійний стратегічний вимір, у якому вплив на сприйняття, довіру, оцінювання та поведінку цільових аудиторій безпосередньо пов'язаний із досягненням політичних цілей конфлікту.

1. Теоретико-методологічні засади дослідження сформовано через поєднання системного, структурно-функціонального, порівняльного, контент-, дискурс- і наративного аналізу. Системний підхід забезпечив розгляд акторів, каналів, повідомлень і реакцій аудиторій як взаємопов'язаних елементів; структурно-функціональний – розмежування їхніх ролей; порівняльний – виявлення спільного й специфічного у конфігураціях впливу. Контент-, дискурс- і наративний аналізи дозволили простежити, як окремі повідомлення поєднуються у стійкі смислові конструкції, що функціонують як рамки політичного оцінювання. У результаті методологічний інструментарій виконав конструктивну функцію: упорядкував різнорідний емпіричний матеріал і забезпечив перехід від опису інформаційних кампаній до пояснення їхньої логіки, механізмів і наслідків.
2. Уточнення категорійно-понятійного апарату дало змогу впорядкувати зміст і співвідношення понять «інформаційна складова сучасної війни», «спеціальна інформаційна операція», «інформаційно-психологічна операція», «когнітивна війна», «наратив», «суспільна свідомість», «деструктивний інформаційний вплив», «механізми впливу на суспільну свідомість», «інформаційна безпека», «стратегічні комунікації» та «когнітивна стійкість». Удосконалений понятійний апарат розмежовує

стратегічний, операційний, смисловий, технологічний і поведінковий рівні інформаційного протиборства та водночас показує їхню функціональну взаємозалежність. Це створило послідовну систему координат для аналізу того, як політичний задум переходить у наратив, операцію, цифрове поширення та конкретний поведінковий ефект.

Зіставлення проаналізованих кампаній дає змогу виокремити кілька найбільш стійких наративних ліній російського інформаційного впливу. До них належить делегітимація української державності та політичної суб'єктності. Окремий напрям становить дискредитація державних інституцій і військово-політичного керівництва. Ще одна стійка лінія пов'язана з формуванням уявлень про виснаження та безперспективність тривалого спротиву через теми воєнних втрат, мобілізації, економічних труднощів і неминучості поступок. Так само системно використовується наратив про послаблення або припинення міжнародної підтримки України. У межах дослідження ці наративи визначаємо як провідні з огляду на їх повторюваність у різних кампаніях і каналах, тривалу політичну функцію та адаптацію до різних цільових аудиторій.

3. Запропоновано та застосовано авторську п'ятиетапну аналітичну модель життєвого циклу спеціальної інформаційної операції, що охоплює когнітивне картографування цільової аудиторії, конструювання наративу, поширення, активну фазу впливу та моніторинг із подальшою адаптацією. Когнітивне картографування виокремлено як самостійний вхідний етап, результатом якого є встановлення зв'язку між вразливостями аудиторії, релевантними темами й тригерами, способом інтерпретації повідомлення та можливою реакцією. На матеріалі кампанії «Doppelgänger» та її подальшої трансформації простежено зв'язок між початковим аналізом аудиторії, конструюванням наративів, інфраструктурою їх поширення та адаптацією операції. Застосування моделі дозволяє розмежовувати операційну спроможність СІО, її цільовий когнітивний вплив та емпірично підтверджені політичні й поведінкові наслідки. У цій логіці когнітивна війна становить ширший стратегічний рівень протиборства, тоді як СІО є

одним з операційних механізмів його реалізації.

4. Аналіз механізмів інформаційної війни в умовах новітніх комунікативних технологій засвідчив, що цифровий вплив виникає через взаємодію смислової конструкції, каналу поширення, алгоритмічного ранжування, емоційного резонансу, координованої мережевої активності та поведінкової реакції аудиторії. Цифрова інфраструктура виконує активну функцію добору, підсилення й закріплення повідомлень у конкретних аудиторних спільнотах. Платформи забезпечують персоналізоване поширення та масштабування контенту, тоді як аналітичні системи й суб'єкти інформаційних операцій використовують цифрові дані для сегментації аудиторій, виявлення вразливостей і коригування впливу. Отже, технологічне середовище стало складником самої архітектури інформаційного протиборства.
5. Соціальні медіа визначено як один із провідних механізмів інформаційно-психологічного впливу на суспільну свідомість і поведінку. Їхня специфіка полягає у поєднанні персоналізації, високої швидкості поширення, емоційного підсилення конфліктних тем, формування цифрових ехо-камер, бот-мереж і астротурфінгу. За таких умов користувач отримує не просто повідомлення, а середовище соціального підтвердження, у якому повторювані оцінки сприймаються як позиція значної частини спільноти. Цільовий політичний ефект таких механізмів пов'язаний зі зміною довіри, емоційної мобілізації, способів оцінювання подій та готовності підтримувати або відкидати певні рішення; його фактична наявність у конкретній кампанії потребує окремого емпіричного підтвердження.
6. Специфіку кібербезпеки у воєнних умовах розкрито через зв'язок технічної стійкості цифрової інфраструктури з політичними й психологічними наслідками кібератак. Порушення доступності, цілісності або достовірності даних безпосередньо зачіпає роботу реєстрів, зв'язку, медіа, цифрових сервісів і критичної інфраструктури, а його політико-комунікаційні наслідки можуть проявлятися у зниженні довіри до

інституцій, відчутті вразливості держави та інформаційній дезорієнтації суспільства. Тому кіберзахист доцільно розглядати як технічний і політико-комунікаційний складник інформаційної безпеки, узгоджений зі стратегічними комунікаціями, аналітичним моніторингом та реагуванням на інформаційно-психологічні операції.

7. Політико-правову основу захисту інформаційного простору України визначено як поєднання конституційно допустимих обмежень, спеціального законодавства, стратегічних документів, санкційних і медіарегуляторних процедур та організаційно-технологічного захисту. Дієвість цієї системи забезпечують правова визначеність, адресність і пропорційність втручання, процедурна відтворюваність, міжвідомча координація, фіксація доказового ланцюжка та регулярний перегляд тимчасових обмежень. Така конфігурація поєднує оперативне реагування на ворожий вплив із захистом прав людини, підтриманням суспільної довіри та дотриманням європейських правових стандартів. Саме через цей зв'язок нормативні рішення набувають політичної легітимності та практичної стійкості.
8. Підхід до аналізу гуманітарних складників антиукраїнських інформаційно-пропагандистських операцій удосконалено через виокремлення трьох взаємопов'язаних домінант: доктрини «руського міра», ревізіоністського переозначення історичної пам'яті й культурної спадщини та мовно-цифрової інфраструктури поширення наративів. Їхня адресність проявляється у диференційованому впливі на мешканців тимчасово окупованих територій, дітей і молодь, внутрішньо переміщених осіб, релігійні громади та українців за кордоном. Ці практики охоплюють ідентичність, пам'ять, довіру, мовно-культурну належність і уявлення про політичне майбутнє України, тому гуманітарний захист становить самостійний напрям інформаційної безпеки.
9. Систематизація цифрових, медійних, організаційних, символічних і примусових інструментів російської гуманітарної агресії показала їхню

взаємодію в єдиній операційній екосистемі. Цифрова окупація, координована неавтентична активність, псевдоновинні мережі, технологічна мімікрія, спеціальні інформаційні операції, кампанії поведінкового впливу та переозначення символічного простору взаємно підсилюють одне одного. Кейс-аналіз бот-мереж, Portal Kombat, «Doppelgänger», Operation Overload і кампанії проти мобілізації підтвердив адаптацію змісту й каналів до локальних вразливостей аудиторій. Протидія такій екосистемі потребує узгодження правових, інституційних, локальних, цифрових і міжнародних механізмів із довготривалим відновленням гуманітарного простору.

10. Подальшого розвитку набули наукові уявлення про роль стратегічних комунікацій у системі інформаційної безпеки. Стратегічні комунікації визначаємо як інструмент випереджального формування зрозумілих пояснювальних наративів, координації державного повідомлення, публічного пояснення рішень і підтримання довіри до інституцій. Їхня функція полягає у поєднанні аналітичного виявлення загроз, узгодженого реагування та формування довготривалої когнітивної стійкості суспільства. Водночас ефективна система протидії поєднує автоматизовану детекцію, OSINT-моніторинг, аналіз бот-мереж, фактчекінг, дебанкінг, пребанкінг, цифрову верифікацію, контрнаративи й медіаграмотність, функціонально узгоджені зі стратегічними комунікаціями держави.
11. Перспективи використання штучного інтелекту в інформаційному захисті держави обґрунтовано через поетапну модель упровадження. Вона охоплює нормативне розмежування цивільних і оборонних застосувань, інтеграцію аналітичних інструментів у чинні процеси, розвиток національних мовних ресурсів і моделей, міжнародну взаємосумісність та обмежене використання проактивних агентних систем. Можливості автоматизованого моніторингу, класифікації, аналізу й прогнозування інформаційних загроз супроводжуються ризиками масштабування

синтетичної дезінформації, персоналізованого маніпулятивного контенту й автоматизованих інформаційно-психологічних операцій. Тому семантичний суверенітет у цій моделі поєднується з незалежною оцінкою, захистом даних, правовим і етичним контролем, реєстрацією автоматизованих дій та збереженням відповідальності за людиною.

Уперше запропоновано та застосовано авторську п’ятиетапну аналітичну модель життєвого циклу спеціальної інформаційної операції, у якій когнітивне картографування виокремлено як самостійний вхідний етап, що пов’язує характеристики й вразливості цільової аудиторії з подальшим конструюванням, поширенням та адаптацією наративного впливу. Цілісна політологічна модель дослідження виконує інтегруючу функцію, поєднуючи цей результат з аналізом когнітивної війни, соціальних медіа, гуманітарних чинників, стратегічних комунікацій, кібербезпеки та технологій штучного інтелекту. Удосконалено понятійний апарат, підхід до аналізу цифрових механізмів впливу, гуманітарних складників антиукраїнських операцій і комплексного захисту інформаційного простору. Подальшого розвитку набули положення про політичну природу сучасного інформаційного протиборства, когнітивну стійкість суспільства, роль стратегічних комунікацій та можливості й ризики використання штучного інтелекту. Узагальнення отриманих результатів дає підстави визначити результативність інформаційного захисту України через узгодження політико-правових, організаційних, комунікаційних, технологічних і гуманітарних інструментів, спрямованих на підтримання суспільної довіри, політичної суб’єктності та довготривалої когнітивної стійкості.

СПИСОК ВИКОРИСТАНИХ ДЖЕРЕЛ

1. Савчук В. А. Історична еволюція інформаційної складової гібридних воєн: від біблійних текстів до алгоритмів соціальних мереж. *Наукові праці Міжрегіональної Академії управління персоналом. Політичні науки та публічне управління*. 2025. № 2(78). С. 157–162. DOI: 10.32689/2523-4625-2025-2(78)-23.

2. Hanks B. K. Warfare and Ritual in Anthropology. *The Ashgate Research Companion to Anthropology* / ed. by P. J. Stewart, A. J. Strathern. Farnham : Ashgate, 2015. P. 273–294.

3. Harrison J. E. Themis: A Study of the Social Origins of Greek Religion. Cambridge : Cambridge University Press, 1912. xxxii, 559 p.

4. Біблія, Книга Суддів, 7:13–7:14; 7:20. Сайт Українського Біблійного Товариства. URL: https://www.ukrbs.org/bible/CUV/JDG.7 (дата звернення: 01.07.2026).

5. Фукідід. Промова Перікла / пер. з дав.-гр. А. Білецького. *Антична література: хрестоматія* / упоряд. О. І. Білецький. 2-ге вид. Київ : Радянська школа, 1968. 612 с. С. 283–287.

6. Гомер. Одіссея / пер. з давньогр. Б. Тена. Київ : Основи, 2015. 496 с. ISBN 978-966-500-430-8.

7. Гай Юлій Цезар. Нотатки про війну з галлами: з додатком Авла Гірція / пер. з лат. В. Д. Литвинова. Вид. 2-ге. Львів : Видавництво «Апріорі», 2024. 248 с.

8. Zanker P. The Power of Images in the Age of Augustus. Ann Arbor : University of Michigan Press, 1988. 385 p.

9. Сунь-цзи. Мистецтво війни / пер. з давньокит. С. Лесняка. Львів : Видавництво Старого Лева, 2015. 105, [4] с. ISBN 978-617-679-145-4.

10. Везерфорд Дж. Чингісхан та історія створення сучасного світу. Харків : Клуб Сімейного Дозвілля, 2024. 320 с. ISBN 978-617-15-0630-5.

11. Vilnius Summit Communiqué. NATO. 2023. 11 July. URL: https://www.nato.int/en/about-us/official-texts-and-resources/official-texts/2023/07/11/vilnius-summit-communique (дата звернення: 03.08.2026).

12. Skinner Q. Machiavelli: A Very Short Introduction. 2nd ed. Oxford : Oxford University Press, 2019. 144 p. ISBN 978-0-19-883757-2.

13. Durant W., Durant A. The Age of Napoleon: A History of European Civilization from 1789 to 1815. New York : Simon & Schuster, 1975. 872 p.

14. Donald D. The Age of Caricature: Satirical Prints in the Reign of George III. New Haven ; London : Yale University Press for the Paul Mellon Centre for Studies in British Art, 1996. viii, 248 p.

15. Harding C. Photographing conflict: Roger Fenton and the Crimean War. National Science and Media Museum Blog. 2012. 11 November. URL: https://blog.scienceandmediamuseum.org.uk/remembrance-day-part-1-photographing-war-fenton-crimean/ (дата звернення: 01.07.2026).

16. British propaganda and information during the First World War. The National Archives. URL: https://www.nationalarchives.gov.uk/help-with-your-research/research-guides/propaganda/ (дата звернення: 03.08.2026).

17. Reeves N. The Power of Film Propaganda: Myth or Reality? London ; New York : Cassell, 1999. viii, 262 p.

18. Hammond M. The Battle of the Somme (1916): An Industrial Process Film that “Wounds the Heart”. *British Silent Cinema and the Great War* / ed. by M. Hammond, M. Williams. London : Palgrave Macmillan, 2011. P. 19–38. DOI: 10.1057/9780230321663_2.

19. Welch D. Germany, Propaganda and Total War, 1914–1918: The Sins of Omission. New Brunswick, NJ : Rutgers University Press, 2000. xii, 355 p.

20. Eisenstein S. A Dialectic Approach to Film Form. *Film Form: Essays in Film Theory* / ed. and transl. by J. Leyda. New York : Harcourt, Brace, 1949. P. 45–63.

21. Taylor P. M. Munitions of the Mind: A History of Propaganda from the Ancient World to the Present Day. 3rd ed. Manchester : Manchester University Press, 2003. 344 p.

22. Welch D. The Third Reich: Politics and Propaganda. 2nd ed. London ; New York : Routledge, 2008. 256 p.

23. Kenez P. The Birth of the Propaganda State: Soviet Methods of Mass Mobilization, 1917–1929. Cambridge : Cambridge University Press, 1985. 308 p.

24. Berkhoff K. C. Motherland in Danger: Soviet Propaganda during World War II. Cambridge, MA : Harvard University Press, 2012. 407 p. ISBN 978-0-674-04924-6.

25. The Motherland Calls. The Art Institute of Chicago. URL: https://archive.artic.edu/tass/motherland-calls/ (дата звернення: 03.08.2026).

26. Russian Films in the Library of Congress. Library of Congress. URL: https://www.loc.gov/rr/mopic/findaid/russian.html (дата звернення: 03.08.2026).

27. Doherty T. Projections of War: Hollywood, American Culture, and World War II. New York : Columbia University Press, 1993. 364 p.

28. Lasswell H. D. Democracy through Public Opinion. Menasha (WI) : George Banta Publishing, 1941. 176 p.

29. Cull N. J. The Cold War and the United States Information Agency: American Propaganda and Public Diplomacy, 1945–1989. Cambridge : Cambridge University Press, 2008. xxvi, 533 p.

30. Our History. Radio Free Europe/Radio Liberty. URL: https://about.rferl.org/our-history/ (дата звернення: 03.08.2026).

31. Gaddis J. L. The Cold War: A New History. New York : Penguin Press, 2005. 333 p.

32. Chung Y. W. Leaflets, and the Nature of the Korean War as Psychological Warfare. *The Review of Korean Studies*. 2004. Vol. 7, no. 3. P. 91–116. ISSN 1229-0076. URL: https://www.accesson.kr/rks/assets/pdf/7510/journal-7-3-91.pdf (дата звернення: 03.08.2026).

33. Hallin D. C. The “Uncensored War”: The Media and Vietnam. Oxford : Oxford University Press, 1986. 285 p. ISBN 0-19-503814-2.

34. Westmoreland W. A Soldier Reports. Garden City (NY) : Doubleday, 1976. 446 p.

35. Knightley P. The First Casualty: The War Correspondent as Hero and Myth-Maker from the Crimea to Kosovo. London : Prion Books, 2000. xiii, 574 p.

36. Lasswell H. D. Propaganda Technique in the World War. Mansfield Centre : Martino Publishing, 2013. 244 p. URL: https://search.worldcat.org/title/892911929 (дата звернення: 15.05.2026).

37. Lippmann W. Public Opinion. Mineola : Dover Publications, 2004. 234 p. URL: https://search.worldcat.org/title/55208303 (дата звернення: 15.05.2026).

38. Gramsci A. Selections from the Prison Notebooks of Antonio Gramsci / ed. and transl. by Q. Hoare, G. Nowell-Smith. New York : International Publishers, 2008.

39. Cassirer E. The Myth of the State. New Haven : Yale University Press, 1961. 320 p.

40. Arendt H. The Origins of Totalitarianism. London : Penguin Classics, 2017. 752 p.

41. Foucault M. The Archaeology of Knowledge / transl. by A. M. Sheridan Smith. 2nd ed. London ; New York : Routledge, 2002. 256 p.

42. Ellul J. Propaganda: The Formation of Men’s Attitudes / transl. by K. Kellen, J. Lerner. New York : Vintage, 2021. 352 p.

43. Habermas J. The Structural Transformation of the Public Sphere: An Inquiry into a Category of Bourgeois Society / transl. by T. Burger. Hoboken : Wiley, 2015. 328 p.

44. Habermas J. The Theory of Communicative Action. Vol. 1: Reason and the Rationalization of Society / transl. by T. McCarthy. Cambridge : Polity, 2015. 512 p.

45. Heidegger M. The Question Concerning Technology, and Other Essays / transl. by W. Lovitt. New York : Harper Perennial, 2013. 224 p.

46. McLuhan M. Understanding Media: The Extensions of Man. 2nd ed. London : Routledge, 2001. 400 p.

47. Baudrillard J. Simulacra and Simulation / transl. by S. F. Glaser. Ann Arbor : University of Michigan Press, 1994. 320 p. DOI: 10.3998/mpub.9904.

48. Joint Chiefs of Staff. Joint Publication 3-13.1. Joint Doctrine for Command and Control Warfare (C2W). Washington, D.C., 7 February 1996. URL: https://www.bits.de/NRANEU/others/jp-doctrine/jp3_13_1.pdf (дата звернення: 03.08.2026).

49. Joint Chiefs of Staff. Joint Publication 3-13. Joint Doctrine for Information Operations. Washington, D.C., 9 October 1998. URL: https://nsarchive.gwu.edu/sites/default/files/documents/4936877/Joint-Chiefs-of-Staff-Joint-Publication-3-13.pdf (дата звернення: 03.08.2026).

50. Information Security Doctrine of the Russian Federation. Approved by President of the Russian Federation on 9 September 2000. URL: https://www.itu.int/en/ITU-D/Cybersecurity/Documents/National_Strategies_Repository/Russia_2000.pdf (дата звернення: 15.11.2024).

51. McDermott R. N. Does Russia Have a Gerasimov Doctrine? *Parameters*. 2016. Vol. 46, no. 1. P. 97–105. DOI: 10.55540/0031-1723.2827.

52. Galeotti M. Hybrid, ambiguous, and non-linear? How new is Russia's "new way of war"? *Small Wars & Insurgencies*. 2016. Vol. 27, no. 2. P. 282–301. DOI: 10.1080/09592318.2015.1129170.

53. Воєнні аспекти протидії «гібридній» агресії: досвід України : монографія / за заг. ред. А. М. Сиротенка. Київ : НУОУ ім. І. Черняховського, 2020. 176 с. URL: https://nuou.org.ua/assets/monography/mono_gibr_viin.pdf (дата звернення: 27.07.2025).

54. Hoffman F. G. Conflict in the 21st Century: The Rise of Hybrid Wars. Arlington, VA : Potomac Institute for Policy Studies, 2007. 72 p. URL: https://www.potomacinstitute.org/images/stories/publications/potomac_hybridwar_0108.pdf (дата звернення: 26.07.2024).

55. Paul C., Matthews M. The Russian “Firehose of Falsehood” Propaganda Model. Santa Monica : RAND Corporation, 2016. 16 p. DOI: 10.7249/PE198.

56. Blatny J. M., Søndergaard S. Cognitive Warfare: NATO Chief Scientist Research Report. Brussels : NATO Science & Technology Organization, 2025. 24 p. (STO-OCS-001). URL: https://www.nato.int/content/dam/nato/webready/documents/sto/chief-scientist-report-cognitive-warfare.pdf (дата звернення: 05.08.2026).

57. Aleksejeva N. et al. Narrative Warfare: How the Kremlin and Russian News Outlets Justified a War of Aggression against Ukraine / research coordinated by N. Aleksejeva ; ed. by A. Carvin. Washington, DC : Atlantic Council, 2023. 54 p. URL: https://www.atlanticcouncil.org/wp-content/uploads/2023/02/Narrative-Warfare-Final.pdf (дата звернення: 03.08.2026).

58. Osadchuk R. et al. Undermining Ukraine: How the Kremlin Employs Information Operations to Erode Global Confidence in Ukraine / research coordinated by R. Osadchuk ; ed. by A. Carvin. Washington, DC : Atlantic Council, 2023. 38 p. URL: https://www.atlanticcouncil.org/wp-content/uploads/2023/02/Undermining-Ukraine-Final.pdf (дата звернення: 03.08.2026).

59. Deppe C., Schaal G. S. Cognitive warfare: a conceptual analysis of the NATO ACT cognitive warfare exploratory concept. *Frontiers in Big Data*. 2024. Vol. 7. Art. 1452129. DOI: 10.3389/fdata.2024.1452129.

60. Palmertz B., Weissmann M., Nilsson N., Engvall J. Building Resilience and Psychological Defence: An Analytical Framework for Countering Hybrid Threats and Foreign Influence and Interference. Lund : Lund University Psychological Defence Research Institute, 2024. Working Paper 2024:1. URL: https://mpf.se/download/18.7bb35f1818ec664dc7a4664/1712909687772/buidling-resilience-and-psychological-defence.pdf (дата звернення: 03.08.2026).

61. Lange L. Decoding China’s AI-Powered “Algorithmic Cognitive Warfare”. Special Competitive Studies Project, 2024. 11 p. URL: https://www.scsp.ai/wp-content/uploads/2024/11/Decoding-Chinas-AI-

Powered-%E2%80%98Algorithmic-Cognitive-Warfare-Final.pdf (дата звернення: 03.08.2026).

62. 21st Century Fog of War: Information Warfare and the Battle for Perception. Norwich University. 2024. 14 October. URL: https://www.norwich.edu/news/21st-century-fog-war-information-warfare-and-battle-perception (дата звернення: 03.08.2026).

63. Почепцов Г. Війна в когнітивному просторі. *Журнал «Ї»*. 2017. URL: http://www.ji-magazine.lviv.ua/2017/Pocheptsov_Vijna_v_kognityvnomu_prostori.htm (дата звернення: 27.07.2024).

64. Зеленін В. В. Психосемантика міфодизайну: до питання інформаційної безпеки. *Медіапсихологія: теорія і практика* : тези доповідей V Всеукраїнської науково-практичної конференції. Київ : Ін-т соц. та політ. психології НАПН України, 2020. URL: https://mediaosvita.org.ua/wp-content/uploads/2020/07/Zelenin_VV-Psyhosemantyka-mifodyzajnu_tezy.pdf (дата звернення: 08.03.2025).

65. Максименко С., Назар М., Ірхін Ю. Інформаційно-психологічні засади ментального протистояння російської агресії в гібридній війні : наук. дослідж. Київ : Вид-во Людмила, 2024. 91 с.

66. Золотухін Д. Як перемогти в інфовійні? : інтерв'ю / канал «РІЗНІ ЛЮДИ». YouTube. 2024. 17 вер. URL: https://www.youtube.com/watch?v=IScYfB6D00Q (дата звернення: 30.09.2024).

67. Каптан М. В. Удосконалення мережі ситуаційних центрів у сфері інформаційної безпеки України. *Аналітично-порівняльне правознавство*. 2023. № 3. С. 279–287. DOI: 10.24144/2788-6018.2023.03.51.

68. Боротьба з російською брехнею та формування позиції держави: підсумки роботи Центру стратегічних комунікацій у 2024 році. Центр стратегічних комунікацій та інформаційної безпеки. 2024. URL: https://spravdi.gov.ua/borotba-z-rosijskoyu-brehneyu-ta-formuvannya-pozycziyi-

derzhavy-pidsumky-roboty-czentru-strategichnyh-komunikaczij-u-2024-roczi/ (дата звернення: 03.08.2026).

69. FIMI в Україні: комунікаційники МВС покращили знання щодо методів протидії іноземним маніпуляціям в інфопросторі. Міністерство внутрішніх справ України. 2025. 26 лют. URL: https://mvs.gov.ua/news/fimi-in-ukraine-komunikaciiniki-mvs-pokrashhili-znannia-shhodo-metodiv-protidiyi-inozemnim-manipuliaciiam-v-infoprostori (дата звернення: 03.08.2026).

70. Савчук В. А. Інформаційна складова сучасних воєн у політологічному дискурсі: зарубіжний та український контексти. *Епістемологічні дослідження в філософії, соціальних і політичних науках*. 2025. Т. 8, № 2. С. 198–203. DOI: 10.15421/342557.

71. Осадчук І. Ю. Методичні рекомендації та матеріали для вивчення навчальної дисципліни «Теорія політики». Львів, 2024–2025 н. р. 18 с. URL: https://filos.lnu.edu.ua/wp-content/uploads/2025/02/Metodychni-rekomendatsii_Teoriia-polityky_2024-2025.pdf (дата звернення: 05.03.2025).

72. Deepfake Zelenskyy Surrender Video Is the “First Intentionally Used” in Ukraine War. Euronews. 2022. 16 March. URL: https://www.euronews.com/my-europe/2022/03/16/deepfake-zelenskyy-surrender-video-is-the-first-intentionally-used-in-ukraine-war (дата звернення: 03.08.2026).

73. United Nations Security Council. S/PV.8999: Maintenance of Peace and Security of Ukraine. New York, 2022. 11 March. URL: https://docs.un.org/en/S/PV.8999 (дата звернення: 03.08.2026).

74. Nimmo B., François C., Eib C. S., Ronzaud L., Ferreira R., Hernon C., Kostelancik T. Exposing Secondary Infektion: Forgeries, Interference, and Attacks on Kremlin Critics Across Six Years and 300 Sites and Platforms. Graphika. 2020. URL: https://www.graphika.com/reports/exposing-secondary-infektion/ (дата звернення: 01.07.2026).

75. Almond G. A. Comparative Political Systems. *The Journal of Politics*. 1956. Vol. 18, no. 3. P. 391–409. DOI: 10.2307/2127255.

76. Collier D. The Comparative Method. *Political Science: The State of the Discipline II* / ed. by A. W. Finifter. Washington, DC : American Political Science Association, 1993. P. 105–119.

77. Зеленін В. Чому ми програємо інформвійну? : інтерв'ю / канал «РІЗНІ ЛЮДИ». YouTube. 2024. 22 жовт. URL: https://www.youtube.com/watch?v=nohtX4gC01A (дата звернення: 15.11.2024).

78. Ягодзінський С. Українська філософія, хейт, війна : інтерв'ю / канал «РІЗНІ ЛЮДИ». YouTube. 2024. 29 жовт. URL: https://www.youtube.com/watch?v=wMRwLMfcrvQ (дата звернення: 20.11.2024).

79. Харебін О. Зеленский бросил вызов! Как Евросоюзу не проиграть? В чем интерес Трампа? Фиаско Путина. Харебин : інтерв'ю / канал «РІЗНІ ЛЮДИ». YouTube. 2025. 26 лют. URL: https://www.youtube.com/watch?v=UggCBBBJleI (дата звернення: 28.09.2026).

80. Саакян О. Політолог Олег Саакян: війна, мир і стратегія України : інтерв'ю / канал «РІЗНІ ЛЮДИ». YouTube. 2024. 19 лист. URL: https://www.youtube.com/watch?v=eYDLGLZp9eM (дата звернення: 10.12.2024).

81. Клімкін П. Як захистити міста від дронів? : інтерв'ю / канал «РІЗНІ ЛЮДИ». YouTube. 2024. 25 лист. URL: https://www.youtube.com/watch?v=9NDt1RUo23I (дата звернення: 15.12.2024).

82. Палій О. Українське кіно: про збоченців чи про перемоги? Ми всі скіфи : інтерв'ю / канал «РІЗНІ ЛЮДИ». YouTube. 2024. 3 груд. URL: https://www.youtube.com/watch?v=FkeTJgkgNnk (дата звернення: 25.12.2024).

83. Савчук В. А. Інформаційні війни як об'єкт міждисциплінарних наукових досліджень. *Сучасна наука: дослідження, економіка та інновації* : зб. наук. праць за матеріалами 3-ї Міжнар. наук.-практ. конф. (Загреб, Хорватія, 22–24 жовт. 2025 р.). Загреб, 2025. С. 282–284. URL: https://isu-conference.com/en/archive/modern-science-research-economy-and-innovation-22-10-25 (дата звернення: 07.08.2026).

84. Осадчук І. Ю. Методичні рекомендації та матеріали для вивчення навчальної дисципліни «Методологія політичних досліджень». Львів, 2024–2025

н. р. 18 с. URL: https://filos.lnu.edu.ua/wp-content/uploads/2024/09/Metodychni-rekomendatsii_Metodolohiia-politychnykh-doslidzhen_2024-2025.pdf (дата звернення: 10.02.2025).

85. Allied Joint Doctrine for Strategic Communications (AJP-10). Edition A, Version 1, with UK national elements (Change 1). NATO Standardization Office, 2023. 184 p. URL: https://assets.publishing.service.gov.uk/media/6525459d244f8e00138e7343/AJP_10_Strat_Comm_Change_1_web.pdf (дата звернення: 15.01.2024).

86. Wardle C., Derakhshan H. Information Disorder: Toward an Interdisciplinary Framework for Research and Policy Making. Revised ed. Strasbourg : Council of Europe, 2018. 112 p. URL: https://rm.coe.int/Report-D/09000016807bf5f6 (дата звернення: 20.02.2024).

87. Roozenbeek J., van der Linden S., Nygren T. Prebunking interventions based on “inoculation” theory can reduce susceptibility to misinformation across cultures. *The Harvard Kennedy School Misinformation Review*. 2020. Vol. 1, issue 2. DOI: 10.37016/mr-2020-008.

88. Про основні засади забезпечення кібербезпеки України : Закон України від 05 жовт. 2017 р. № 2163-VIII. База даних «Законодавство України» / Верховна Рада України. URL: https://zakon.rada.gov.ua/go/2163-19 (дата звернення: 13.01.2026).

89. Савчук В. А. Когнітивна війна: теоретичні засади та інституційна практика. *Регіональні студії*. 2025. № 42. С. 154–160. DOI: 10.32782/2663-6170/2025.42.24.

90. Почепцов Г. З історії поняття гібридної війни в США і Росії. Детектор медіа (MediaSapiens). 01.11.2015. URL: https://ms.detector.media/mediaanalitika/post/14619/2015-11-01-z-istorii-ponyattya-gibrydnoi-viyny-v-ssha-i-rosii/ (дата звернення: 13.02.2026).

91. Курбан О. В. Інформаційне супроводження російської гібридної агресії в Донбасі (2014–2016). *Бібліотекознавство. Документознавство.*

Інформологія. 2017. № 2. С. 66–73. URL: http://nbuv.gov.ua/UJRN/bdi_2017_2_11 (дата звернення: 15.03.2024).

92. Countering Cognitive Warfare. NATO Innovation Hub, 08.10.2021. URL: https://www.act.nato.int/article/nato-innovation-challenge-fall-2021-countering-cognitive-warfare/ (дата звернення: 13.02.2026).

93. Claverie B., du Cluzel F. The Cognitive Warfare Concept. NATO ACT Innovation Hub, 2021. 11 p. URL: https://innovationhub-act.org/wp-content/uploads/2023/12/CW-article-Claverie-du-Cluzel-final_0.pdf (дата звернення: 13.02.2026).

94. Yang Cunshe. Accurately Grasping the Pulse of Cognitive Domain Operations: An Analysis of the Characteristics and Development Trends of Cognitive Domain Operations. PLA Daily. 16.08.2022. URL: http://www.81.cn/jfjbmap/content/2022-08/16/content_322064.htm (дата звернення: 13.02.2026).

95. Arthur G. China's PLA Reshapes to Deliver 'Intelligentisation'. *Asian Military Review*. 06.11.2024. URL: https://www.asianmilitaryreview.com/2024/11/chinas-pla-reshapes-to-deliver-intelligentisation/ (дата звернення: 13.02.2026).

96. Золотухін Д. Когнітивна війна: новомодне словосполучення чи концепція шостого поля бою. Детектор медіа. 06.07.2021. URL: https://detector.media/infospace/article/189826/2021-07-06-kognityvna-viyna-novomodne-slovospoluchennya-chy-kontseptsiya-shostogo-polya-boyu/ (дата звернення: 03.03.2025).

97. Kahneman D. Thinking, Fast and Slow. New York : Farrar, Straus & Giroux, 2011. 499 p.

98. Hasher L., Goldstein D., Toppino T. Frequency and the Conference of Referential Validity. *Journal of Verbal Learning and Verbal Behavior*. 1977. Vol. 16, no. 1. P. 107–112. DOI: 10.1016/S0022-5371(77)80012-1.

99. Fazio L. K., Brashier N. M., Payne B. K., Marsh E. J. Knowledge Does Not Protect Against Illusory Truth. *Journal of Experimental Psychology: General*. 2015. Vol. 144, no. 5. P. 993–1002. DOI: 10.1037/xge0000098.

100. Pennycook G., Cannon T. D., Rand D. G. Prior Exposure Increases Perceived Accuracy of Fake News. *Journal of Experimental Psychology: General*. 2018. Vol. 147, no. 12. P. 1865–1880. DOI: 10.1037/xge0000465.

101. Chiossi F., Haliburton L., Ou C., Butz A., Schmidt A. Short-Form Videos Degrade Our Capacity to Retain Intentions: Effect of Context Switching on Prospective Memory. *Proceedings of the 2023 CHI Conference on Human Factors in Computing Systems*. New York : Association for Computing Machinery, 2023. P. 1–15. DOI: 10.1145/3544548.3580778.

102. Thaler R., Sunstein C. Nudge: Improving Decisions about Health, Wealth, and Happiness. New Haven : Yale University Press, 2008. 312 p.

103. Kensinger E. A. Remembering the Details: Effects of Emotion. *Emotion Review*. 2009. Vol. 1, no. 2. P. 99–113. DOI: 10.1177/1754073908100432.

104. Hassan A., Barber S. J. The effects of repetition frequency on the illusory truth effect. *Cognitive Research: Principles and Implications*. 2021. Vol. 6, art. 38. P. 1–12. DOI: 10.1186/s41235-021-00301-5.

105. Su C., Zhou H., Gong L., Teng B., Geng F., Hu Y. Viewing Personalized Video Clips Recommended by TikTok Activates Default Mode Network and Ventral Tegmental Area. *NeuroImage*. 2021. Vol. 237. Art. 118136. DOI: 10.1016/j.neuroimage.2021.118136.

106. Geissler D., Bär D., Pröllochs N., Feuerriegel S. Russian propaganda on social media during the 2022 invasion of Ukraine. *EPJ Data Science*. 2023. Vol. 12. Article 35. DOI: 10.1140/epjds/s13688-023-00414-5.

107. Osadchuk R. Massive Russian influence operation targeted former Ukrainian defense minister on TikTok. Digital Forensic Research Lab. 2023. URL: https://dfrlab.org/2023/12/14/massive-russian-influence-operation-targeted-former-ukrainian-defense-minister-on-tiktok/ (дата звернення: 01.07.2026).

108. Undermining Ukraine: How Russia widened its global information war in 2023 / Digital Forensic Research Lab. Atlantic Council. 2024. URL: https://www.atlanticcouncil.org/in-depth-research-reports/report/undermining-ukraine-how-russia-widened-its-global-information-war-in-2023/ (дата звернення: 01.07.2026).

109. Edgar J. L. The Role of Special Operations Forces in Information Warfare: Enablers, Not Cyber Warriors. Newport : Naval War College, 2000. 26 p.

110. Про Доктрину інформаційної безпеки України : Указ Президента України; Доктрина від 08.07.2009 № 514/2009. База даних «Законодавство України» / Верховна Рада України. URL: https://zakon.rada.gov.ua/go/514/2009 (дата звернення: 03.08.2026).

111. Основи протидії інформаційно-психологічному впливові в особливий період : навч.-метод. посіб. / П. П. Ткачук, В. В. Шемчук, Ю. П. Сальник та ін. Львів : НАСВ, 2015. 189 с.

112. Allied Joint Doctrine for Psychological Operations (AJP-3.10.1). Edition B, Version 1. Brussels : NATO Standardization Office, 2014. 89 p. URL: https://www.gov.uk/government/publications/ajp-3101-allied-joint-doctrine-for-psychological-operations (дата звернення: 03.08.2026).

113. Почепцов Г. Г. Сучасні інформаційні війни. 2-ге вид., допов. Київ : Києво-Могилянська академія, 2016. 504 с.

114. Domańska M., Żochowski P. Putin’s article: ‘On the historical unity of Russians and Ukrainians’. Centre for Eastern Studies. 2021. URL: https://www.osw.waw.pl/en/publikacje/analyses/2021-07-13/putins-article-historical-unity-russians-and-ukrainians (дата звернення: 01.07.2026).

115. Belton C. Kremlin runs covert disinformation campaign to undermine Zelensky, documents show. *The Washington Post*. 2024. 16 February. URL: https://www.washingtonpost.com/world/2024/02/16/russian-disinformation-zelensky-zaluzhny (дата звернення: 01.07.2026).

116. Hunder M. Russia vs Ukraine: the Biggest War of the Fake News Era. Reuters. 2024. 31 July. URL: https://www.reuters.com/world/europe/russia-vs-ukraine-biggest-war-fake-news-era-2024-07-31/ (дата звернення: 01.07.2026).

117. Paul C., Schwille M. The Evolution of Special Operations as a Model for Information Forces. *Joint Force Quarterly*. 2021. № 100. P. 8–13. URL: https://ndupress.ndu.edu/Portals/68/Documents/jfq/jfq-100/jfq-100_8-13_Paul-Schwille.pdf (дата звернення: 08.03.2026).

118. Суд у Києві засудив Мединського до 10 років за пропагандистський підручник з історії. Інститут масової інформації (IMI) : вебсайт. 2026. 8 травня. URL: https://imi.org.ua/news/peregovornyk-rf-medynskyj-otrymav-10-rokiv-za-pidruchnyk-shcho-vypravdovuvav-vijnu-proty-ukrayiny (дата звернення: 19.05.2026).

119. Portal Kombat : un réseau structuré et coordonné de propagande prorusse / VIGINUM ; Secrétariat général de la défense et de la sécurité nationale (SGDSN). Rapport technique. 12 février 2024. URL: https://www.sgdsn.gouv.fr/viginum/publications/portal-kombat-un-reseau-structure-et-coordonne-de-propagande-prorusse (дата звернення: 19.05.2026).

120. Faou M. Operation Texonto: Information operation targeting Ukrainian speakers in the context of the war. ESET Research. 21 Feb. 2024. URL: https://www.welivesecurity.com/en/eset-research/operation-texonto-information-operation-targeting-ukrainian-speakers-context-war/ (дата звернення: 19.05.2026).

121. Новицька Н. Б., Петрик В. М., Кудико В. М. Пропаганда, диверсифікація громадської думки, психологічний тиск та поширення чуток як методи ведення спеціальних інформаційних операцій рф проти України. *Ірпінський юридичний часопис*. 2022. Вип. 2(9). С. 105–113. DOI: 10.33244/2617-4154-2(9)-2022-105-113.

122. Lefebvre V. A., Farley J. D. The Torturer’s Dilemma: A Theoretical Analysis of the Societal Consequences of Torturing Terrorist Suspects. *Studies in Conflict & Terrorism*. 2007. Vol. 30, no. 7. P. 635–646. DOI: 10.1080/10576100701385974.

123. Lefebvre V. A. Algebra of Conscience: A Comparative Analysis of Western and Soviet Ethical Systems. Dordrecht : D. Reidel Publishing Company, 1982. 194 p. DOI: 10.1007/978-94-010-9051-3.

124. Thomas T. L. Russia's Reflexive Control Theory and the Military. *The Journal of Slavic Military Studies*. 2004. Vol. 17, no. 2. P. 237–256. DOI: 10.1080/13518040490450529.

125. BIS odhalila ruskou vlivovou síť. Aktéři skončili na sankčním seznamu / Bezpečnostní informační služba. 28.03.2024. URL: https://www.bis.cz/aktuality/bis-odhalila-ruskou-vlivovou-sit-akteri-skoncili-na-sankcnim-seznamu-ff8aacba.html (дата звернення: 19.05.2026).

126. Information manipulation in Russia's war of aggression against Ukraine: EU lists two individuals and one entity / Council of the European Union. 27.05.2024. URL: https://www.consilium.europa.eu/en/press/press-releases/2024/05/27/information-manipulation-in-russia-s-war-of-aggression-against-ukraine-eu-lists-two-individuals-and-one-entity/ (дата звернення: 19.05.2026).

127. Kulchynsky R., Pastukh H., Dukach Yu., Mikhalkov S., Herasymenko V., Kelm N., Drozdova Ye. The Piggyback Trick: How YouTube Algorithms Promote Conspirology and Propaganda. Texty.org.ua. 28.11.2023. URL: https://texty.org.ua/d/2023/youtube-recommendations/en/ (дата звернення: 19.05.2026).

128. Naidon Y., Naumiuk S., Rybynskyi Y., Kravchenko O., Buriak N. Destructive information influence and its implementation. *Amazonia Investiga*. 2022. Vol. 11, iss. 58. P. 65–73. DOI: 10.34069/AI/2022.58.10.7.

129. Danyk Y., Briggs C. M. Modern Cognitive Operations and Hybrid Warfare. *Journal of Strategic Security*. 2023. Vol. 16, no. 1. P. 35–50. DOI: 10.5038/1944-0472.16.1.2032.

130. Fake: Ukrainian Commander-in-Chief Zaluzhny Is Preparing a Military Coup / StopFake. 08.11.2023. URL: https://www.stopfake.org/en/fake-ukrainian-commander-in-chief-zaluzhny-is-preparing-a-military-coup/ (дата звернення: 19.05.2026).

131. Disinfo: The Ukrainian trident is a Nazi symbol / EUvsDisinfo. 06.01.2025. URL: https://euvsdisinfo.eu/report/the-ukrainian-trident-is-a-nazi-symbol/ (дата звернення: 19.05.2026).

132. Нетеса Н. В., Мокляк В. В. Спеціальні інформаційні операції проти України як елемент гібридної війни та напрями протидії їм. *Інформація і право*. 2023. № 3(46). С. 98–107. DOI: 10.37750/2616-6798.2023.3(46).287168.

133. IAEA Inspectors Complete In-Field Verification Activities at Three Ukraine locations, No Indications of Undeclared Nuclear Activities and Materials / International Atomic Energy Agency. 03.11.2022. URL: https://www.iaea.org/newscenter/pressreleases/iaea-inspectors-complete-in-field-verification-activities-at-three-ukraine-locations-no-indications-of-undeclared-nuclear-activities-and-materials (дата звернення: 19.05.2026).

134. Key narratives in pro-Kremlin disinformation: “Nazis” / EUvsDisinfo. 25.11.2022. URL: https://euvsdisinfo.eu/key-narratives-in-pro-kremlin-disinformation-nazis/ (дата звернення: 19.05.2026).

135. Верголяс О. О. Інформаційно-правове забезпечення спеціальних інформаційних операцій. *Інформація і право*. 2018. № 4(27). С. 126–133. DOI: 10.37750/2616-6798.2018.4(27).273376.

136. СБУ повідомила про підозру Діані Панченко, яка виправдовує збройну агресію РФ проти України : офіційне повідомлення Служби безпеки України. 2023. 24 січня. URL: https://ssu.gov.ua/news/sbu-povidomyla-pro-pidozru-diani-panchenko-yaka-vypravdovuie-zbroinu-ahresiiu-rf-proty-ukrainy (дата звернення: 19.05.2026).

137. СБУ заблокувала спроби спецслужб РФ створити фейкові «народні ради» для дестабілізації ситуації в регіонах : офіційне повідомлення Служби безпеки України. 2016. 14 квітня. URL: https://ssu.gov.ua/news/sbu-zablokuvala-sproby-spetssluzhb-rf-stvoryty-feikovi-narodni-rady-dlia-destabilizatsii-sytuatsii-v-rehionakh (дата звернення: 19.05.2026).

138. European External Action Service. 2nd EEAS Report on Foreign Information Manipulation and Interference Threats. 2024. URL:

https://www.eeas.europa.eu/sites/default/files/documents/2024/EEAS-2nd-Report%20on%20FIMI%20Threats-January-2024_0.pdf (дата звернення: 19.08.2026).

139. Grahn H., Pamment J. Exploitation of Psychological Processes in Information Influence Operations: Insights from Cognitive Science. Lund : Lund University Psychological Defence Research Institute, 2024. Working Paper 2024:4. 20 p. ISBN 978-91-8104-329-7. URL: https://www.psychologicaldefence.lu.se/sites/psychologicaldefence.lu.se/files/2024-12/241206_LU%20Working%20Paper%202024-4_Exploitation%20of%20psychological%20processes%20in%20information%20influence%20operations_0.pdf (дата звернення: 04.08.2026).

140. Anniversary: “The crucified boy” turns two / EUvsDisinfo. 2016. 15 July. URL: https://euvsdisinfo.eu/anniversary-the-crucified-boy-turns-two/ (дата звернення: 04.08.2026).

141. Semeniuk N. Cognitive Warfare in the Modern Architecture of Hybrid Warfare. *Military Science*. 2024. Vol. 2, no. 3. P. 99–107. DOI: 10.62524/msj.2024.2.3.08.

142. Панченко В. М. Інформаційні операції в системі стратегічних комунікацій. *Стратегічні пріоритети. Серія: Політика*. 2016. № 4. С. 72–79. URL: http://nbuv.gov.ua/UJRN/sppol_2016_4_11 (дата звернення: 15.01.2024).

143. Ensuring accountability for the downing of flight MH17 : report / Parliamentary Assembly of the Council of Europe. Doc. 15543. Strasbourg, 2022. 13 p. URL: https://pace.coe.int/en/files/30063/html (дата звернення: 04.08.2026).

144. Молчанова М. О. Нейромережеве виявлення і класифікація прийомів та об’єктів пропаганди у текстовому контенті. *Вимірювальна та обчислювальна техніка в технологічних процесах*. 2024. № 4. С. 153–161. DOI: 10.31891/2219-9365-2024-80-19.

145. Helmus T. C., Holynska K. Ukrainian Resistance to Russian Disinformation: Lessons for Future Conflict. Santa Monica, CA : RAND Corporation, 2024. 96 p. DOI: 10.7249/RRA2771-1.

146. Савчук В. А. Інструменти виявлення та подолання деструктивних впливів та пропагандистських наративів інформаційних операцій: типологія, основні характеристики. *Актуальні проблеми філософії та соціології*. 2025. Вип. 54. С. 224–229. DOI: 10.32782/apfs.v054.2025.33.

147. Barrón-Cedeño A., Da San Martino G., Jaradat I., Nakov P. Proppy: A System to Unmask Propaganda in Online News. *Proceedings of the AAAI Conference on Artificial Intelligence*. 2019. Vol. 33, no. 1. P. 9847–9848. DOI: 10.1609/aaai.v33i01.33019847.

148. Liu Y., Ott M., Goyal N. et al. RoBERTa: A Robustly Optimized BERT Pretraining Approach. arXiv preprint. 2019. 13 p. DOI: 10.48550/arXiv.1907.11692.

149. Kuntur S., Krzywda M., Wróblewska A., Paprzycki M., Ganzha M. Comparative Analysis of Graph Neural Networks and Transformers for Robust Fake News Detection: A Verification and Reimplementation Study. *Electronics*. 2024. Vol. 13, no. 23. Art. 4784. DOI: 10.3390/electronics13234784.

150. Truică C.-O., Apostol E.-S. MisRoBÆRTa: Transformers versus Misinformation. *Mathematics*. 2022. Vol. 10, no. 4. Art. 569. DOI: 10.3390/math10040569.

151. Jiang B. et al. Disinformation Detection: An Evolving Challenge in the Age of LLMs. *Proceedings of the 2024 SIAM International Conference on Data Mining*. 2024. P. 427–435. DOI: 10.1137/1.9781611978032.50.

152. Zavolokina L., Sprenkamp K., Katashinskaya Z., Jones D. G., Schwabe G. Think Fast, Think Slow, Think Critical: Designing an Automated Propaganda Detection Tool. *Proceedings of the CHI Conference on Human Factors in Computing Systems (CHI ’24)*. New York : ACM, 2024. Art. 491. 24 p. DOI: 10.1145/3613904.3642805.

153. Wei J., Wang X., Schuurmans D. et al. Chain-of-Thought Prompting Elicits Reasoning in Large Language Models. *Advances in Neural Information Processing Systems*. 2022. Vol. 35. P. 24824–24837.

154. Indiana University. Tracking Coordinated Disinformation Campaigns Online Made Easier with New BotSlayer Tool. Indiana University News. 2019. 12

Sept. URL: https://news.iu.edu/live/news/26311-tracking-coordinated-disinformation-campaigns (дата звернення: 04.08.2026).

155. Gong J., Peng J., Qu J., Du S., Wang K. Enhancing Twitter Bot Detection via Multimodal Invariant Representations. arXiv preprint. 2024. DOI: 10.48550/arXiv.2408.03096.

156. Peng H., Zhang J., Huang X. et al. Unsupervised Social Bot Detection via Structural Information Theory. arXiv preprint. 2024. DOI: 10.48550/arXiv.2404.13595.

157. Vastel A. Bot Detection 101: How to Detect Bots in 2025? The Castle Blog. 2025. 25 Mar. URL: https://blog.castle.io/bot-detection-101-how-to-detect-bots-in-2025-2/ (дата звернення: 04.08.2026).

158. Van der Linden S. Misinformation: Susceptibility, Spread, and Interventions to Immunize the Public. *Nature Medicine*. 2022. Vol. 28. P. 460–467. DOI: 10.1038/s41591-022-01713-6.

159. McPhedran R., Ratajczak M., Mawby M. et al. Psychological Inoculation Protects against the Social Media Infodemic. *Scientific Reports*. 2023. Vol. 13. Art. 5780. DOI: 10.1038/s41598-023-32962-1.

160. Fact Check Ratings. Snopes. URL: https://www.snopes.com/fact-check-ratings/ (дата звернення: 04.08.2026).

161. The Commitments of the Code of Principles. International Fact-Checking Network. URL: https://ifcncodeofprinciples.poynter.org/the-commitments (дата звернення: 04.08.2026).

162. What Is OSINT: Open-Source Intelligence? Official Portal for European Data. 2023. 24 Jan. URL: https://data.europa.eu/en/publications/datastories/what-osint-open-source-intelligence (дата звернення: 04.08.2026).

163. Bellingcat Investigation Team. Hospitals Bombed and Apartments Destroyed: Mapping Incidents of Civilian Harm in Ukraine. Bellingcat. 2022. 17 Mar. URL: https://www.bellingcat.com/news/2022/03/17/hospitals-bombed-and-apartments-destroyed-mapping-incidents-of-civilian-harm-in-ukraine/ (дата звернення: 04.08.2026).

164. StopFake.org – IFCN Code of Principles. Poynter / International Fact-Checking Network. URL: https://ifcncodeofprinciples.poynter.org/application/public/stopfakeorg/661a8b14ba7689d481433f78 (дата звернення: 14.02.2026).

165. Про VoxCheck. VoxUkraine. URL: https://voxcheck.voxukraine.org/ (дата звернення: 14.02.2026).

166. MIT Sloan Office of Communications. Warning Labels from Fact-Checkers Work Even If You Don’t Trust Them. MIT Sloan Ideas Made to Matter. 2024. 2 Sept. URL: https://mitsloan.mit.edu/press/warning-labels-fact-checkers-work-even-if-you-dont-trust-them (дата звернення: 07.08.2025).

167. Adam D. Does Fact-Checking Work? What the Science Says. *Nature*. 2025. 10 Jan. DOI: 10.1038/d41586-025-00027-0.

168. Putin’s New Plan to Undermine Fact-Checking. European Digital Media Observatory. 2024. 29 Nov. URL: https://edmo.eu/publications/putins-new-plan-to-undermine-fact-checking/ (дата звернення: 07.08.2025).

169. Russia: Fact-Checking Is the Kremlin’s Latest Propaganda Tool. Reporters Without Borders. 2025. 24 June. URL: https://rsf.org/en/russia-fact-checking-kremlins-latest-propaganda-tool (дата звернення: 07.08.2025).

170. Fact Check Explorer. Google Fact Check Tools. URL: https://toolbox.google.com/factcheck/explorer (дата звернення: 04.08.2026).

171. Fact Check Markup Tool. Google Fact Check Tools. URL: https://toolbox.google.com/factcheck/markuptool (дата звернення: 04.08.2026).

172. Fact Check (ClaimReview) Structured Data. Google for Developers. URL: https://developers.google.com/search/docs/appearance/structured-data/factcheck (дата звернення: 04.08.2026).

173. Fake News Debunker InVID WeVerify VeraAI. Chrome Web Store. URL: https://chromewebstore.google.com/detail/fake-news-debunker-by-inv/mhccpoafgdgbhnjfhkcmgknndkeenfhe (дата звернення: 04.08.2026).

174. Deepware Scanner. Deepware. URL: https://deepware.ai (дата звернення: 04.08.2026).

175. AI-Generated & Deepfake Content Detection. Hive. URL: https://thehive.ai/apis/ai-generated-content-classification (дата звернення: 04.08.2026).

176. TinEye Reverse Image Search. TinEye. URL: https://tineye.com/ (дата звернення: 04.08.2026).

177. Koettl C. Real vs. Fake: How to Authenticate YouTube Videos for Human Rights Work. Amnesty International. 2014. 8 July. URL: https://www.amnesty.org/en/latest/campaigns/2014/07/real-vs-fake-how-to-authenticate-youtube-videos-for-human-rights-work/ (дата звернення: 04.08.2026).

178. Newman N., Fletcher R., Robertson C. T., Ross Arguedas A., Nielsen R. K. Reuters Institute Digital News Report 2025. Oxford : Reuters Institute for the Study of Journalism, 2025. 17 June. URL: https://reutersinstitute.politics.ox.ac.uk/sites/default/files/2025-06/Digital_News-Report_2025.pdf (дата звернення: 04.08.2026).

179. Голуб О. Соціальні мережі, які диктують ритм новин. Дослідження IMI. Інститут масової інформації. 11.12.2024. URL: https://imi.org.ua/monitorings/sotsialni-merezhi-yaki-dyktuyut-rytm-novyn-doslidzhennya-imi-i65389 (дата звернення: 14.02.2026).

180. Дослідження: Telegram залишається для українців основною соцмережею для спілкування та новин. Інститут масової інформації. 07.11.2024. URL: https://imi.org.ua/news/doslidzhennya-telegram-zalyshayetsya-dlya-ukrayintsiv-osnovnoyu-sotsmerezheyu-dlya-spilkuvannya-ta-i64761 (дата звернення: 04.08.2026).

181. Brady W. J. et al. Emotion shapes the diffusion of moralized content in social networks. *Proceedings of the National Academy of Sciences*. 2017. Vol. 114, no. 28. P. 7313–7318. DOI: 10.1073/pnas.1618923114.

182. NATO Strategic Communications Centre of Excellence. Social Media Manipulation 2022/2023: Assessing the Ability of Social Media Companies to Combat Platform Manipulation. Riga, 2023. 20 p. ISBN 978-9934-619-32-8. URL: https://stratcomcoe.org/publications/social-media-manipulation-20222023-assessing-

the-ability-of-social-media-companies-to-combat-platform-manipulation/272 (дата звернення: 14.02.2026).

183. Vosoughi S., Roy D., Aral S. The spread of true and false news online. *Science*. 2018. Vol. 359, no. 6380. P. 1146–1151. DOI: 10.1126/science.aap9559.

184. Karlsen R., Aalberg T. Social Media and Trust in News: An Experimental Study of the Effect of Facebook on News Story Credibility. *Digital Journalism*. 2023. Vol. 11, no. 1. P. 144–160. DOI: 10.1080/21670811.2021.1945938.

185. McCombs M., Shaw D. The Agenda-Setting Function of Mass Media. *Public Opinion Quarterly*. 1972. Vol. 36, no. 2. P. 176–187. DOI: 10.1086/267990.

186. Entman R. M. Framing: Toward Clarification of a Fractured Paradigm. *Journal of Communication*. 1993. Vol. 43, no. 4. P. 51–58. DOI: 10.1111/j.1460-2466.1993.tb01304.x.

187. Noelle-Neumann E. The Spiral of Silence: Public Opinion – Our Social Skin. Chicago : University of Chicago Press, 1984. URL: https://archive.org/details/spiralofsilencep0000noel (дата звернення: 14.02.2026).

188. Балабанова К. Аналіз тенденцій медіаспоживання в Україні за 2022–2024 роки. *Інтегровані комунікації*. 2024. № 1 (17). С. 32–36. DOI: 10.28925/2524-2644.2024.173.

189. Павленко Д. Динаміка сучасних соціальних медіа в Україні в контексті підтримки інформаційної безпеки. *Наукові праці Національної бібліотеки України імені В. І. Вернадського*. 2023. Вип. 67. С. 108–117. DOI: 10.15407/np.67.108.

190. Kemp S. Digital 2025: Ukraine. DataReportal. 03.03.2025. URL: https://datareportal.com/reports/digital-2025-ukraine (дата звернення: 04.08.2026).

191. Telegram FAQ. Telegram. URL: https://telegram.org/faq (дата звернення: 04.08.2026).

192. Telegram FAQ for the Technically Inclined. Telegram. URL: https://core.telegram.org/techfaq (дата звернення: 04.08.2026).

193. La Morgia M., Mei A., Mongardini A. M., Wu J. Uncovering the Dark Side of Telegram: Fakes, Clones, Scams, and Conspiracy Movements. arXiv preprint, 2021. arXiv:2111.13530. DOI: 10.48550/arXiv.2111.13530.

194. Guess A., Nagler J., Tucker J. Less than you think: Prevalence and predictors of fake news dissemination on Facebook. *Science Advances*. 2019. Vol. 5, no. 1. Art. eaau4586. DOI: 10.1126/sciadv.aau4586.

195. Google Threat Analysis Group. TAG Bulletin: Q1 2025. 15.05.2025. URL: https://blog.google/threat-analysis-group/tag-bulletin-q1-2025/ (дата звернення: 14.02.2026).

196. Google Threat Analysis Group. TAG Bulletin: Q2 2025. 21.07.2025. URL: https://blog.google/threat-analysis-group/tag-bulletin-q2-2025/ (дата звернення: 14.02.2026).

197. Meta. Adversarial Threat Report: First Quarter 2025. 2025. URL: https://transparency.meta.com/sr/Q1-2025-Adversarial-threat-report/ (дата звернення: 14.02.2026).

198. Bergmanis-Korāts G., Haiduchyk T. Social Media Manipulation for Sale: Experiment on Platform Capabilities to Detect and Counter Inauthentic Social Media Engagement. Riga : NATO Strategic Communications Centre of Excellence, 2024. 28 p. ISBN 978-9934-619-07-6. URL: https://stratcomcoe.org/publications/social-media-manipulation-for-sale-experiment-on-platform-capabilities-to-detect-and-counter-inauthentic-social-media-engagement/311 (дата звернення: 04.08.2026).

199. TikTok. Covert Influence Operations (June 2025). TikTok Transparency Center. URL: https://www.tiktok.com/transparency/en/covert-influence-operations-june-2025 (дата звернення: 14.02.2026).

200. TikTok: Report March 2025. Transparency Centre (EU Code of Practice on Disinformation). URL: https://disinfocode.eu/reports/tiktok/5 (дата звернення: 14.02.2026).

201. Telegram. User guidance for the EU Digital Services Act (DSA). URL: https://telegram.org/tos/eu-dsa (дата звернення: 14.02.2026).

202. Детектор медіа. Ключові «болючі точки», які російська пропаганда використовувала у 2024 році для впливу на українців. 07.01.2025. URL: https://detector.media/infospace/article/236894/2025-01-07-klyuchovi-bolyuchi-tochky-yaki-rosiyska-propaganda-vykorystovuvala-u-2024-rotsi-dlya-vplyvu-na-ukraintsiv/ (дата звернення: 15.02.2025).

203. Iyengar S., Hahn K. S. Red Media, Blue Media: Evidence of Ideological Selectivity in Media Use. *Journal of Communication*. 2009. Vol. 59, no. 1. P. 19–39. DOI: 10.1111/j.1460-2466.2008.01402.x.

204. Nickerson R. S. Confirmation Bias: A Ubiquitous Phenomenon in Many Guises. *Review of General Psychology*. 1998. Vol. 2, no. 2. P. 175–220. DOI: 10.1037/1089-2680.2.2.175.

205. Tversky A., Kahneman D. Availability: A Heuristic for Judging Frequency and Probability. *Cognitive Psychology*. 1973. Vol. 5, no. 2. P. 207–232. DOI: 10.1016/0010-0285(73)90033-9.

206. KI-Textscanner gegen Manipulationen: Alle 27 Bias-Kategorien im Überblick. MDR WISSEN. 20.02.2024. URL: https://www.mdr.de/wissen/Kategorien-ki-textscanner-manipulationen100.html (дата звернення: 10.01.2025).

207. Детектор медіа. «Українців чекає жахлива зима»: що російські пропагандисти пишуть у телеграмі про зиму 2024–2025 років в Україні. 23.09.2024. URL: https://disinfo.detector.media/post/ukraintsiv-chekaie-zhakhlyva-zyma-shcho-rosiiski-propahandysty-pyshut-u-telehrami-pro-zymu-2024-2025-rokiv-v-ukraini (дата звернення: 10.11.2024).

208. EUvsDisinfo. National Whataboutism as a State Ideology. 10.02.2021. URL: https://euvsdisinfo.eu/national-whataboutism-as-a-state-ideology/ (дата звернення: 15.03.2024).

209. Gilbert D. Fake Taylor Swift Quotes Are Being Used to Spread Anti-Ukraine Propaganda. *WIRED*. 06.12.2023. URL: https://www.wired.com/story/russia-ukraine-taylor-swift-disinformation/ (дата звернення: 20.02.2024).

210. *The Times*. How Russia targets Ukrainians' hearts and minds through their phones. 2025. 5 August. URL: https://www.thetimes.co.uk/article/russia-targets-ukrainians-phones-29zl8fb3v (дата звернення: 25.10.2025).

211. EUvsDisinfo. The Kremlin's disinformation narratives about the Summit on Peace in Ukraine. 17.06.2024. URL: https://euvsdisinfo.eu/the-kremlins-disinformation-narratives-about-the-summit-on-peace-in-ukraine/ (дата звернення: 10.08.2024).

212. Pennycook G., Rand D. G. The Implied Truth Effect: Attaching Warnings to a Subset of Fake News Stories Increases Perceived Accuracy of Stories Without Warnings. *Management Science*. 2020. Vol. 66, no. 11. P. 4944–4957. DOI: 10.1287/mnsc.2019.3478.

213. Bail C. A. et al. Exposure to opposing views on social media can increase political polarization. *Proceedings of the National Academy of Sciences*. 2018. Vol. 115, no. 37. P. 9216–9221. DOI: 10.1073/pnas.1804840115.

214. Детектор медіа. У Twitter та Viber запустили провокативний флешмоб, у межах якого українців закликають масово вмикати світло. 01.11.2022. URL: https://disinfo.detector.media/post/u-tviteri-ta-vaiberi-zapustyly-provokatyvnyi-fleshmob-u-mezhakh-iakoho-ukraintsiv-zaklykaiut-masovo-vmykaty-svitlo (дата звернення: 15.01.2024).

215. Служба безпеки України. СБУ повідомила про підозру нападниці на відомого волонтера та активіста Сергія Стерненка. 02.05.2025. URL: https://ssu.gov.ua/novyny/sbu-povidomyla-pro-pidozru-napadnytsi-na-vidomoho-volontera-ta-aktyvista-serhiia-sternenka-video (дата звернення: 12.06.2025).

216. Миколаївщина та диверсії: як російські спецслужби залучають підлітків до терору. Центр публічних розслідувань. 15.01.2025. URL: https://cpi.org.ua/news/mikolayivshina-ta-diversiyi-yak-rosijski-specsluzh/ (дата звернення: 04.08.2026).

217. Antoniuk D. Ukraine detains alleged FSB agent recruited via TikTok for spying on military. The Record. 5 May 2025. URL: https://therecord.media/ukraine-arrests-fsb-agent-spying-recruited-tiktok (дата звернення: 15.06.2025).

218. «Спали» ФСБшника : інформаційна кампанія та офіційний чатбот. Служба безпеки України. URL: https://ssu.gov.ua/spaly-fsbshnyka (дата звернення: 04.08.2026).

219. World Economic Forum. Global Cybersecurity Outlook 2025. 13 January 2025. URL: https://reports.weforum.org/docs/WEF_Global_Cybersecurity_Outlook_2025.pdf (дата звернення: 14.08.2025).

220. Scott S. Counting the Costs: A Cybersecurity Metrics Framework for Policy. Atlantic Council, 2025. 25 p. URL: https://www.atlanticcouncil.org/wp-content/uploads/2025/05/Counting-the-costs-A-cybersecurity-metrics-framework-for-policy.pdf (дата звернення: 14.08.2025).

221. Swiss Cyber Institute. Top 5 cybersecurity trends in 2025. 20 Feb. 2025. URL: https://swisscyberinstitute.com/blog/top-5-cybersecurity-trends-2025/ (дата звернення: 14.08.2025).

222. Standards for Security Categorization of Federal Information and Information Systems. FIPS PUB 199. Gaithersburg, MD : National Institute of Standards and Technology, 2004. 13 p. URL: https://csrc.nist.gov/pubs/fips/199/final (дата звернення: 04.08.2026).

223. Тренди кібербезпеки на 2025 рік: як захистити бізнес. Kyivstar Business Hub. 16 груд. 2024. URL: https://hub.kyivstar.ua/articles/ostanni-trendy-kiberbezpeky (дата звернення: 15.08.2025).

224. Rose S., Borchert O., Mitchell S., Connelly S. Zero Trust Architecture. NIST Special Publication 800-207. Gaithersburg, MD : National Institute of Standards and Technology, 2020. 59 p. DOI: 10.6028/NIST.SP.800-207.

225. Абібулаєв А. Р., Піскозуб А. З. Аналіз сучасних підходів управління доступом у хмарному середовищі. *Сучасний захист інформації*. 2025. № 1(61). С. 174–188. DOI: 10.31673/2409-7292.2025.017186.

226. War and Cyber: Three Years of Struggle and Lessons for Global Security : analytical report. Kyiv : SSSCIP Ukraine, 2025. 21 p. URL:

https://cip.gov.ua/services/cm/api/attachment/download?id=69131 (дата звернення: 15.08.2025).

227. Pakharenko G. Cyber Operations at Maidan: A First-Hand Account. Cyber War in Perspective: Russian Aggression against Ukraine / ed. K. Geers. Tallinn : NATO Cooperative Cyber Defence Centre of Excellence, 2015. URL: https://ccdcoe.org/uploads/2018/10/Ch07_CyberWarinPerspective_Pakharenko.pdf (дата звернення: 04.08.2026).

228. Statement from the Press Secretary regarding the attribution of the NotPetya cyberattack. The White House, 2018. 15 Feb. URL: https://web.archive.org/web/20180216151954/https://www.whitehouse.gov/briefings-statements/statement-press-secretary-25/ (дата звернення: 14.08.2025).

229. ESET: Головною жертвою вірусу-шифрувальника Petya.A стала Україна. 2017. URL: https://web.archive.org/web/20170702080436/http://itc.ua/blogs/eset-glavnoy-zhertvoy-virusa-shifrovalshhika-petya-a-stala-ukraina-gde-zaregistrirovano-bolee-75-vseh-sluchaev-zarazheniya/ (дата звернення: 14.08.2025).

230. Поліція розпочала кримінальне провадження за фактом кібератак на сайти державних органів. Кіберполіція України. 14.01.2022. URL: https://cyberpolice.gov.ua/news/policziya-rozpochala-kryminalne-provadzhennya-za-faktom-kiberatak-na-sajty-derzhavnyx-organiv-1549/ (дата звернення: 04.08.2026).

231. Destructive malware targeting Ukrainian organizations. Microsoft Security Blog. 15.01.2022. URL: https://www.microsoft.com/en-us/security/blog/2022/01/15/destructive-malware-targeting-ukrainian-organizations/ (дата звернення: 04.08.2026).

232. Russia behind cyber-attack with Europe-wide impact an hour before Ukraine invasion. Government of the United Kingdom. 10.05.2022. URL: https://www.gov.uk/government/news/russia-behind-cyber-attack-with-europe-wide-impact-an-hour-before-ukraine-invasion (дата звернення: 04.08.2026).

233. Зупинено строки адміністративного провадження через кібератаку на державні реєстри: Уряд ухвалив постанову № 1445. Центральне

міжрегіональне управління Міністерства юстиції. 26.12.2024. URL: https://centraljust.gov.ua/news/info/zupineno-stroki-administrativnogo-provadjennya-cherez-kiberataku-na-derjavni-reestri-uryad-uhvaliv-postanovu-1445 (дата звернення: 04.08.2026).

234. CERT-UA минулого року опрацювала 4315 кіберінцидентів. Державна служба спеціального зв'язку та захисту інформації України. 08.01.2025. URL: https://cip.gov.ua/ua/news/cert-ua-minulogo-roku-opracyuvala-4315-kiberincidentiv (дата звернення: 04.08.2026).

235. Огляд ринку кібербезпеки в Україні / IT Ukraine Association, European Business Association; за підтримки USAID. Січень 2025. 43 с. URL: https://itukraine.org.ua/files/Ukraine-Cybersec-Market-Review.pdf (дата звернення: 04.08.2026).

236. NETSCOUT. DDoS: НАСТУПНЕ ПОКОЛІННЯ. Звіт про розвідку DDoS-загроз. Випуск 14. 2025. 21 р. URL: https://www.netscout.com/threatreport/wp-content/uploads/2025/03/TR_2H2024_Web-FINAL.pdf (дата звернення: 15.08.2025).

237. ESET Threat Report T1 2022. Bratislava : ESET, 2022. 54 p. URL: https://www.eset.com/fileadmin/ESET/INT/B2B_Resource_centrum/Reports/T1-2022_Threat-Report.pdf (дата звернення: 15.08.2025).

238. Зведена інформація щодо діяльності угрупування UAC-0010 станом на липень 2023 року. CERT-UA. 31.07.2023. URL: https://csirt.csi.cip.gov.ua/uk/posts/uac-0010-2023 (дата звернення: 04.08.2026).

239. Російські кібероперації: аналітика за друге півріччя 2023 року. Державна служба спеціального зв'язку та захисту інформації України, CERT-UA. 2024. URL: https://cip.gov.ua/services/cm/api/attachment/download?id=64621 (дата звернення: 04.08.2026).

240. Російські спецслужби активізували спроби зламу облікових записів українців за допомогою соціальної інженерії. Держспецзв'язок України. 5 черв. 2025. URL: https://cip.gov.ua/ua/faqs/rosiiski-specsluzhbi-aktivizuvali-sprobi-zlamu-

oblikovikh-zapisiv-ukrayinciv-za-dopomogoyu-socialnoyi-inzheneriyi (дата звернення: 15.08.2025).

241. Колосовський Є. Ю., Круць Е. М. Сучасний стан кібербезпеки України в умовах воєнного періоду. *Юридичний науковий електронний журнал*. 2023. № 12. С. 402–405. DOI: 10.32782/2524-0374/2023-12/100.

242. Про внесення змін до деяких законів України щодо захисту інформації та кіберзахисту державних інформаційних ресурсів : Закон України від 27.03.2025 № 4336-IX. URL: https://zakon.rada.gov.ua/go/4336-20 (дата звернення: 15.08.2025).

243. Directive (EU) 2022/2555 of the European Parliament and of the Council of 14 December 2022 on measures for a high common level of cybersecurity across the Union (NIS 2 Directive). *Official Journal of the European Union*. 2022. L 333. P. 80–152. URL: https://eur-lex.europa.eu/eli/dir/2022/2555/oj/eng (дата звернення: 04.08.2026).

244. Проєкт Закону про Кіберсили Збройних Сил України : проєкт Закону України від 19.12.2024 № 12349. Верховна Рада України. URL: https://itd.rada.gov.ua/billinfo/Bills/Card/45453 (дата звернення: 04.08.2026).

245. Досвід розвитку системи кібербезпеки та кібероборони провідних країн світу / С. Г. Вдовенко та ін. *Сучасні інформаційні технології у сфері безпеки та оборони*. 2020. № 37(1). С. 31–48. DOI: 10.33099/2311-7249/2020-37-1-31-48.

246. Польща створила Війська оборони кіберпростору. Польське радіо. 08.02.2022. URL: https://www.polskieradio.pl/398/7856/artykul/2898349 (дата звернення: 14.03.2024).

247. Freedom House. Should Ukraine Drop Sanctions against Russian Tech Companies? 2019. URL: https://freedomhouse.org/report/policy-brief/2019/should-ukraine-drop-sanctions-against-russian-tech-companies (дата звернення: 22.04.2024).

248. Конституція України : Закон України від 28 черв. 1996 р. № 254к/96-ВР. База даних «Законодавство України» / Верховна Рада України. URL: https://zakon.rada.gov.ua/laws/show/254к/96-вр (дата звернення: 13.01.2024).

249. Про правовий режим воєнного стану : Закон України від 12 трав. 2015 р. № 389-VIII. База даних «Законодавство України» / Верховна Рада України. URL: https://zakon.rada.gov.ua/go/389-19 (дата звернення: 15.01.2024).

250. Про доступ до публічної інформації : Закон України від 13 січ. 2011 р. № 2939-VI. База даних «Законодавство України» / Верховна Рада України. URL: https://zakon.rada.gov.ua/go/2939-17 (дата звернення: 13.01.2026).

251. Про інформацію : Закон України від 02 жовт. 1992 р. № 2657-XII. База даних «Законодавство України» / Верховна Рада України. URL: https://zakon.rada.gov.ua/go/2657-12 (дата звернення: 13.01.2026).

252. Про медіа : Закон України від 13 груд. 2022 р. № 2849-IX. База даних «Законодавство України» / Верховна Рада України. URL: https://zakon.rada.gov.ua/go/2849-20 (дата звернення: 13.01.2026).

253. Про захист інформації в інформаційно-комунікаційних системах : Закон України від 05 лип. 1994 р. № 80/94-ВР. База даних «Законодавство України» / Верховна Рада України. URL: https://zakon.rada.gov.ua/go/80/94-вр (дата звернення: 13.01.2026).

254. Про санкції : Закон України від 14 серп. 2014 р. № 1644-VII. База даних «Законодавство України» / Верховна Рада України. URL: https://zakon.rada.gov.ua/go/1644-18 (дата звернення: 13.01.2026).

255. Про національну безпеку України : Закон України від 21 черв. 2018 р. № 2469-VIII. База даних «Законодавство України» / Верховна Рада України. URL: https://zakon.rada.gov.ua/go/2469-19 (дата звернення: 13.01.2026).

256. Про рішення Ради національної безпеки і оборони України від 29 грудня 2016 року «Про Доктрину інформаційної безпеки України» : Указ Президента України від 25 лют. 2017 р. № 47/2017. База даних «Законодавство України» / Верховна Рада України. URL: https://zakon.rada.gov.ua/go/47/2017 (дата звернення: 13.01.2026).

257. Стратегія інформаційної безпеки України : Указ Президента України від 28 груд. 2021 р. № 685/2021. Офіційне інтернет-представництво Президента України. URL: https://www.president.gov.ua/documents/6852021-41069 (дата звернення: 04.12.2025).

258. Про введення в дію рішення Ради національної безпеки і оборони України від 28 квітня 2017 року «Про застосування персональних спеціальних економічних та інших обмежувальних заходів (санкцій)» : Указ Президента України від 15 трав. 2017 р. № 133/2017. Офіційне інтернет-представництво Президента України. URL: https://www.president.gov.ua/documents/1332017-21850 (дата звернення: 17.02.2026).

259. Ukraine: Revoke Ban on Dozens of Russian Web Companies. Human Rights Watch. 16 May 2017. URL: https://www.hrw.org/news/2017/05/17/ukraine-revoke-ban-dozens-russian-web-companies (дата звернення: 17.02.2026).

260. Arbitrary Internet blocking jeopardises freedom of expression. Council of Europe Commissioner for Human Rights. 26 Sept 2017. URL: https://www.coe.int/en/web/commissioner/-/arbitrary-internet-blocking-jeopardises-freedom-of-expression (дата звернення: 17.02.2026).

261. Про введення в дію рішення Ради національної безпеки і оборони України від 2 лютого 2021 року «Про застосування персональних спеціальних економічних та інших обмежувальних заходів (санкцій)» : Указ Президента України від 2 лют. 2021 р. № 43/2021. Офіційне інтернет-представництво Президента України. URL: https://www.president.gov.ua/documents/432021-36441 (дата звернення: 17.02.2026).

262. In Ukraine, taking three pro-Russia channels off the air raises complex issues. Human Rights Watch. 11 Feb 2021. URL: https://www.hrw.org/news/2021/02/11/ukraine-taking-three-pro-russia-channels-air-raises-complex-issues (дата звернення: 17.02.2026).

263. OSCE Representative on Freedom of the Media meets with Permanent Representative of Ukraine to the OSCE. OSCE RFoM. 3 Feb 2021. URL:

https://www.osce.org/representative-on-freedom-of-media/477451 (дата звернення: 17.02.2026).

264. OSCE Media Freedom Representative concerned about sanctions in Ukraine that endanger media freedom and free flow of information. OSCE Representative on Freedom of the Media. 25 Aug. 2021. URL: https://rfom.osce.org/representative-on-freedom-of-media/496339 (дата звернення: 04.08.2026).

265. Про введення в дію рішення Ради національної безпеки і оборони України від 20 серпня 2021 року «Про застосування персональних спеціальних економічних та інших обмежувальних заходів (санкцій)» : Указ Президента України від 21 серп. 2021 р. № 376/2021. Офіційне інтернет-представництво Президента України. URL: https://www.president.gov.ua/documents/3762021-39745 (дата звернення: 17.02.2026).

266. Freedom on the Net 2021: Ukraine. Freedom House. 2021. URL: https://freedomhouse.org/country/ukraine/freedom-net/2021 (дата звернення: 17.02.2026).

267. Про введення в дію рішення Ради національної безпеки і оборони України від 11 лютого 2022 року «Про застосування персональних спеціальних економічних та інших обмежувальних заходів (санкцій)» : Указ Президента України від 11 лют. 2022 р. № 52/2022. Офіційне інтернет-представництво Президента України. URL: https://www.president.gov.ua/documents/522022-41353 (дата звернення: 17.02.2026).

268. Kremlin plan to install pro-Russian leadership in Ukraine exposed. UK Government (Foreign, Commonwealth & Development Office). 22 Jan 2022. URL: https://www.gov.uk/government/news/kremlin-plan-to-install-pro-russian-leadership-in-ukraine-exposed (дата звернення: 17.02.2026).

269. Richter A. Sanction law against Russian and Belarusian audiovisual media. IRIS Extra 2022. Strasbourg : European Audiovisual Observatory, 2022. 36 p. URL: https://rm.coe.int/iris-extra-2022-sanction-law-against-russian-and-belarusian-audiovisua/1680a8ff9f (дата звернення: 04.08.2026).

270. Україна синхронізувала санкції з Великою Британією, а також застосувала обмеження відповідно до резолюцій Радбезу ООН. Офіційне інтернет-представництво Президента України. 27 груд. 2025. URL: https://www.president.gov.ua/news/ukrayina-sinhronizuvala-sankciyi-z-velikoyu-britaniyeyu-tako-102221 (дата звернення: 17.02.2026).

271. Україна запровадила санкції проти російських спортивних пропагандистів та діячів шоу-бізнесу. Офіційне інтернет-представництво Президента України. 17 січ. 2026. URL: https://www.president.gov.ua/news/ukrayina-zaprovadila-sankciyi-proti-rosijskih-sportivnih-propagandistiv-ta-diyachiv-shou-biznesu-102477 (дата звернення: 17.02.2026).

272. Council Regulation (EU) 2022/350 of 1 March 2022 amending Regulation (EU) No 833/2014 concerning restrictive measures in view of Russia's actions destabilising the situation in Ukraine. *Official Journal of the European Union*. 2022. L 65. P. 1–4. URL: http://data.europa.eu/eli/reg/2022/350/oj (дата звернення: 17.02.2026).

273. Про рішення Ради національної безпеки і оборони України від 14 травня 2021 року «Про Стратегію кібербезпеки України» : Указ Президента України від 26 серп. 2021 р. № 447/2021. База даних «Законодавство України» / Верховна Рада України. URL: https://zakon.rada.gov.ua/go/447/2021 (дата звернення: 13.01.2026).

274. Русакевич А. Інформаційна безпека в умовах воєнного стану у аспекті захисту інформаційних прав громадян. *Law. State. Technology*. 2024. Вип. 2. С. 58–62. DOI: 10.32782/LST/2024-2-11.

275. Красноступ Г. М. Нова стратегія інформаційної безпеки: правова відповідь на російське інформаційне маніпулювання та втручання. *Інформація і право*. 2025. № 2(53). С. 136–146. DOI: 10.37750/2616-6798.2025.2(53).334149.

276. Лопатченко І. М., Помаза-Пономаренко А. Л., Батир Ю. Г. Державне регулювання у сфері інформаційної безпеки України в умовах воєнного стану. *Вісник Національного університету цивільного захисту України. Серія*

«Державне управління». 2024. № 1(20). С. 14–24. DOI: 10.52363/2414-5866-2024-1-2.

277. Пашковський В. Ф. Гуманітарна політика у вимірі механізмів забезпечення інформаційної безпеки України. *Політологічний вісник*. 2021. № 86. С. 190–209. DOI: 10.17721/2415-881x.2021.86.190-209.

278. Зозуля І. В. Глобальний, регіональний та національний виміри російсько-української війни. *Форум права*. 2023. № 1(74). С. 52–67. DOI: 10.5281/zenodo.7016665.

279. Савчук В. А. Гуманітарні складники антиукраїнських інформаційно-пропагандистських операцій: сучасні домінанти та механізми протидії. *Філософія та політологія в контексті сучасної культури*. 2025. Т. 17, № 2. С. 76–81. DOI: 10.15421/352551.

280. Hordiichuk O., Halapsis A., Kozlovets M. How the Information Warfare Turns into Full-Scale Military Aggression: The Experience of Ukraine. *Przegląd Strategiczny*. 2023. Vol. 16, no. 1. P. 345–362. DOI: 10.14746/ps.2023.1.25.

281. Shultz D., Jasparro C. How Does Russia Exploit History and Cultural Heritage for Information Warfare? Recommendations for NATO. Antiquities Coalition Think Tank Policy Brief. 2022. No. 11. 6 p. URL: https://acthinktank.scholasticahq.com/article/118601-how-does-russia-exploit-history-and-cultural-heritage-for-information-warfare-recommendations-for-nato (дата звернення: 04.12.2025).

282. Shyshkina Ye. K. Information Technologies in Political Propaganda: The Case of the Russian-Ukrainian Information War (2014–2022). *Вчені записки ТНУ імені В. І. Вернадського. Серія: Історичні науки*. 2025. Т. 36(75), № 2. С. 269–273. DOI: 10.32782/2663-5984.2025/2.39.

283. Masiyenko Y., Zahryvenko K., Koval N., Tereshchenko D. “The Russian Flag Will Be Flown Wherever Russian Is Spoken”: “Russkiy Mir” Foundation. Case Study. Kyiv : Ukrainian Institute; MZ Hub, 2022. 52 p. URL: https://ui.org.ua/wp-content/uploads/2022/07/case-study_russkiy-mir-foundation.pdf (дата звернення: 04.12.2025).

284. Lytvynchuk O., Shevchuk A., Hrytsyshena Z. Hybrid War: The Influence of the Russian Orthodox Church on the Ukrainian Media. *Occasional Papers on Religion in Eastern Europe*. 2025. Vol. 45, iss. 6, art. 3. DOI: 10.55221/2693-2229.2665.

285. Brytsyn M., Vasin M. Faith Under Russian Terror: Analysis of the Religious Situation in Ukraine. Franklin, TN : Mission Eurasia; Kyiv : O. V. Pugach, 2025. 52 p. URL: https://missioneurasia.org/wp-content/uploads/2025/01/2025-Mission-Eurasia-report-on-Ukraine-ENG.pdf (дата звернення: 15.02.2026).

286. Gudziak B. Russian Orthodox leader Patriarch Kirill's unholy war against Ukraine. Atlantic Council. 3 Aug. 2023. URL: https://www.atlanticcouncil.org/blogs/ukrainealert/russian-orthodox-leader-patriarch-kirills-unholy-war-against-ukraine/ (дата звернення: 04.12.2025).

287. Meienberger A. The Concept of the "Russkiy Mir": History of the Concept and Ukraine. *Euxeinos*. 2023. Vol. 13, no. 35. P. 15–29. DOI: 10.55337/35.QLPT4607.

288. Rotari I. 'Russian World': Interpretations of a Dynamic Tool of the Russian Federation's Foreign Policy. *Codrul Cosminului*. 2023. Vol. 29, no. 1. P. 171–192. DOI: 10.4316/CC.2023.01.09.

289. Громадянська мережа ОПОРА. Media Consumption of Ukrainians: the Third Year of a Full-Scale War. 10.07.2024. URL: https://oporaua.org/viyna/media-consumption-of-ukrainians-the-third-year-of-a-full-scale-war-25292 (дата звернення: 04.12.2025).

290. Civil Network OPORA. Social Cohesion in Ukrainian Society: Challenges and Barriers for Vulnerable Groups. 16.07.2025. URL: https://oporaua.org/viyna/social-cohesion-in-ukrainian-society-challenges-and-barriers-for-vulnerable-groups-25748 (дата звернення: 04.12.2025).

291. Dukach Y., Adam I., Furbish M. Digital Occupation: Pro-Russian Bot Networks Target Ukraine's Occupied Territories on Telegram. Atlantic Council. 16.07.2025. URL: https://www.atlanticcouncil.org/in-depth-research-reports/report/report-russian-bot-networks-occupied-ukraine/ (дата звернення: 04.12.2025).

292. Lychko T., Shapoval O. Russian Propaganda Camps: Where and Why Russia Takes Children from the Temporarily Occupied Territories. Kyiv : CCE “Almenda”, 2024. 56 p. URL: https://almenda.org/wp-content/uploads/2024/11/Tabory_web_eng.pdf (дата звернення: 04.12.2025).

293. Філатов В. В. Перспективи розвитку інформаційного законодавства в умовах перехідного періоду в Україні. *Вчені записки Таврійського національного університету імені В. І. Вернадського. Серія: юридичні науки*. 2024. Т. 35(74), № 6. С. 71–75. DOI: 10.32782/TNU-2707-0581/2024.6/13.

294. Ukrainian Media Landscape 2022–2024: Changes in Media During the Full-Scale Invasion : analytical report / S. Shturkhetskyi et al. Kyiv : Center for Free Press, 2024. 104 p. ISBN 978-617-7370-71-9. URL: https://www.aup.com.ua/wp-content/uploads/2025/01/Ukrainian_Media_Landscape_2022-2024_EN.pdf (дата звернення: 04.12.2025).

295. Detector Media team. Media Literacy Index of Ukrainians: 2020–2024 Fifth Wave : web publication. 07.05.2025. URL: https://en.detector.media/post/media-literacy-index-of-ukrainians-2020-2024-fifth-wave (дата звернення: 04.12.2025).

296. Research on information environment: Ukraine : report / INFO OPS Polska Foundation; DFRLab (Atlantic Council). 2025. 182 p. URL: https://disinfodigest.pl/wp-content/uploads/2025/07/Information-environment-research-UKRAINE.pdf (дата звернення: 04.12.2025).

297. Detector Media; Kosciuszko Institute; Civic Resilience Initiative. Resilience to Disinformation: Lublin Triangle Perspective / supported by Open Information Partnership. 2022. 56 p. URL: https://www.gov.pl/attachment/38d364fe-b7b6-4293-9626-160abaa0ecda (дата звернення: 15.02.2026).

298. Operation Overload: More Platforms, New Techniques, Powered by AI. Activity Update June 2025. CheckFirst. 2025. 138 p. URL: https://checkfirst.network/wp-content/uploads/2025/06/Overload%C2%A02_%20Main%20Draft%20Report_compressed.pdf (дата звернення: 05.08.2026).

299. Савчук В. А. Стратегії та інструменти інформаційно-психологічного впливу в російській гібридній агресії проти України. *Протидія дезінформації в умовах російської агресії проти України: виклики і перспективи* : тези доп. учасників міжнар. наук.-практ. конф. (Анн-Арбор – Харків, 12–13 грудня 2023 р.). Харків, 2023. С. 286–289. DOI: 10.32782/PPSS.2023.1.74.

300. Цифровая Армия России : Telegram-канал. URL: https://t.me/digitalarmyrus (дата звернення: 05.08.2026).

301. Doppelganger – Media Clones Serving Russian Propaganda. EU DisinfoLab. 27.09.2022. URL: https://www.disinfo.eu/doppelganger/ (дата звернення: 05.08.2026).

302. RRN: A Complex and Persistent Information Manipulation Campaign. VIGINUM; Secrétariat général de la défense et de la sécurité nationale. 2023. 28 p. URL: https://www.sgdsn.gouv.fr/files/files/Publications/20230719_NP_VIGINUM_RAPPORT-CAMPAGNE-RRN_EN.pdf (дата звернення: 05.08.2026).

303. Pamment J., Tsurtsumia D. Beyond Operation Doppelgänger: A Capability Assessment of the Social Design Agency. MPF Report Series. 2025. No. 8. Psychological Defence Agency. 215 p. ISBN 978-91-989646-3-9. URL: https://mpf.se/download/18.7cffbee41969f6d83e115221/1747230166207/Beyond%20Operation%20Doppelganger.pdf (дата звернення: 05.08.2026).

304. Operation Overload: how pro-Russian actors flood newsrooms with fake content and seek to divert their efforts. CheckFirst : website. 2024. 4 June. URL: https://checkfirst.network/operation-overload-how-pro-russian-actors-flood-newsrooms-with-fake-content-and-seek-to-divert-their-efforts/ (дата звернення: 01.07.2026).

305. Russian 'disinformation' hyped Paris bedbug scare, French minister says. Reuters. 2024. 1 March. URL: https://www.reuters.com/world/europe/russian-disinformation-hyped-paris-bedbug-scare-french-minister-says-2024-03-01/ (дата звернення: 01.07.2026).

306. Justice Department Disrupts Covert Russian Government-Sponsored Foreign Malign Influence Operation Targeting Audiences in the United States and Elsewhere. U.S. Department of Justice, Office of Public Affairs. 04.09.2024. URL: https://www.justice.gov/archives/opa/pr/justice-department-disrupts-covert-russian-government-sponsored-foreign-malign-influence (дата звернення: 05.08.2026).

307. Raising Online Defenses Through Transparency and Collaboration. Meta Adversarial Threat Report. Q3 2023. URL: https://about.fb.com/news/2023/11/metas-adversarial-threat-report-q3-2023/ (дата звернення: 01.07.2026).

308. Як ru-пропаганда намагається зірвати мобілізацію в Україні. Центр протидії дезінформації. 12.10.2024. URL: https://cpd.gov.ua/result/yak-ru-propaganda-namagayetsya-zirvaty-mobilizacziyu-v-ukrayini/ (дата звернення: 05.08.2026).

309. ЦПД: юристи Медведчука, українці за кордоном, боти та недоексперти займаються дискредитацією мобілізації в Україні. ZN.UA. 2024. 7 травня. URL: https://zn.ua/ukr/war/tspd-juristi-medvedchuk-ukrajintsi-za-kordonom-boti-ta-nedoeksperti-zajmajutsja-diskretizatsijeju-mobilizatsiji-v-ukrajini-.html (дата звернення: 14.02.2025).

310. Фейк про мобілізацію громадян Молдови в Одесі та області. Центр протидії дезінформації. 03.07.2025. URL: https://cpd.gov.ua/international-direction/yevropa/fejk-pro-mobilizacziyu-gromadyan-moldovy-v-odesi-ta-oblasti/ (дата звернення: 05.08.2026).

311. У Маріуполі окупанти зруйнували пам’ятник жертвам Голодомору. Національний музей Голодомору-геноциду. URL: https://holodomormuseum.org.ua/news/u-mariupoli-okupanty-zrujnuvaly-pam-iatnyk-zhertvam-holodomoru/ (дата звернення: 09.03.2025).

312. Абрамова А. Окупанти встановили пам’ятник Сталіну в захопленому Мелітополі. Громадське. 09.05.2025. URL: https://hromadske.ua/viyna/244437-okupanty-vstanovyly-pamiatnyk-stalinu-v-zakhoplenomu-melitopoli (дата звернення: 05.08.2026).

313. Окупанти вивезли понад 10 тис. експонатів з музею в Херсоні. Двом особам повідомлено про підозру. Офіс Генерального прокурора. 10.02.2026. URL: https://gp.gov.ua/ua/posts/okupanti-vivezli-ponad-10-tis-eksponativ-z-muzeyu-v-xersoni-dvom-osobam-povidomleno-pro-pidozru (дата звернення: 05.08.2026).

314. Damaged Cultural Sites in Ukraine Verified by UNESCO. UNESCO. Останнє оновлення: 22.06.2026. URL: https://www.unesco.org/en/ukraine-war/damaged-cultural-sites (дата звернення: 05.08.2026).

315. Brooke L. It's Time StratCom Got Strategic about AI. *Defence Strategic Communications*. 2025. Vol. 16. P. 222–244. DOI: 10.30966/2018.RIGA.16.7.

316. Bolt N., Lange-Ionatamišvili E. The NextGen Information Environment. Riga : NATO Strategic Communications Centre of Excellence, 2026. 28 p. ISBN 978-9934-619-76-2. URL: https://stratcomcoe.org/publications/the-nextgen-information-environment/339 (дата звернення: 05.08.2026).

317. Artificial Intelligence Risk Management Framework (AI RMF 1.0). Gaithersburg : National Institute of Standards and Technology (NIST), 2023. 48 p. DOI: 10.6028/NIST.AI.100-1.

318. Від супутникового зв'язку до ШІ-асистента в Дії та оборонних технологій: підсумки Мінцифри у 2025 році / Міністерство цифрової трансформації України. 24 груд. 2025. URL: https://thedigital.gov.ua/news/progress/vid-shi-asystenta-v-diyi-do-suputnykovoho-zviazku-ta-oboronnykh-tekhnolohiy-pidsumky-mintsyfry-u-2025-rotsi (дата звернення: 05.08.2026).

319. Під час другого засідання Національного кластера з інформаційної стійкості обговорено використання інноваційних технологій у боротьбі з дезінформацією / Рада національної безпеки і оборони України. 22 верес. 2023. URL: https://www.rnbo.gov.ua/ua/Diialnist/6627.html (дата звернення: 18.01.2025).

320. С. Демедюк: BRAVE1 сприятиме проведенню розвідувальних та наступальних операцій у кібер- та інформаційному просторі / Рада національної безпеки і оборони України. 26 квіт. 2023. URL: https://www.rnbo.gov.ua/ua/Diialnist/6290.html (дата звернення: 19.01.2025).

321. Cyabra. Authenticity Analysis; Coordination & Amplification Analysis; Uncover Bot Networks : official product pages. URL: https://cyabra.com/solutions/uncover-bot-networks/ (дата звернення: 05.08.2026).

322. Підсумки року роботи Мінцифри 2025 / Міністерство цифрової трансформації України. URL: https://2025.thedigital.gov.ua/ (дата звернення: 05.08.2026).

323. Kalenský J., Osadchuk R. How Ukraine fights Russian disinformation: Beehive vs mammoth. Hybrid CoE Research Report 11. Helsinki : European Centre of Excellence for Countering Hybrid Threats, 2024. 48 p. URL: https://www.hybridcoe.fi/publications/hybrid-coe-research-report-11-how-ukraine-fights-russian-disinformation-beehive-vs-mammoth/ (дата звернення: 08.08.2025).

324. OpenAI. Disrupting malicious uses of AI. 25 Feb. 2026. URL: https://openai.com/index/disrupting-malicious-ai-uses/ (дата звернення: 05.08.2026).

325. Microsoft Digital Defense Report 2025. Redmond : Microsoft, 2025. 85 p. URL: https://www.microsoft.com/en-us/corporate-responsibility/topics/cybersecurity/reports/microsoft-digital-defense-report-2025/ (дата звернення: 05.08.2026).

326. World Economic Forum. The Global Risks Report 2026 : Insight Report. 21st Edition. Geneva : WEF, 2026. 92 p. URL: https://www.weforum.org/publications/global-risks-report-2026/ (дата звернення: 10.02.2026).

327. Daukšas V., Venclauskienė L. The Collage of the Kremlin’s Communication Strategy. Riga : NATO Strategic Communications Centre of Excellence, 2025. 127 p. URL: https://stratcomcoe.org/publications/the-collage-of-the-kremlins-communication-strategy/324 (дата звернення: 05.08.2026).

328. Barbu E., Banerjee S., Lim T., Zīvere L. AI in Support of StratCom: The Use and Evaluation of Large Language Models in Less Widely Used Official EU Languages. Riga : NATO Strategic Communications Centre of Excellence, 2025. 40 p. URL: https://stratcomcoe.org/publications/ai-in-support-of-stratcom-the-use-and-

evaluation-of-large-language-models-in-less-widely-used-official-eu-languages/326 (дата звернення: 05.08.2026).

329. Жахалов Я. Коли вийде національна LLM і скільки коштує її розробка. Головні питання СТО ШІ-центру Мінцифри Дмитру Овчаренку. DOU. 10 квіт. 2025. URL: https://dou.ua/lenta/interviews/dmytro-ovcharenko-about-national-llm/ (дата звернення: 05.08.2026).

330. Burdette Z., Phillips D., Heim J. L., Geist E., Frelinger D. R., Heitzenrater C., Mueller K. P. How Artificial Intelligence Could Reshape Four Essential Competitions in Future Warfare. Santa Monica : RAND Corporation, 2026. 22 January. 79 p. RR-A4316-1. DOI: 10.7249/RRA4316-1.

331. Два роки Талліннського механізму: системна міжнародна підтримка кіберстійкості України / Міністерство цифрової трансформації України. 22 груд. 2025. URL: https://thedigital.gov.ua/news/progress/dva-roky-tallinnskoho-mekhanizmu-systemna-miznarodna-pidtrymka-kiberstiykosti-ukrayiny (дата звернення: 05.08.2026).

332. Regulation (EU) 2024/1689 of the European Parliament and of the Council of 13 June 2024 laying down harmonised rules on artificial intelligence (Artificial Intelligence Act). *Official Journal of the European Union*. 2024. OJ L, 2024/1689. URL: https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX:32024R1689 (дата звернення: 05.08.2026).

333. Council of Europe Framework Convention on Artificial Intelligence and Human Rights, Democracy and the Rule of Law (CETS No. 225). Strasbourg : Council of Europe, 2024. URL: https://www.coe.int/en/web/artificial-intelligence/the-framework-convention-on-artificial-intelligence (дата звернення: 05.08.2026).

334. EU AI Act: Harmonised rules on artificial intelligence : Briefing. Brussels : European Parliament, 2024. URL: https://www.europarl.europa.eu/thinktank/en/document/EPRS_BRI(2021)690445 (дата звернення: 11.03.2025).

335. Як відповідально використовувати штучний інтелект: розробили рекомендації для медіа / Міністерство цифрової трансформації України. 24 січ. 2024. URL: https://thedigital.gov.ua/news/technologies/yak-vidpovidalno-vikoristovuvati-shtuchniy-intelekt-rozrobili-rekomendatsii-dlya-media (дата звернення: 05.08.2026).

ДОДАТОК А

СПИСОК ПУБЛІКАЦІЙ ЗДОБУВАЧА ЗА ТЕМОЮ ДИСЕРТАЦІЇ ТА ВІДОМОСТІ ПРО АПРОБАЦІЮ РЕЗУЛЬТАТІВ

Праці, у яких опубліковано основні наукові результати дисертації

Статті у наукових фахових виданнях України:

1. Савчук В. А. Інструменти виявлення та подолання деструктивних впливів та пропагандистських наративів інформаційних операцій: типологія, основні характеристики. *Актуальні проблеми філософії та соціології*. 2025. Вип. 54. С. 224–229. DOI: 10.32782/apfs.v054.2025.33.

2. Савчук В. А. Історична еволюція інформаційної складової гібридних воєн: від біблійних текстів до алгоритмів соціальних мереж. *Наукові праці Міжрегіональної Академії управління персоналом. Політичні науки та публічне управління*. 2025. № 2(78). С. 157–162. DOI: 10.32689/2523-4625-2025-2(78)-23.

3. Савчук В. А. Гуманітарні складники антиукраїнських інформаційно-пропагандистських операцій: сучасні домінанти та механізми протидії. *Філософія та політологія в контексті сучасної культури*. 2025. Т. 17, № 2. С. 76–81. DOI: 10.15421/352551.

4. Савчук В. А. Інформаційна складова сучасних воєн у політологічному дискурсі: зарубіжний та український контексти. *Епістемологічні дослідження в філософії, соціальних і політичних науках*. 2025. Т. 8, № 2. С. 198–203. DOI: 10.15421/342557.

5. Савчук В. А. Когнітивна війна: теоретичні засади та інституційна практика. *Регіональні студії*. 2025. № 42. С. 154–160. DOI: 10.32782/2663-6170/2025.42.24.

Тези, опубліковані за матеріалами конференцій

1. Савчук В. А. Стратегії та інструменти інформаційно-психологічного впливу в російській гібридній агресії проти України. *Протидія дезінформації в умовах російської агресії проти України: виклики і перспективи* : тези доп.

учасників міжнар. наук.-практ. конф. (Анн-Арбор – Харків, 12–13 груд. 2023 р.). Харків, 2023. С. 286–289. DOI: 10.32782/PPSS.2023.1.74.

2. Савчук В. А. Інформаційні війни як об’єкт міждисциплінарних наукових досліджень. *Сучасна наука: дослідження, економіка та інновації* : зб. наук. праць за матеріалами 3-ї Міжнар. наук.-практ. конф. (Загреб, Хорватія, 22–24 жовт. 2025 р.). Загреб, 2025. С. 282–284. URL: https://isu-conference.com/en/archive/modern-science-research-economy-and-innovation-22-10-25 (дата звернення: 07.08.2026).

Відомості про апробацію результатів дисертації

1. Міжнародна науково-практична конференція «Протидія дезінформації в умовах російської агресії проти України: виклики і перспективи». Анн-Арбор – Харків, 12–13 грудня 2023 р. Форма участі: публікація тез доповіді в матеріалах конференції.

2. 3-тя Міжнародна науково-практична конференція «Сучасна наука: дослідження, економіка та інновації» (Modern Science: Research, Economy and Innovation). Загреб, Хорватія, 22–24 жовтня 2025 р. Форма участі: дистанційна, з публікацією тез доповіді в матеріалах конференції.