Карпатський національний університет імені Василя Стефаника
Міністерство освіти і науки України
Карпатський національний університет імені Василя Стефаника
Міністерство освіти і науки України

Кваліфікаційна наукова
праця на правах рукопису

Кобець Тарас Анатолійович

УДК 351.746.1(477)’06:316.276]659.3-029:32(043.5)

ДИСЕРТАЦІЯ
ПОЛІТИКО-ІНФОРМАЦІЙНИЙ СКЛАДНИК КОГНІТИВНОЇ БЕЗПЕКИ СУЧАСНОЇ УКРАЇНИ

052 Політологія
05 Соціальні та поведінкові науки

Подається на здобуття наукового ступеня доктора філософії

Дисертація містить результати власних досліджень. Використання ідей, результатів і текстів інших авторів мають посилання на відповідне джерело _____ Т. А. Кобець

Науковий керівник: Монолатій Іван Сергійович, доктор політичних наук, професор

Івано-Франківськ – 2026

АНОТАЦІЯ

Кобець Т. А. Політико-інформаційний складник когнітивної безпеки сучасної України. – Кваліфікаційна наукова праця на правах рукопису.

Дисертація на здобуття ступеня доктора філософії в галузі знань 05 Соціальні та поведінкові науки за спеціальністю 052 Політологія. – Карпатський національний університет імені Василя Стефаника, Міністерство освіти і науки України, м. Івано-Франківськ, 2026.

У дисертації вирішено актуальне наукове завдання, яке полягає в теоретичному обґрунтуванні та концептуалізації когнітивної безпеки як ключового виміру національної безпеки України в умовах гібридної війни. Дослідження спрямоване на виявлення загроз, пов'язаних із маніпуляцією суспільною свідомістю, інформаційно-психологічним впливом і порушенням стійкості до дезінформаційних атак, а також на розробку підходів до формування ефективної системи когнітивного захисту.

У вступі обґрунтовано актуальність обраної теми дисертації в контексті сучасного наукового та суспільного дискурсу, сформульовано мету дослідження та окреслено його ключові завдання. Визначено наукову новизну отриманих результатів і підкреслено їхню теоретичну та практичну важливість. Зазначено взаємозв'язок дослідження з науковими програмами, темами та проєктами, конкретизовано об'єкт і предмет наукового аналізу. Наведено дані щодо апробації основних положень роботи, оприлюднення результатів у наукових публікаціях, а також висвітлено особистий внесок здобувача в проведене дослідження. Надано узагальнену характеристику структури та логіки дисертаційного дослідження.

У першому розділі дисертації *«Теоретико-концептуальні засади когнітивної безпеки в політичній науці»* охарактеризовано еволюцію формування категоріального апарату когнітивної безпеки та здійснено міждисциплінарний аналіз підходів до її розуміння. Визначено сутність когнітивної безпеки як стратегічного інструменту національної безпеки в умовах

гібридних загроз, зокрема з боку інформаційно-психологічних операцій, дезінформаційних кампаній та маніпулятивного впливу на суспільну свідомість.

Уточнено понятійно-категоріальний апарат дослідження: терміни «когнітивна безпека», «когнітивна стійкість», «когнітивна війна», «гібридні загрози», «гібридна війна» розглянуто у взаємозв'язку з категоріями інформаційної та кібербезпеки. Здійснено аналітичний огляд провідних концепцій українських і зарубіжних дослідників про когнітивний вимір безпеки, зокрема, вивчено праці Г. Почепцова, М. Кастельса, Ю. Габермаса, Т. Парсонса, які стали теоретичною основою для розуміння природи когнітивного впливу.

Проаналізовано політико-інформаційну складову когнітивної безпеки як окремий об'єкт наукового дослідження. Запропоновано концептуальну модель взаємодії інституцій держави та громадянського суспільства у сфері забезпечення захисту когнітивного простору. Підкреслено важливість поєднання нормативно-правових, технічних, психологічних і комунікативних інструментів для формування дієвої системи когнітивної безпеки України в умовах війни.

Визначено основні напрями дослідження когнітивної безпеки: аналіз когнітивних загроз у політичних процесах; вивчення стратегічних наративів і контрнаративів; моделювання механізмів когнітивного моніторингу та розробка індикаторів вразливості до маніпуляцій. Показано, що когнітивна безпека не лише захищає від зовнішнього впливу, але й виконує роль основи суспільної стійкості, ідентичності та державної єдності.

У другому розділі дисертації *«Когнітивна безпека українського суспільства в умовах гібридного протистояння: аналіз загроз та класифікаційних основ»* здійснено комплексне дослідження сучасних викликів когнітивній безпеці України, зумовлених гібридною війною, розвитком технологій штучного інтелекту та інтенсифікацією інформаційно-психологічних впливів. Розкрито сутність поняття «загроза когнітивній безпеці» та проаналізовано методологічні підходи до їхньої класифікації за рівнем реалізації, походженням, ступенем шкоди та ймовірності настання. Встановлено, що інформаційно-комунікаційне

середовище стало ареною стратегічного протистояння, у якому основною мішенню є людська свідомість і спроможність до критичного мислення.

У межах розділу охарактеризовано зовнішні та внутрішні загрози, як-от: маніпуляції наративами, дезінформаційні кампанії, когнітивне перевантаження, технології дипфейків і вплив алгоритмів персоналізації контенту. Особливу увагу приділено впливу ШІ на когнітивну вразливість населення, зокрема через механізми деструктивного формування реальності, порушення конфіденційності, посилення емоційних реакцій і зниження здатності до самостійного ухвалення рішень.

Досліджено функціонування гібридної війни як багатовимірної стратегії, у межах якої когнітивна безпека розглядається не як допоміжний елемент, а як ключовий фронт інформаційно-психологічного протистояння. Показано, що гібридна агресія охоплює не лише фізичні атаки, але й когнітивні, наприклад, у формі операцій впливу, спрямованих на ерозію суспільної єдності, делегітимацію державних інституцій та розмивання національної ідентичності.

На основі аналізу політико-інформаційного дискурсу виокремлено особливості когнітивної війни як окремого домену конфлікту, у якому маніпуляція ментальними структурами суспільства стає пріоритетним інструментом впливу. Досліджено співвідношення когнітивної, інформаційної, кібер- та психологічної безпеки, а також їхню роль у структурі національної безпеки. Встановлено, що ефективна протидія загрозам можлива лише за умов впровадження системи когнітивної резильєнтності – здатності особистості, спільноти й держави зберігати критичне мислення, раціональність та внутрішню цілісність.

Сформульовано концептуальні напрями забезпечення когнітивної безпеки: розвиток освіти й медіаграмотності, моніторинг когнітивного середовища, етичне впровадження ШІ, інформаційна децентралізація та формування позитивних національних наративів. Акцентовано на важливості інтеграції державних, громадянських і міжнародних зусиль у боротьбі з когнітивними загрозами в умовах гібридної війни.

У третьому розділі дисертації «*Механізми забезпечення когнітивної безпеки в умовах гібридної війни: стратегічний вимір*» проаналізовано інституційні, нормативно-правові, комунікативні та освітні механізми забезпечення когнітивної безпеки в умовах триваючого гібридного протистояння. Розкрито роль публічної комунікації як ресурсу протидії когнітивним загрозам, а також окреслено функції державних і недержавних акторів у формуванні когнітивної резильєнтності суспільства.

Особливу увагу приділено дослідженню стратегічних наративів як інструментів зміцнення суспільної єдності, підвищення довіри до інституцій та формування позитивного образу держави в умовах когнітивного протистояння. Визначено принципи побудови ефективної комунікативної політики держави в умовах гібридної війни, з огляду на актуальні виклики, пов’язані з дезінформацією, маніпулятивними медіатехнологіями, інформаційним тиском і когнітивними атаками.

Обґрунтовано необхідність формування цілісної стратегії когнітивної безпеки, яка базується на мультиакторному підході, інтегрує діяльність органів державної влади, медіа, системи освіти, громадянського суспільства та міжнародних партнерів. Наголошено на важливості розвитку когнітивної культури, цифрової грамотності, критичного мислення та етичного споживання інформації.

У межах розділу виокремлено ключові напрями реалізації когнітивної безпеки: комунікативна стратегія держави, розвиток медіаосвіти, підвищення інституційної прозорості, підтримка національного культурного контенту, а також впровадження технологій моніторингу та аналітики когнітивних впливів. Досліджено взаємозв’язок між когнітивною безпекою та стійкістю системи стратегічного управління в умовах воєнного часу.

Запропоновано структурну модель когнітивної безпеки як складника національної безпеки, що охоплює когнітивну стійкість, захист інформаційного середовища, протидію маніпуляціям і збереження ідентичності. Наголошено, що в сучасних умовах перемога у війні великою мірою залежить від ефективності

захисту свідомості – як простору політичного, соціального й особистісного вибору.

У четвертому розділі дисертації «*Пріоритети та стратегічні орієнтири когнітивної безпеки України в умовах гібридної війни*» обґрунтовано системну необхідність формування довгострокової державної політики у сфері когнітивної безпеки, що має зважати як на воєнно-політичні загрози, так і на соціальні, освітні та культурні чинники. Проаналізовано міжнародний досвід стратегічного планування у сфері когнітивної безпеки, зокрема, у рамках НАТО, ЄС, Ізраїлю, а також здійснено порівняльний аналіз основних моделей когнітивного протистояння.

Розкрито роль когнітивної безпеки в системі стійкості національної безпеки України та виокремлено її як самостійний стратегічний пріоритет у державній політиці. Когнітивна сфера визнається критично важливою, на рівні з фізичними доменами безпеки: сушею, морем, повітрям, космосом і кіберпростором. Обґрунтовано, що контроль за когнітивним простором громадян, тобто за процесами сприйняття, інтерпретації, емоційної реакції й ухвалення рішень стає новою формою геополітичної сили.

У межах розділу визначено основні стратегічні завдання для формування національної моделі когнітивної безпеки: розробка законодавчого забезпечення, створення системи когнітивного моніторингу, розвиток спеціалізованої експертизи, адаптація системи освіти, посилення інформаційної автономії держави та консолідація національної ідентичності. Особлива увага приділена розвитку когнітивної стійкості як запобіжника до деструктивного зовнішнього впливу.

Сформульовано ідею когнітивної безпеки як елемента екосистемного мислення в національному стратегічному плануванні. Запропоновано бачення когнітивного суверенітету як мети нової безпекової парадигми, що вимагає комплексної взаємодії між урядом, громадянським суспільством, академічною спільнотою, цифровими платформами та міжнародними партнерами.

Доведено, що тільки за умови системної інтеграції когнітивної безпеки в національну політику Україна зможе ефективно протистояти багатовимірним загрозам, зберегти суб'єктність у глобальному порядку денному та забезпечити цілісність і стійкість держави у післявоєнному періоді.

Наукова новизна й теоретичне значення дисертації полягає в концептуалізації когнітивної безпеки як самостійного стратегічного напряму державної політики в умовах гібридної війни та в розробці теоретичних, методичних і прикладних підходів до її забезпечення у контексті політичної безпеки й інформаційного суверенітету України. Уперше обґрунтовано концепт когнітивного суверенітету як стратегічної мети безпекової політики та запропоновано структурно-функціональну модель когнітивної безпеки України (когнітивна стійкість, публічна комунікація, інформаційний захист, наративна стратегія, освітньо-просвітницький компонент, міжнародна координація) для використання у стратегічному плануванні. Удосконалено теоретико-методологічні підходи до розуміння когнітивної безпеки як інтегративного політичного феномену, класифікацію когнітивних загроз (за джерелами, рівнями, масштабом, інструментами та ефектом підриву стійкості), а також компонентну модель забезпечення (нормативно-правовий, освітній, комунікаційно-інституційний і технологічний блоки). Подальшого розвитку набули понятійно-категоріальний апарат, підходи до аналізу стратегічних наративів/контрнаративів, методологія порівняльного аналізу міжнародних практик та пропозиції щодо інтеграції когнітивної безпеки у стратегічне планування і національний безпековий менеджмент як основи політичного та інформаційного суверенітету держави.

Практичне значення отриманих результатів полягає в тому, що викладені в дисертації положення, концептуальні підходи та рекомендації можуть бути використані у сфері державної політики та безпеки як підґрунтя для формування й реалізації комплексної стратегії забезпечення когнітивної безпеки України в умовах гібридної війни, зокрема для створення механізмів моніторингу когнітивних загроз, побудови системи протидії інформаційно-психологічним

операціям, підвищення когнітивної стійкості громадян і вдосконалення комунікативної політики у сфері стратегічних наративів; у науково-дослідній сфері матеріали роботи можуть слугувати основою для подальших досліджень у політичній науці, безпекових студіях, комунікаціях і соціальній психології, зокрема для аналізу причинно-наслідкових зв'язків гібридної агресії росії проти України та соціально-політичних чинників нових викликів для політичної стабільності, державної єдності й демократичного розвитку, що сприятиме поглибленню розуміння механізмів впливу когнітивних загроз на політичний процес і вдосконаленню політичної практики; у навчальному процесі результати можуть бути використані під час підготовки лекцій, навчальних програм, підручників і посібників із дисциплін «Політологія», «Масмедіа в політичному житті суспільства», «Медіаграмотність», «Політична психологія», «Інформаційна безпека», «Гібридна війна» тощо, а також у науково-дослідній роботі студентів, магістрантів та аспірантів, які вивчають проблематику інформаційної безпеки, політичної комунікації, державної безпеки та когнітивної сфери; у практичній площині напрацьовані положення можуть бути застосовані під час реалізації соціально-політичних реформ, трансформації органів державної влади та безпеки, формування нових підходів до управління суспільними процесами в умовах гібридних загроз, а також у діяльності органів державної влади, громадських організацій, аналітичних центрів і медіаструктур, що працюють у сфері інформаційної політики, кризового реагування, стратегічних комунікацій та інформаційної протидії агресору.

Ключові слова: геополітика, гібридна війна, дезінформація, державна інформаційна політика, інформаційна безпека, інформаційна війна, інформаційно-комунікативні механізми взаємодії, інформаційний простір, когнітивні загрози, медіа, національна безпека, національна ідентичність, політичний простір, російська пропаганда, Україна.

SUMMARY

Kobets T.A. The Political and informational component of cognitive security in contemporary Ukraine. – Qualifying scientific work on the rights of manuscript.

Dissertation submitted for the degree Doctor of Philosophy in the field of knowledge 05 Social and Behavioral Sciences on the specialty 052 Political Science. – Vasyl Stefanyk Carpathian National University, Ministry of Education and Science of Ukraine, Ivano-Frankivsk, 2026.

In the dissertation, an urgent scientific problem is addressed, which consists in the theoretical substantiation and conceptualization of cognitive security as a key dimension of Ukraine's national security in the context of hybrid warfare. The research is aimed at identifying threats associated with the manipulation of public consciousness, information-psychological influence, and the undermining of resilience to disinformation attacks, as well as developing approaches to the formation of an effective system of cognitive protection.

The introduction substantiates the relevance of the chosen dissertation topic within the context of contemporary academic and societal discourse. The research objective is foulated, and the key tasks of the study are outlined. The scientific novelty of the obtained results is defined, along with their theoretical and practical significance. The study's connection to current scientific programs, thematic areas, and projects is highlighted, and the object and subject of the research are specified. Information is provided regarding the approval of the dissertation's main findings, their dissemination in scholarly publications, as well as the author's personal contribution to the conducted research.

A general overview of the structure and logic of the dissertation is also presented.In the first chapter of the dissertation, "Theoretical and Conceptual Foundations of Cognitive Security in Political Science," the evolution of the categorical apparatus of cognitive security is characterized, and an interdisciplinary analysis of approaches to its understanding is carried out. The essence of cognitive security is defined as a strategic instrument of national security in conditions of hybrid

threats, in particular those arising from information-psychological operations, disinformation campaigns, and manipulative influence on public consciousness.

The conceptual and categorical apparatus of the study is clarified: the terms “cognitive security,” “cognitive resilience,” “cognitive warfare,” “hybrid threats,” and “hybrid war” are examined in relation to the categories of information and cyber security. An analytical review of leading concepts by Ukrainian and foreign researchers on the cognitive dimension of security is carried out, including studies by H. Pocheptsov, M. Castells, J. Habermas, and T. Parsons, which form the theoretical basis for understanding the nature of cognitive influence.

The political-informational component of cognitive security is analyzed as a distinct object of scientific research. A conceptual model of interaction between state institutions and civil society in the field of protecting the cognitive space is proposed. The importance of combining normative-legal, technical, psychological, and communicative tools to form an effective system of Ukraine’s cognitive security in wartime is emphasized.

The main directions of cognitive security research are identified: analysis of cognitive threats in political processes; study of strategic narratives and counter-narratives; modeling mechanisms of cognitive monitoring; and development of indicators of vulnerability to manipulation. It is shown that cognitive security not only protects against external influence but also serves as the basis for social resilience, identity, and state unity.

In the second chapter of the dissertation, “Cognitive Security of Ukrainian Society in Conditions of Hybrid Confrontation: Analysis of Threats and Classification Foundations,” a comprehensive study of contemporary challenges to Ukraine’s cognitive security is carried out, caused by hybrid warfare, the development of artificial intelligence technologies, and the intensification of information-psychological influences. The essence of the concept of “threat to cognitive security” is revealed, and methodological approaches to their classification by level of realization, origin, degree of harm, and likelihood are analyzed. It has been established that the information-

communication environment has become an arena of strategic confrontation in which the primary target is human consciousness and the ability to think critically.

Within the chapter, external and internal threats are characterized, in particular narrative manipulations, disinformation campaigns, cognitive overload, deepfake technologies, and the influence of content personalization algorithms. Special attention is paid to the impact of artificial intelligence on the cognitive vulnerability of the population, specifically through mechanisms of destructive reality formation, privacy violations, heightened emotional reactions, and diminished capacity for independent decision-making.

The functioning of hybrid war is studied as a multidimensional strategy in which cognitive security is viewed not as an auxiliary element but as a key front of information-psychological confrontation. It is shown that hybrid aggression encompasses not only physical attacks but also cognitive operations aimed at eroding social unity, delegitimizing state institutions, and diluting national identity.

Based on an analysis of political-informational discourse, the features of cognitive warfare as a separate domain of conflict are highlighted, in which the manipulation of mental structures of society becomes a priority instrument of influence. The relationship between cognitive, informational, cyber, and psychological security, and their roles within the framework of national security is examined. It has been established that effective countermeasures against threats are possible only by implementing a system of cognitive resilience – the ability of an individual, community, and state to maintain critical thinking, rationality, and internal integrity.

Conceptual directions for ensuring cognitive security have been formulated: the development of education and media literacy, cognitive environment monitoring, ethical deployment of artificial intelligence, informational decentralization, and the formation of positive national narratives. Emphasis is placed on the importance of integrating state, civil, and international efforts in combating cognitive threats in the context of hybrid warfare.

In the third chapter of the dissertation, “Mechanisms for Ensuring Cognitive Security in Conditions of Hybrid War: Strategic Dimension,” the institutional,

normative-legal, communicative, and educational mechanisms for ensuring cognitive security in ongoing hybrid confrontation are analyzed. The role of public communication as a resource for countering cognitive threats, as well as the functions of state and non-state actors in building societal cognitive resilience, are outlined.

Special attention is devoted to the study of strategic narratives as tools for strengthening social cohesion, increasing trust in institutions, and forming a positive image of the state in conditions of cognitive confrontation. Principles of building an effective communication policy of the state in hybrid war conditions, taking into account current challenges related to disinformation, manipulative media technologies, informational pressure, and cognitive attacks, are identified.

The necessity of forming a coherent cognitive security strategy based on a multi-actor approach that integrates the activities of government bodies, media, educational systems, civil society, and international partners is substantiated. The importance of developing cognitive culture, digital literacy, critical thinking, and ethical information consumption is emphasized.

Within the chapter, key directions for the realization of cognitive security are identified: state communication strategy, media education development, enhancement of institutional transparency, support for national cultural content, and the implementation of technologies for monitoring and analyzing cognitive influences. The interrelationship between cognitive security and the resilience of strategic management systems in wartime is explored.

A structural model of cognitive security as a component of national security is proposed, encompassing cognitive resilience, protection of the informational environment, counteraction to manipulation, and preservation of identity. It is emphasized that, in modern conditions, victory in war largely depends on the effectiveness of protecting consciousness as a space of political, social, and personal choice.

In the fourth chapter of the dissertation, “Priorities and Strategic Orientations of Ukraine’s Cognitive Security in Conditions of Hybrid War,” the systemic necessity of forming long-term state policy in the field of cognitive security is substantiated, taking

into account military-political, social, educational, and cultural factors. The international experience of strategic planning in the field of cognitive security, particularly within NATO, the EU, Israel, is analyzed, and a comparative analysis of major models of cognitive confrontation is conducted.

The role of cognitive security in the resilience system of Ukraine's national security is revealed, and it is identified as an independent strategic priority in state policy. The cognitive sphere is recognized as critically important – on par with physical security domains such as land, sea, air, space, and cyberspace. It is substantiated that control of the cognitive space of citizens – that is, the processes of perception, interpretation, emotional response, and decision-making – becomes a new form of geopolitical power.

Within the chapter, the main strategic tasks for forming a national model of cognitive security are defined: the development of legislative support, the creation of a cognitive monitoring system, the development of specialized expertise, adaptation of the education system, strengthening the informational autonomy of the state, and consolidation of national identity. Particular attention is paid to the development of cognitive resilience as a safeguard against destructive external influence.

The idea of cognitive security as an element of ecosystem thinking in national strategic planning is formulated. A vision of cognitive sovereignty as the goal of the new security paradigm is proposed, requiring comprehensive interaction among government, civil society, academia, digital platforms, and international partners.

It is demonstrated that only through systemic integration of cognitive security into national policy can Ukraine effectively counter multidimensional threats, preserve agency in the global agenda, and ensure the integrity and resilience of the state during the post-war period.

The scientific novelty and theoretical significance of the dissertation lie in conceptualizing cognitive security as an independent strategic domain of public policy under conditions of hybrid warfare and in developing theoretical, methodological, and applied approaches to its provision in the context of Ukraine's political security and information sovereignty. For the first time, the dissertation substantiates the concept of

cognitive sovereignty as a strategic goal of security policy and proposes a structural and functional model of Ukraine's cognitive security (cognitive resilience, public communication, information protection, narrative strategy, educational and outreach component, and international coordination) for use in strategic planning. The study further refines theoretical and methodological approaches to understanding cognitive security as an integrative political phenomenon, improves the classification of cognitive threats (by sources, levels, scale, instruments, and the effect of undermining resilience), and elaborates a component-based provision model (legal and regulatory, educational, communication-institutional, and technological blocks). Further development is provided to the conceptual and categorical framework, approaches to analyzing strategic narratives/counter-narratives, the methodology for comparative analysis of international practices, and proposals for integrating cognitive security into strategic planning and national security management as a foundation of the state's political and information sovereignty.

The practical significance of the results obtained lies in the fact that the provisions, conceptual approaches, and recommendations set out in the dissertation can be applied in several important areas. In particular, in the field of public policy and security, the findings may serve as a basis for developing and implementing a comprehensive strategy to ensure Ukraine's cognitive security under conditions of hybrid war, including the creation of mechanisms for monitoring cognitive threats, building a system to counter information and psychological operations, strengthening citizens' cognitive resilience, and improving communication policy in the domain of strategic narratives; in the research sphere, the dissertation materials may be useful for further studies in political science, security studies, communication, and social psychology, including identifying the cause-and-effect links of Russia's hybrid aggression against Ukraine and analyzing socio-political factors that generate new challenges to political stability, state unity, and democratic development, which will deepen scholarly understanding of how cognitive threats affect political processes and contribute to improving political practice; in education, the results can be used in preparing lectures, curricula, textbooks, and manuals for courses such as "Political

Science," "Mass Media in the Political Life of Society," "Media Literacy," "Political Psychology," "Information Security," and "Hybrid War," as well as in the research work of undergraduate students, master's students, and PhD candidates studying information security, political communication, state security, and the cognitive domain; and in practical terms, the developed provisions may be applied in the implementation of socio-political reforms, the transformation of public authorities and security institutions, and the formation of new approaches to governing social processes under hybrid threats, as well as in the activities of public authorities, civil society organizations, think tanks, and media structures working in information policy, crisis response, strategic communications, and information counteraction against the aggressor.

Keywords: geopolitics, hybrid warfare, disinformation, state information policy, information security, information warfare, information and communication mechanisms of interaction, information space, cognitive threats, media, national security, national identity, political space, russian propaganda, Ukraine.

СПИСОК ОПУБЛІКОВАНИХ ПРАЦЬ ЗА ТЕМОЮ ДИСЕРТАЦІЇ

Статті у наукових фахових виданнях України категорії Б:

1. Кобець Т. Основні підходи до розуміння «когнітивна безпека» в сучасній науці: політичний та інформаційний аспект. *Вісник Львівського університету. Серія філософсько-політологічні студії.* 2023. Вип. 49. С.278–285.

DOI: https://doi.org/10.30970/PPS.2023.49.34

URL: http://fps-visnyk.lnu.lviv.ua/archive/49_2023/34.pdf

2. Кобець Т. Когнітивна безпека в умовах гібридної війни. *Вісник Прикарпатського університету. Серія: Політологія*. 2024. Випуск 17. С.67–73.

DOI: https://doi.org/10.32782/2312-1815/2024-17-9

URL: https://journals.pnu.if.ua/index.php/politology/article/view/116/114

3. Кобець Т. Аналіз загроз когнітивній безпеці українського суспільства: класифікаційні підстави. *Вісник Прикарпатського університету. Серія: Політологія.* 2024. Випуск 19. С.67–72.

DOI: https://doi.org/10.32782/2312-1815/2024-19-8

URL: https://journals.pnu.if.ua/index.php/politology/article/view/182/178

4. Кобець Т. Використання технологій інформаційних операцій у політичній практиці. *Літопис Волині*. 2024. № 31. С.134–139

DOI: https://doi.org/10.32782/2305-9389/2024.31.21

URL: http://litopys.volyn.ua/index.php/litopys/article/view/562/493

5.Кобець Т. Інформаційні спеціальні операції: особливості реалізації в сучасних умовах. *Вісник Прикарпатського університету. Серія: Політологія*. 2025. Випуск 20. С.256–263.

DOI: https://doi.org/10.32782/2312-1815/2025-20-30

URL: https://journals.pnu.if.ua/index.php/politology/article/view/246/241

Публікації, у періодичних наукових виданнях інших держав, які індексуються у базах даних Scopus:

6. Ivanytska B., Kobets T., Savchenko V., Pugachov V., Kursyk O. Countering Disinformation in the Hybrid Information Environment: A Cross-Sectoral Analysis of Public Policy, Education, and Media Strategies. *Ianna Journal of Interdisciplinary Studies*. 2026. № 8 (1). P.327–343.

DOI: https://doi.org/10.5281/zenodo.17710407

URL: https://scopus.com/pages/publications/105028731483?origin=resultslist

Наукові праці, які засвідчують апробацію матеріалів дисертації:

7. Кобець Ю. В., Кобець Т. А. Теоретико-методологічні підходи до дослідження політичної безпеки. *Політичні процеси сучасності: глобальний та регіональні виміри*. Збірник матеріалів IV Всеукраїнської науково-практичної конференції (м. Івано-Франківськ, 27-28 жовтня 2022 р.). Івано-Франківськ, 2022. С.45–51.

URL: https://kpol.pnu.edu.ua/wp-content/uploads/sites/102/2024/07/zbirnyk-materialiv-vseukrainskoi-konferentsii-politychni-protsesy-suchasnosti-hlobalnyj-ta-rehionalnyj-vymiry-27-28-zhovtnia-2022r.-ch-i.pdf

8. Кобець Т. Безпека в умовах воєнного стану. *Освітній процес в умовах війни та у повоєнний період: виклики, правила, перспективи* : матеріали всеукраїнського науково-педагогічного підвищення кваліфікації, 4 березня – 14 квітня 2024 року. Львів – Торунь : Liha-Pres, 2024. С.146–149.

URL:https://cuesc.org.ua/images/informlist/%D0%9C%D0%B0%D0%BA%D0%B5%D1%82%20advanced_training_UDU.pdf

9. Кобець Ю.В., Кобець Т.А. Когнітивна війна як сучасна форма ведення мережево-центричного протистояння. *Політичні процеси сучасності: глобальний та регіональний виміри*. Збірник матеріалів V Міжнародної науково-практичної конференції (м. Івано-Франківськ, 25-26 квітня 2024 р.). Івано-Франківськ, 2024. С.217–238.

URL: https://kpol.pnu.edu.ua/wp-content/uploads/sites/102/2024/12/zbirnyk-materialiv-v-mizhnarodnoi-naukovo-praktychnoi-konferentsii-politychni-protsesy-suchasnosti-hlobalnyj-ta-rehionalnyj-vymiry-2024r.pdf

10. Кобець Т. А. Вплив національної ідентичності на формування інформаційної та когнітивної безпеки українського суспільства. *Політичні процеси сучасності: глобальний та регіональні виміри :* збірник матеріалів VI Міжнародної науково-практичної конференції (м. Івано-Франківськ, 8–9 квітня 2025 р.). Електронне видання. Івано-Франківськ : Карпат. нац. ун-т ім. В.Стефаника, 2025. С.171–174.

URL: https://kpn.cnu.edu.ua/wp-content/uploads/sites/197/2025/11/zbirnyk-materialiv-vi-mizhnarodnoi-naukovo-praktychnoi-konferentsii.pdf

11. Кобець Т.А. Особливості верифікації даних журналістом в епоху штучного інтелекту. *Global Trends in the Development of Information Technology and Science:* Collection of Scientific Papers "International Scientific Unity" with Proceedings of the 3rd International Scientific and Practical Conference. April 2-4, 2025. Stockholm, Sweden. P. 135–138.

DOI: https://doi.org/10.70286/isu-02.04.2025

URL: https://isu-conference.com/wp-content/uploads/2025/04/Stockholm_Sweden_02.04.25.pdf

12. Кобець Т.А. Контекстуальна верифікація як елемент фактчекінгу. *Modern Scientific Research: Theoretical and Practical Aspects* (August 25-27, 2025, Riga, Latvia). European Open Science Space, 2025. P.48–52.

DOI: https://doi.org/10.70286/EOSS-25.08.2025

URL: https://www.eoss-conf.com/wp-content/uploads/ 2025/08/Riga_Latvia_25.08.25.pdf

Праці, які додатково відображають наукові результати дисертації:

13. Кобець Т. Порівняльний аналіз технологій пропаганди та контрпропаганди в умовах воєнного стану. *Вісник Прикарпатського університету*. Серія: Політологія. 2023. Випуск 15. С.33–42.

DOI: https://doi.org/10.32782/2312-1815/2024-1-5

URL: https://journals.pnu.if.ua/index.php/politology/article/view/51/50

ЗМІСТ

ПЕРЕЛІК СКОРОЧЕНЬ І УМОВНИХ ПОЗНАЧЕНЬ……..21
ВСТУП……...22
РОЗДІЛ 1. ТЕОРЕТИКО-КОНЦЕПТУАЛЬНІ ЗАСАДИ КОГНІТИВНОЇ БЕЗПЕКИ В НАУЦІ…….…….35
1.1.Концепт «когнітивна безпека» в науці: стан наукової розробки проблематики…….35
1.2.Політико-інформаційний складник когнітивної безпеки: теоретичні підходи та концептуалізація механізмів захисту……...51
РОЗДІЛ 2. КОГНІТИВНА БЕЗПЕКА УКРАЇНСЬКОГО СУСПІЛЬСТВА В УМОВАХ ГІБРИДНОГО ПРОТИСТОЯННЯ…….69
2.1. Аналіз та класифікація загроз когнітивній безпеці українського суспільства …….69
2.2. Гібридна війна як загроза когнітивній безпеці сучасного суспільства…….82
2.3. Когнітивна війна як інструмент гібридного протистояння: виклики для когнітивної безпеки …….91
РОЗДІЛ 3. ІНФОРМАЦІЙНІ СПЕЦІАЛЬНІ ОПЕРАЦІЇ ТА ТЕХНОЛОГІЇ КОГНІТИВНОГО ВПЛИВУ В УМОВАХ ВОЄННОГО СТАНУ…….…..106
3.1. Когнітивний аспект використання технологій інформаційних операцій в політичній практиці ……106
3.2. Інформаційні спеціальні операції: особливості впливу на свідомість в сучасних умовах……...117
3.3. Порівняльний аналіз технологій пропаганди та інформаційних операцій в умовах воєнного стану: досвід України…….129
РОЗДІЛ 4. МОДЕЛЬ ФОРМУВАННЯ КОГНІТИВНОЇ БЕЗПЕКИ СУЧАСНОЇ УКРАЇНИ……...……..146
4.1. Роль когнітивної безпеки у формуванні та збереженні легітимності політичної влади: виклики для України……146

4.2. Вплив національної ідентичності на формування когнітивної безпеки українського суспільства: політико-інформаційні аспекти…….161
4.3. Формування когнітивної стійкості (резильєнтності) в суспільстві як компоненту когнітивної безпеки в сучасній Україні……170
ВИСНОВКИ…….190
СПИСОК ВИКОРИСТАНИХ ДЖЕРЕЛ……199
ДОДАТКИ……...….231

ПЕРЕЛІК СКОРОЧЕНЬ І УМОВНИХ ПОЗНАЧЕНЬ

ГЕС	Гідроелектростанція
ЄС	Європейський Союз
ЗМІ	Засоби масової інформації
ЗСУ	Збройні сили України
ЗУ	Закон України
ІКТ	Інформаційно-комунікаційні технології
ІПВ	Інформаційно-психологічний вплив
ІПО	Інформаційно-психологічні операції
ІПСО	Інформаційно-психологічні спеціальні операції
КНП	Координована неавтентична поведінка
НБ	Національна безпека
ПЗ	Програмне забезпечення
РНБО	Рада безпеки і оборони України
рф	російська федерація
СІО	Спеціальні інформаційні операції
Ст	Стаття
ЦПД	Центр протидії дезінформації
ШІ	Штучний інтелект
DDoS-атака	Denial of service attack
DGI	Індекс цифрового врядування
DHS	Департамент внутрішньої безпеки
GDPR	Загальний регламент про захист даних
GPT	Generative Partained Transformer
HME	Human machine engagement
HMI	Human machine interface
NATO	North Atlantic Treaty Organization
OODA/ СОРД	Спостереження, Орієнтація, Рішення, Дія
PSYOPS	Психологічні операції

ВСТУП

Актуальність теми. В умовах тривалої гібридної війни, спрямованої проти України, питання когнітивної безпеки набуло особливого значення. Сучасне інформаційне середовище стало полем не лише комунікації, а й бойових дій, де об'єктом атаки виступає не фізична інфраструктура, а людська свідомість, ментальні структури, національна ідентичність і здатність до критичного мислення. Це визначає когнітивну безпеку як одну з ключових передумов національної безпеки, політичної стабільності та збереження суб'єктності держави в глобальному середовищі.

З початку повномасштабної збройної агресії російської федерації (далі – рф) проти України інтенсивність інформаційно-психологічних операцій зросла до безпрецедентного рівня. Дезінформація, маніпуляція наративами, розпалювання недовіри до державних інституцій, використання технологій дипфейків, мікротаргетинг та алгоритмічне програмування контенту – усе це трансформувало уявлення про безпеку. Традиційні засоби захисту виявилися недостатніми для протидії новітнім загрозам, які функціонують непомітно, але з глибоким і довготривалим ефектом.

Когнітивна безпека охоплює питання захисту свідомості громадян від зовнішнього інформаційного тиску, внутрішніх деструктивних процесів, а також від порушення здатності до рефлексії, аналізу, ухвалення обґрунтованих рішень. Йдеться про забезпечення такої стійкості мислення, яка дозволяє протистояти спробам нав'язати викривлену картину світу, підмінити історичну пам'ять, делегітимізувати державу та деморалізувати суспільство.

Актуальність дослідження когнітивної безпеки також зумовлена розвитком технологій штучного інтелекту, які радикально змінюють механізми виробництва, поширення і споживання інформації. У 2026 році спостерігається зростання загроз, пов'язаних з автоматизованим формуванням контенту, зниженням ролі традиційних медіа та посиленням інформаційних монополій. Це створює передумови для масового когнітивного викривлення – явища, коли

мільйони користувачів одночасно потрапляють у сфери інформаційної ізоляції та ідеологічної інженерії.

У політичному вимірі когнітивна безпека є чинником, що впливає на легітимність влади, рівень довіри до інституцій, ефективність управлінських рішень і національну єдність. У військовому вимірі – це елемент, від якого залежить моральний дух армії, стійкість тилу, підтримка міжнародної коаліції. У соціальному – вона визначає здатність суспільства протистояти страху, хаосу, зневірі та когнітивному паралічу. Таким чином, когнітивна безпека є не лише академічною чи фаховою проблемою, а викликом загальнонаціонального масштабу.

Аналіз сучасного стану когнітивної безпеки України демонструє фрагментарність політики в цій сфері, відсутність системного нормативного забезпечення, низький рівень координації між суб'єктами безпекового середовища та недостатню інтеграцію питань когнітивного захисту в стратегії національної безпеки. Це підтверджує необхідність глибокого наукового осмислення проблеми, розробки теоретичних засад, категоріального апарату, стратегічних орієнтирів і практичних механізмів протидії.

Серед основних загроз когнітивній безпеці України в сучасних умовах виокремлюються такі: систематичне ведення інформаційно-психологічних операцій з боку ворожих держав; масове поширення дезінформації та фейкових новин; використання алгоритмічних механізмів впливу на поведінку користувачів соціальних мереж; технології глибоких фейків, що здатні підривати довіру до лідерів суспільної думки та інституцій; програмування негативних емоційних станів через спеціально сконструйований медіаконтент. З огляду на багатовимірний характер загроз, модель когнітивної безпеки для України повинна мати інтегрований характер.

Теоретико-методологічне підґрунтя дослідження когнітивної безпеки України в умовах гібридної війни становить широкий спектр сучасної міждисциплінарної історіографії. У центрі наукової уваги перебувають когнітивна безпека, стійкість, маніпуляція суспільною свідомістю,

інформаційно-психологічні операції, стратегічні комунікації, інформаційна війна та цифрові загрози.

Вагомий внесок у розвиток теорії когнітивної безпеки здійснили українські дослідники: А. Геращенко, О. Гіда, В. Горбулін, О. Данільян, О. Дзьобан, М. Загірняк, К. Захаренко, О. Зозуля, С. Корнієнко, Н. Крилова, О. Литвиненко, В. Ліпкан, В. Марков, О. Мороз, І. Ніколаєв, Г. Почепцов, І. Рущенко, Т. Ткачук, О. Фомін, Л. Харченко, С. Шевченко, М. Яремчук та інші.

Питання безпеки та захисту національного інформаційного простору досліджували численні науковці, зокрема Б. Кормич, В. Ліпкан, А. Марущак, С. Матвієнків, В. Петрик та інші. Проблеми безпеки в мережі були предметом аналізу таких фахівців, як С. Базарний, О. Дубас Ю. Гаркушелко, С. Герасимов, Ю. Жданов, Р. Лук'янчук, С.Шевченко, та інші. Проте розглядали інформаційна та кібернетична безпека зазвичай як складник національної безпеки, без детального аналізу загроз, джерел їхнього виникнення, технологій ведення когнітивних війн і психологічних операцій.

Особлива увага в роботах українських науковців зосереджена на таких проблемах, як когнітивна війна (Г. Почепцов), стратегічні наративи та контрнаративи (О. Мороз), цифрова грамотність та опір маніпуляціям (О. Золотар), інформаційна безпека в період воєнного стану (В. Галіпчак, О. Курбан).

В українському науковому дискурсі проблеми гібридної війни та її наслідків для національної і когнітивної безпеки досліджували В.Горбулін, О. Данільян, С. Дерев'янко, О. Дзьобан, В. Ліпкан, М. Литвин, О. Мороз, Г. Почепцов, Ю. Радковець, І. Рущенко, С. Шевченко, які акцентують на інформаційно-психологічних операціях, маніпуляції наративами, підриві ідентичності та ерозії довіри до державних інституцій як ключових інструментах гібридної агресії російської федерації проти України.

Значну увагу приділено також філософсько-політичним та інституційним аспектам когнітивної безпеки, зокрема питанням нормативно-правового регулювання (В. Петрик, В. Присяжнюк), структурного місця когнітивної безпеки в політиці національної безпеки (Ю. Радковець, В. Гусаров), ролі

держави та суспільства в зміцненні когнітивної стійкості (Н. Дніпренко, І. Проноза, І. Зіма).

У міжнародному вимірі формуванню теоретичної бази когнітивної безпеки сприяли праці Б. Б'юкенена, Ф. Вебстера, К. Воттса, К. Джайлза, Я. Каленського, Р. Кларка, М. Лібікі, Т. Маурера, Б. Німмо, А. Ратмелла, Т. Ріда, Р. Сілі, П. Сінгера, Г. Тамбера, С. Фелдстайна, А. Фрідмана, які розглядали інформаційні впливи, стратегічні комунікації та інформаційне протиборство як основні засоби сучасної війни.

Таким чином, історіографія проблеми когнітивної безпеки охоплює широкий комплекс українських і зарубіжних джерел, які свідчать про зростання наукового інтересу до феномену захисту свідомості як ключового елементу сучасної безпекової парадигми.

Узагальнення та аналіз цих позицій стали основою формування власної наукової позиції автора дисертації і довели, що дослідження когнітивної безпеки в умовах гібридної війни є не лише науково важливим, а й суспільно необхідним. Воно створює передумови для формування нового безпекового напряму, що відповідає викликам XXI століття та інтегрує гуманітарні, технологічні й стратегічні підходи до збереження суверенітету, демократії та ідентичності України

Зв'язок роботи з науковими програмами, планами, темами. Тема дисертаційного дослідження затверджена Вченою радою Прикарпатського національного університету імені Василя Стефаника (протокол № 09 від 01 листопада 2022 року). Дисертаційне дослідження здійснене на кафедрі політичних наук у рамках наукової теми кафедри «Трансформація сучасної політичної системи України: внутрішньополітичні виклики та зовнішні впливи» за номером державної реєстрації 0117U004396. Внесок автора полягає в обґрунтуванні теоретичних засад і формуванні практичних підходів до забезпечення когнітивної безпеки в умовах гібридної війни, спрямованих на зміцнення стійкості суспільної свідомості, протидію інформаційно-психологічним впливам та збереження національної ідентичності.

Мета і завдання дослідження. Метою дисертаційного дослідження є розробка теоретичних та прикладних основ забезпечення інформаційно-політичного складника когнітивної безпеки України в умовах гібридної війни з акцентом на формуванні стійкості суспільної свідомості, захисті від інформаційно-психологічного впливу та зміцненні національної ідентичності.

Для досягнення визначеної мети сформульовано такі основні завдання:

– систематизувати теоретичні підходи до розуміння категорії «когнітивна безпека»;

– здійснити дослідження та класифікацію загроз когнітивній безпеці з огляду на різноманітні критерії та підстави, особливо зважити на особливості психологічних аспектів безпеки захисту національного інформаційного простору через реальні й потенційні загрози та деструктивні пропагандистсько-маніпулятивні інформаційні впливи;

– провести концептуальний аналіз понять «гібридна війна» та «когнітивна війна» як форм деструктивного впливу на суспільство;

– охарактеризувати інструменти когнітивного впливу, що використовуються у межах гібридної агресії проти України;

– здійснити компаративний аналіз технологій пропаганди та інформаційних операцій в умовах воєнного стану;

– провести порівняльний аналіз міжнародного досвіду (на прикладі США та Естонії) у сфері протидії дезінформації та забезпечення когнітивної безпеки з метою виокремлення апробованих механізмів та моделей.

Об’єктом дисертаційного дослідження є когнітивна безпека в умовах гібридного протистояння.

Предметом дисертаційного дослідження є інформаційно-політичні аспекти забезпечення когнітивної безпеки України: концептуалізація та стратегічні орієнтири в умовах внутрішніх та зовнішніх інформаційно-психологічних загроз.

Методи дослідження. У дисертації застосовано комплекс загальнонаукових, спеціальних і міждисциплінарних методів, які забезпечили

системне осмислення когнітивної безпеки держави в умовах гібридної війни. Комплексний характер теми вимагає використання мультидисциплінарного підходу. Це зумовлено тим, що когнітивна безпека охоплює політичні, інформаційні, соціальні, психологічні та технологічні аспекти впливу на свідомість, ухвалення рішень та суспільну стійкість.

- Аналіз та синтез – використовувалися для деталізації сутності когнітивної безпеки, формулювання концептуальних підходів до її визначення, а також розгляду її взаємозв'язку з іншими сферами безпеки (розділи 1.1, 1.2).
- Узагальнення – для систематизації теоретичних позицій, підходів та емпіричних спостережень щодо когнітивної безпеки з подальшим формулюванням авторських висновків і пропозицій (розділи 1.1, 1.2).
- Порівняльний аналіз використано для дослідження підходів до забезпечення когнітивної безпеки в різних країнах, порівняння механізмів протидії пропаганді, інформаційним-психологічним операціям та іншим когнітивним загрозам з огляду на досвід держав, які вже стикалися з гібридними формами війни (зокрема, Литва, Естонія, Грузія, Ізраїль). Порівняльний аналіз застосовувався для порівняння національних моделей забезпечення когнітивної безпеки в Україні та за кордоном (зокрема, у США, Ізраїлі, Тайвані, країнах НАТО і ЄС); зіставлення стратегій реагування на гібридні загрози, дезінформацію, пропаганду та ІПСО (інформаційно-психологічні операції) в різних політичних контекстах (розділи 1.1, 1.2); аналізу еволюції пропагандистських практик та їхньої адаптації до цифрового середовища, соціальних мереж та алгоритмічних платформ (розділи 2.1, 2.2, 4.1).
- Системний аналіз дозволив встановити взаємозв'язки між когнітивною, інформаційною, кібер- та національною безпекою, а також розглянути когнітивну безпеку як інтегральний елемент політичної стабільності (розділи 4.1, 4.2, 4.3).
- Моделювання використовувалось для побудови концептуальної моделі когнітивної безпеки, визначення її складників, механізмів реалізації та стратегічних сценаріїв у державній політиці (розділи 4.1-4.3). Моделювання

застосовано для розробки структурної моделі когнітивної безпеки, зокрема з урахуванням сценаріїв загроз, ступенів вразливості та шляхів підвищення резильєнтності на індивідуальному, інституційному та національному рівнях.

- Дискурс-аналіз дозволив вивчити структуру й зміст стратегічних наративів, мову когнітивної агресії, а також механізми легітимації чи делегітимації суб'єктів у політичному дискурсі (розділ 4.1).
- Контент-аналіз застосовано для дослідження стратегічних, законодавчих, аналітичних матеріалів, офіційних рішень, а також позицій міжнародних організацій щодо когнітивної безпеки, протидії дезінформації та впливу ШІ (розділи 1.2, 2.3, 3.2) та для аналізу інформаційних потоків, каналів поширення дезінформації, цільових груп когнітивного впливу та характеру інформаційних атак (розділи 2.2, 3.2).
- Неоінституційний метод використано для аналізу інституційної архітектури забезпечення когнітивної безпеки, зокрема ролі державних органів, сектору безпеки і оборони, медіа, громадянського суспільства та міжнародних партнерів у формуванні й реалізації політик протидії когнітивним загрозам (розділи 1.2, 4.1, 4.3).
- Темпоральний метод застосовано для відтворення динаміки еволюції когнітивних загроз і трансформації інструментів впливу в часовому вимірі, а також для періодизації розвитку політико-інформаційних механізмів протидії. Завдяки темпоральному аналізу простежено зміни характеру когнітивної війни та інформаційно-психологічних операцій у різні етапи гібридної агресії, що дало змогу визначити закономірності ескалації, адаптації та ускладнення технологій впливу (розділи 1.2, 3.2, 4.1, 4.3).
- Статистичний метод використано для кількісного опису й узагальнення емпіричних проявів когнітивних загроз та їхніх соціально-психологічних ефектів, зокрема через аналіз результатів соціологічних опитувань, моніторингових звітів, індикаторів медіаспоживання та показників поширення інформаційних кампаній у цифровому середовищі.

- Нормативний метод застосовано для аналізу нормативно-правового та стратегічного підґрунтя забезпечення когнітивної безпеки, а також для оцінки відповідності наявних політик заявленим цілям національної безпеки (розділ 1.2, 1.3).

Наукова гіпотеза ґрунтується на положенні, що політико-інформаційний складник когнітивної безпеки в сучасних гібридних конфліктах виступає системним інструментом забезпечення стійкості політичної системи, оскільки визначає, яким чином інформаційні потоки, комунікаційні практики та наративні конструкції впливають на суспільну свідомість, політичні установки й легітимаційні механізми. Його результативність залежить від здатності держави та суспільних інституцій синхронно поєднувати три взаємопідсилювальні компоненти: (1) інформаційно-психологічний вимір протидії, що мінімізує емоційне зараження, панічні настрої та маніпулятивні ефекти; (2) технологічний вимір управління інформаційним середовищем (моніторинг, аналітика, протидія координованим кампаніям, алгоритмічному підсиленню та мережевим операціям, включно з ШІ-контентом), який забезпечує швидкість і масштаб реагування; (3) наративно-комунікаційний вимір, що формує смисловий каркас публічної політики, забезпечує узгоджені стратегічні комунікації та підтримує сталі інтерпретаційні рамки, через які суспільство осмислює події. У сукупності ці чинники визначають здатність держави зберігати довіру до інституцій і легітимних джерел, запобігати поляризації та нейтралізувати делегітимаційні впливи, які підривають керованість політичної системи та знижують спроможність до мобілізації в умовах війни.

Наукова новизна та теоретичне значення одержаних результатів дисертаційного дослідження полягає в концептуалізації когнітивної безпеки як самостійного стратегічного напряму державної політики в умовах гібридної війни, а також у розробці теоретичних, методичних і прикладних підходів до її забезпечення в контексті політичної безпеки та інформаційного суверенітету України.

Уперше запропоновано:

– концепт когнітивного суверенітету як стратегічної мети національної безпекової політики, що передбачає здатність держави зберігати контроль над своїм ментальним простором, захищати суспільну свідомість від зовнішнього впливу та формувати національні смисли у внутрішньому й міжнародному комунікативному середовищі;

– структурно-функціональну модель когнітивної безпеки України як складника політичної безпеки, що охоплює блоки когнітивної стійкості, публічної комунікації, інформаційного захисту, наративної стратегії, освітньо-просвітницької діяльності та міжнародної координації; модель може бути використана для стратегічного планування та розробки національної політики у сфері когнітивної безпеки.

У дисертаційні роботі *удосконалено:*

– теоретико-методологічні підходи до розуміння когнітивної безпеки як інтегративного політичного феномену, що охоплює інформаційні, психологічні, соціальні, культурні та технологічні виміри безпеки держави, а також забезпечує захист свідомості громадян від деструктивних впливів у гібридній війні;

– класифікацію когнітивних загроз у політичному просторі за джерелом походження, рівнем реалізації, масштабом впливу, інструментами здійснення (дезінформація, ІПСО, пропаганда, дипфейки, алгоритмічні атаки) та ступенем підриву суспільної стійкості;

– модель когнітивної безпеки України, що передбачає чотири ключові компоненти: нормативно-правовий (законодавче регулювання та стандарти), освітній (медіаграмотність, критичне мислення), комунікаційно-інституційний (участь держави, медіа, громадськості) та технологічний (системи моніторингу, виявлення і нейтралізації когнітивних атак);

– концептуальні підходи до аналізу стратегічних наративів та контрнаративів у межах когнітивної війни, а також методику їх використання для посилення політичної стійкості, згуртованості суспільства та легітимації державних інституцій;

– методологічні засади порівняльного аналізу когнітивної безпеки, що дозволили зіставити міжнародні практики (НАТО, Ізраїль, США) та виробити рекомендації щодо імплементації успішних моделей в українському безпековому контексті;

– механізми забезпечення когнітивної резильєнтності – здатності особистості, громади та держави зберігати критичне мислення, ідентичність і раціональність у ситуації масованого інформаційного впливу.

Новий рівень розвитку в науковій роботі отримали:

– понятійно-категоріальний апарат дослідження, зокрема трактування термінів «когнітивна безпека», «когнітивна війна», «когнітивна стійкість», «гібридна агресія», «ментальні операції», а також їх співвідношення з поняттями «інформаційна безпека», «національна безпека», «політична стабільність»;

– підходи до структуризації механізмів забезпечення когнітивної безпеки з урахуванням політичного контексту, інформаційного середовища, інституційного потенціалу та глобальних викликів, спричинених цифровізацією;

– науково-практичні підходи до побудови стратегій публічної комунікації як інструменту посилення довіри до інституцій, згуртування суспільства та забезпечення суб’єктності України в міжнародному дискурсі в умовах гібридної війни;

– пропозиції щодо інтеграції когнітивної безпеки в систему стратегічного планування та національного безпекового менеджменту, створення системи когнітивного моніторингу, законодавчого регулювання, аналітики та освітніх ініціатив;

– бачення когнітивної безпеки як основи політичного та інформаційного суверенітету держави, що забезпечує її здатність протидіяти гібридним впливам і зберігати єдність у ситуації екзистенційних загроз.

Практичне значення отриманих результатів полягає в тому, що викладені в дисертації положення, концептуальні підходи та рекомендації можуть бути використані в кількох важливих сферах. Зокрема, у сфері державної політики та безпеки результати дослідження можуть слугувати основою для формування і

реалізації комплексної стратегії забезпечення когнітивної безпеки України в умовах гібридної війни. Напрацьовані в роботі теоретичні моделі здатні допомогти державним органам у створенні механізмів моніторингу когнітивних загроз, побудові системи протидії інформаційно-психологічним операціям, підвищенні когнітивної стійкості громадян, а також удосконаленні комунікативної політики у сфері стратегічних наративів.

У науково-дослідній сфері матеріали дисертації можуть бути корисними для подальших досліджень у галузі політичної науки, безпекових студій, комунікацій, соціальної психології, зокрема для виявлення причинно-наслідкових зв'язків гібридної агресії росії проти України, аналізу соціально-політичних чинників, що зумовлюють нові виклики для політичної стабільності, державної єдності та демократичного розвитку. Це дозволить поглибити наукове розуміння механізмів впливу когнітивних загроз на політичний процес і сприятиме вдосконаленню політичної практики. У навчальному процесі результати дослідження можуть бути використані при підготовці лекцій, навчальних програм, підручників та посібників із дисциплін «Політологія», «Масмедіа в політичному житті суспільства», «Медіаграмотність», «Політична психологія», «Інформаційна безпека», «Гібридна війна» тощо. Матеріали дисертації можуть також бути корисними для науково-дослідної роботи студентів, магістрантів та аспірантів, які вивчають питання інформаційної безпеки, політичної комунікації, державної безпеки та когнітивної сфери. У практичній площині напрацьовані положення можуть бути використані під час реалізації соціально-політичних реформ, трансформації органів державної влади та безпеки, формування нових підходів до управління суспільними процесами в умовах гібридних загроз. Вони також можуть бути застосовані в діяльності органів державної влади, громадських організацій, аналітичних центрів і медіаструктур, що працюють у сфері інформаційної політики, кризового реагування, стратегічних комунікацій та інформаційної протидії агресору.

Особистий внесок здобувача полягає у комплексному опрацюванні проблематики когнітивної безпеки як нового стратегічного напряму

національної безпеки України в умовах гібридної війни. Здобувач всебічно актуалізував сучасну історіографію, міждисциплінарні підходи та джерельну базу, що дозволило системно проаналізувати когнітивний вимір у структурі політичної безпеки держави.

У процесі дослідження було вперше обґрунтовано авторське бачення когнітивної безпеки як ключового домену стратегічного протистояння в умовах сучасної війни, що охоплює як зовнішньоагресивні інформаційно-психологічні впливи, так і внутрішні фактори політичної стабільності та соціальної єдності. Внеском здобувача є також формулювання авторського визначення понять «когнітивна безпека», «когнітивна стійкість» та «когнітивна війна» в контексті національної безпеки, їхнє теоретичне розмежування з інформаційною та кібербезпекою.

Розроблено концептуальну модель когнітивної безпеки, яка бере до уваги специфіку гібридних загроз, роль стратегічних наративів, інституційну взаємодію між органами державної влади, громадянським суспільством і медіа, а також потребу формування когнітивної резильєнтності як захисного механізму суспільства. Обґрунтовано принципи побудови ефективної політики у сфері когнітивної безпеки з урахуванням воєнно-політичних, інформаційно-комунікаційних та соціокультурних чинників.

Автор самостійно здійснив аналіз основних когнітивних загроз, систематизував форми й механізми маніпулятивного впливу в інформаційному середовищі, запропонував стратегічні орієнтири для державної політики у сфері захисту когнітивного простору. У роботі застосовано інноваційний міждисциплінарний підхід, який поєднує інструменти політичної науки, комунікативістики, безпекових студій та нейропсихології.

Усі теоретичні положення, аналітичні висновки та практичні рекомендації, винесені на захист, отримані здобувачем самостійно, є обґрунтованими, достовірними та можуть бути використані в науковій, освітній та практичній діяльності.

Апробація результатів дослідження. Основні положення, наукові

результати та висновки дисертаційної роботи були обговорені на засіданнях кафедри політичних наук Карпатського національного університету імені Василя Стефаника, що засвідчило їхню наукову новизну та практичну значущість.

Результати дослідження апробовані під час виступів на наукових і науково-практичних конференціях різного рівня, зокрема IV Всеукраїнській науково-практичній конференції «Політичні процеси сучасності: глобальний та регіональні виміри» (м. Івано-Франківськ, 27-28 жовтня 2022 р.), V Міжнародній науково-практичній конференції «Політичні процеси сучасності: глобальний та регіональний виміри» (м. Івано-Франківськ, 25–26 квітня 2024 р.), VI Міжнародній науково-практичній конференції «Політичні процеси сучасності: глобальний та регіональні виміри» (м. Івано-Франківськ, 8–9 квітня 2025 р.), 3rd International Scientific and Practical Conference «Global Trends in the Development of Information Technology and Science» (Stockholm, Sweden, 2–4 april, 2025), European Open Science Space «Modern Scientific Research: Theoretical and Practical Aspects» (Riga, Latvia, 25–27 august, 2025).

Публікації. Матеріали дисертаційної роботи викладені в 13 наукових публікаціях, зокрема, 5 статей – у наукових фахових виданнях України категорії Б; 1 стаття – у фаховому науковому журналі, який індексується наукометричною базою Scopus; 1 стаття, яка додатково відображає результати дослідження; 6 тез і матеріалів наукових конференцій.

Структура та обсяг дисертації. Дисертація складається зі вступу, чотирьох розділів, що поділяються на дванадцять підрозділів, висновків, списку використаних джерел та літератури, який налічує 275 позицій, з них 86 – іноземними мовами, і додатків (на 7 сторінках). Загальний обсяг дисертації – 238 сторінок, з них основний текст – 178.

РОЗДІЛ 1. ТЕОРЕТИКО-КОНЦЕПТУАЛЬНІ ЗАСАДИ КОГНІТИВНОЇ БЕЗПЕКИ В НАУЦІ

1.1. Концепт «когнітивна безпека» в науці: стан наукової розробки проблематики

В сучасну епоху питання когнітивної безпеки набуває критичного значення. Лавиноподібне поширення неправдивої інформації, фальшивих новин та цифрових загроз руйнує довіру до інформаційного простору. Громадяни стають беззахисними перед інформаційними атаками, поступово втрачаючи навички аналітичного мислення. Наслідком цього є розповсюдження хибних переконань та загострення суспільно-політичних суперечностей.

Брак належної когнітивної захищеності негативно впливає на якість рішень, сприяє зростанню популістичних настроїв та екстремізму. Руйнування довіри до медіа та державних органів створює загрозу для суспільної стабільності. Тому розвиток когнітивної безпеки є ключовим для захисту інформаційного простору та підтримання демократичних принципів.

Когнітивна безпека – фундаментальний елемент національної безпеки в сучасних умовах. Прогрес цифрових технологій породжує нові виклики, серед яких інформаційні війни, хакерські атаки та психологічний вплив. Створення когнітивного захисту передбачає формування в населення навичок аналітичного мислення, здатності виявляти фальшиві повідомлення та протистояти цифровим загрозам.

Ключовим фактором для посилення оборонного потенціалу країни є збереження авторитету державних структур та забезпечення соціальної стабільності. Більше того, когнітивна безпека покращує якість комунікації між владою та громадськістю, що становить основу ефективного державного управління та національної безпеки й оборони.

Когнітивна безпека набуває особливої актуальності в контексті гібридної агресії, коли поряд з традиційними військовими діями застосовуються

інформаційні, дипломатичні та фінансові важелі впливу. За таких обставин маніпулятивна пропаганда, психологічний тиск та кібернетичні операції стають потужною зброєю. Формування когнітивного захисту охоплює навчання населення методів виявлення та протидії маніпуляціям, розвиток умінь відрізняти достовірні факти від пропагандистських матеріалів, а також культивування критичного ставлення до інформації. Такий підхід знижує ефективність гібридних атак, підвищує опірність соціуму та зміцнює національну оборону. У контексті гібридного протистояння когнітивна безпека служить щитом проти інформаційних маніпуляцій, посилює стійкість громадянського суспільства та гарантує захист інформаційного суверенітету.

Посилення впливу психологічних чинників на суспільну свідомість, державне й політичне управління та інтерпретацію інформаційних потоків підкреслює актуальність всебічного дослідження поняття «когнітивна безпека». Детальне вивчення політичних та інформаційних вимірів цієї концепції створює підґрунтя для формування механізмів боротьби з інформаційними маніпуляціями, фальсифікацією даних та психологічними загрозами. Таким чином, дослідження цієї проблематики забезпечує більш повне розуміння сучасних небезпек і створення дієвих інструментів для підтримання суспільної стабільності та безпеки.

Усвідомлення ролі психологічних механізмів у соціальній динаміці набуває особливого значення в умовах трансформації медіапростору та розвитку цифрових технологій. Дослідження феномена «когнітивна безпека» відкриває можливості не тільки для вивчення психологічних основ сприйняття інформації, а й для створення методів підвищення інформаційної компетентності та аналітичного мислення населення. Аналіз політичних та інформаційних складників цього поняття забезпечує формування відповідних тактик протидії маніпулятивним впливам та пропагандистським кампаніям. Це становить принципово важливий етап у побудові стабільного інформаційного простору та підтриманні соціальної злагоди, що й визначає важливість обраної тематики дослідження.

Концепція когнітивної безпеки стала предметом численних досліджень українських науковців. Так, Л. Бєлкін визначає її як стійкість проти інформаційно-психологічних впливів на людину і суспільство, учений здійснив компаративний аналіз термінів «інформаційна безпека», «безпека інформації» та «когнітивна безпека», визначивши їхні взаємозв'язки та відмінності [13]. Н.Зубар пропонує більш широкий підхід, визначаючи когнітивну безпеку як концепцію, що охоплює заходи та стратегії для захисту когнітивних процесів, інтелектуальних зусиль та психологічного благополуччя як на індивідуальному, так і на колективному рівні. Таке бачення особливо актуальне в умовах цифрових технологій та онлайн-середовищ, де когнітивні процеси можуть зазнавати загроз або зловживань. Водночас Н. Зубар сфокусувалася на вивченні когнітивної безпеки України в умовах російської агресії повного масштабу. І. Рущенко розглядає когнітивну безпеку як сукупність загроз і ризиків, пов'язаних із пізнавальною діяльністю, негативними впливами масмедіа та перебуванням людини у віртуальній реальності [69, с. 267–270; 162].

З. Коваль присвятив свої дослідження аналізу психологічних аспектів воєнних конфліктів та їхнього впливу на історичний розвиток і сучасне соціальне середовище та акцентував на тому, що когнітивна безпека передбачає виявлення, аналіз і протидію загрозам, які виникають через маніпуляції мисленням, сприйняттям, увагою та ухваленням рішень [81, с. 79–84]. Її головною метою є забезпечення надійного функціонування інтелектуальних систем, запобігання зловживанням і злочинним впливам, а також підтримка довіри й прозорості у використанні штучного інтелекту та його впливу на суспільство. Н. Журибіда зосередився на дослідженні стратегічних завдань та функціональних характеристик економічної безпеки банківської сфери [66, с. 123]. С. Спасітєлєва, Ю. Жданова, І. Чичкань приділили увагу проблемам захисту універсальних систем управління інформацією [171].

У своїй праці «Війна в когнітивному просторі» Г. Почепцов підкреслює, що поширене уявлення про інформаційну війну як процес передачі чи поширення інформації є сутнісно неповним і обмеженим. На його думку, справжня суть

сучасного інформаційного протистояння полягає не стільки в русі інформаційних потоків, скільки в боротьбі наративів, що визначають спосіб мислення, сприйняття реальності й поведінкові реакції аудиторії [139]. Дослідник одним із перших у межах українського політологічного дискурсу вводить у науковий обіг поняття «інформаційна бульбашка» та «когнітивна безпека», демонструючи, що об'єктом впливу в інформаційній війні є не лише зовнішній інформаційний ландшафт, а передусім когнітивний простір особистості та суспільства загалом. Він аргументовано доводить, що саме когнітивний вимір, власне, система уявлень, переконань, цінностей і очікувань, стає головною мішенню будь-якої інформаційної агресії як у мирний час (зокрема під час виборчих кампаній), так і в умовах відкритого збройного конфлікту.

Як зазначає Г. Почепцов, узагальнюючи концептуальні підходи західних дослідників, сучасна інформаційна війна розгортається в чотирьох ключових вимірах: фізичному, соціальному, інформаційному та когнітивному. Когнітивний вимір охоплює сферу людського сприйняття, систему цінностей, переконань і ментальних моделей, що визначають процес ухвалення рішень. Саме в цьому вимірі вирішальну роль відіграють наративи, які стають основним інструментом впливу й зброєю в протистоянні між сторонами, які конфліктують [140].

З огляду на те, що російська стратегія ведення інформаційної війни та вплив на когнітивну безпеку відзначаються особливою агресивністю, постає нагальна потреба у впровадженні ефективних заходів протидії. Як зазначає Центр розвитку наукової політичної думки та ідеології, когнітивна війна в цьому контексті трактується як цілеспрямоване введення в інтелектуальний простір держави-противника хибних наукових теорій, концептуальних парадигм, стратегічних підходів і моделей, які впливають на процеси державного управління, підриваючи національні захисні механізми та ключові потенціали [162].

Колектив авторів, на чолі з С. Наумкіною, вводить у науковий обіг поняття «когнітивне виживання», пояснюючи, що людський та політико-правовий виміри національної безпеки набувають пріоритетного значення, поступово трансформуючись із другорядних компонентів у центральну основу, навколо якої має формуватися державна політика. Цей вимір має подвійну природу: з одного боку, він охоплює питання фізичного збереження нації – її демографічного потенціалу, стану здоров'я населення, розвитку людського капіталу; з іншого – забезпечує когнітивне виживання народу, що охоплює стійкість до інформаційно-психологічних впливів, збереження національної ідентичності, ціннісної орієнтації та готовності до спротиву [120, с. 99].

Актуальність дослідження цього комплексу проблем зумовлена екзистенційним характером загроз, з якими зіштовхнулась Україна через повномасштабну агресію. Демографічні втрати, загострені наслідками війни, та системні когнітивні атаки на ментальну сферу українського суспільства – це взаємозалежні складники гібридної стратегії виснаження та знищення, спрямованої як на фізичне, так і на ментальне послаблення нації.

Нехтування будь-яким із цих напрямів на користь винятково гуманітарного чи винятково безпекового підходу матиме стратегічно катастрофічні наслідки. Лише цілісна модель безпеки, що інтегрує фізичний, демографічний та когнітивний складники, здатна забезпечити стійкість держави в довготривалій перспективі [120, с. 100].

О. Топчій у своїх працях розглянула різноманітні аспекти інформаційної безпеки дітей та підлітків, запропонувавши інноваційні підходи до розв'язання цієї проблематики [175, с. 122–126].

О. Автюзенко проаналізував методологію та практичні засоби теорії ухвалення рішень для створення багаторівневих систем інформаційного захисту. В. Москаленко сконцентрувався на дослідженні когнітивних особливостей творчого мислення в процесі розв'язання складних надситуативних завдань [119, с. 107–113].

У західній науці домінує технологічний підхід до когнітивної безпеки. У той час як традиційні засоби кіберзахисту, зокрема, брандмауери та антивірусне програмне забезпечення, спрямовані на технічну безпеку цифрових пристроїв, в умовах зростання інформаційних загроз актуалізується новий вимір – когнітивна безпека. На думку К. Бейкера, цей напрям охоплює захист особистості від прихованого цілеспрямованого впливу дезінформації, дипфейків, маніпулятивних алгоритмів і медіанаративів, що мають на меті не порушення технічної інфраструктури, а втручання в процеси людського пізнання. Найуразливішим елементом цифрового середовища сьогодні часто виявляється не технічна вразливість мережі чи ненадійність пароля, а когнітивна сприйнятливість індивіда до маніпулятивного впливу [198].

Використовуючи пізнавально-інформаційний підхід до когнітивної безпеки, автори дослідження «Актуальні проблеми інформаційної безпеки» констатують, що сучасне постіндустріальне суспільство дедалі більше ґрунтується не на матеріальному виробництві, а на продукуванні інформації та знань. Ми перебуваємо в епосі стрімкого зростання інформаційних потоків і розвитку когнітивних (розумних) систем, де ключову роль відіграє когнітивний капітал – сукупність знань, пам’яті, мислення, мови та свідомості людини. Усе це робить пізнання центральним чинником людського й суспільного розвитку [2, с. 239].

Знання – це не просто сукупність фактів, а результат пізнавальної діяльності, що формує уявлення про закономірності світу. Інформація ж є лише інструментом, засобом передачі нових знань. Проблема сучасності полягає в підміні понять: спрощене тлумачення знання як інформації веде до втрати глибини розуміння та зниження рівня критичного мислення. У суспільстві знань основними сферами стають виробництво, обмін, розподіл і споживання знань. Важливу роль відіграють когнітивні працівники – ті, хто створює, передає, організовує та використовує знання. Фундаментальним чинником виступає також пізнання як процес здобуття істинного знання про дійсність. На цьому тлі поняття «інформаційна безпека» набуває нового звучання. Вона вже не

обмежується захистом технічної інфраструктури чи доступом до даних. Справжні загрози сьогодні пов’язані з дезінформацією, маніпуляцією свідомістю, порушенням когнітивної рівноваги. Саме тому зростає значення когнітивної безпеки як здатності особистості та суспільства протистояти спотворенню реальності, критично осмислювати інформацію, відновлювати смисли й ухвалювати обґрунтовані рішення. Когнітивна безпека стає продовженням і водночас поглибленням інформаційної безпеки, охоплюючи не лише технічні аспекти, а й мислення, переконання, цінності, емоційні реакції. Захист свідомості – це захист національного суверенітету в цифрову епоху [2, с. 240].

Отже, забезпечення когнітивної безпеки вимагає не лише технологічних засобів, а й стратегій, що охоплюють освіту, критичне мислення, інформаційну гігієну, стратегічні комунікації та формування смислової стійкості. У цьому полягає новий вимір безпеки в епоху знань.

Когнітивна безпека як міждисциплінарна галузь формується на перетині інформаційної безпеки, психології, нейронаук та комунікаційних стратегій. Вона покликана забезпечити стійкість до складних кампаній впливу, які можуть змінювати суспільні установки, фрагментувати колективну ідентичність або формувати поведінкові патерни через опосередковані імпульси. Цей динамічний напрям визнає, що захист у цифрову епоху означає не лише охорону інфраструктури, а й протидію впливу на способи мислення, ухвалення рішень та взаємодію людини з навколишнім світом.

У зв’язку з цим виникає необхідність осмислення когнітивної безпеки як стратегічного пріоритету як у державному, так і в корпоративному управлінні. Представлений аналітичний огляд слугує інтегрованим вступом до тематики когнітивної безпеки, її викликів та перспектив для сучасних інституцій. В. Богданович працював над створенням методології когнітивного моделювання деструктивного впливу гібридних загроз на державну безпеку [15-16]. О.Дергильова розробляла концептуальну модель науково-технічного сектору в системі забезпечення оборонної безпеки країни [53].

Г. Тараненко акцентує на внутрішніх та зовнішніх аспектах когнітивної безпеки, яка є одним із ключових вимірів сучасної війни за Незалежність України. У центрі когнітивної війни – цілеспрямований вплив на пізнавальні процеси людини: її здатність до раціонального осмислення дійсності, критичного мислення та ухвалення обґрунтованих рішень. Основна мета такого типу війни – завоювання «умів і сердець» людей через формування викривленого сприйняття дійсності. Відповідно, завдання когнітивної безпеки полягає в зміцненні стійкості особистості до шкідливих інформаційно-психологічних впливів, які можуть призвести до дезорієнтації, втрати автономного мислення та зниження суспільної єдності [173, с. 371].

О. Салієва займалася конструюванням когнітивної моделі для оцінки рівня захищеності об’єктів критичної інфраструктури. С. Гаценко присвятила свої дослідження моделюванню процедур ідентифікації загроз військовій безпеці як компонента загальнонаціональної безпеки держави [31, с. 111].

В умовах щораз більшої психоемоційної напруги, що характерна для інформаційного середовища сучасних криз, когнітивна безпека передбачає не лише здатність оперативно сприймати й опрацьовувати значні обсяги інформації, але й забезпечувати адекватну реакцію на події, зокрема з умінням точно оцінювати часові межі, необхідні для ухвалення рішень та реалізації відповідних дій [167].

На думку П. Лисянського, проблематика когнітивного впливу на свідомість людини й здатність до критичного мислення дедалі активніше досліджується в сучасному науковому середовищі, наприклад, у контексті інформаційних війн, стратегічних комунікацій та безпекових досліджень. У більшості наукових праць когнітивний вплив трактується як сукупність деструктивних інформаційних практик, спрямованих на маніпуляцію масовою свідомістю, трансформацію ціннісних орієнтирів та підрив індивідуальної здатності до самостійного аналізу інформації. Водночас у науковому обігу превалюють підходи, орієнтовані на інформаційний, психологічний або комунікативний рівень аналізу, тоді як смисловий вимір когнітивної безпеки, пов’язаний із глибинними архетипами,

світоглядними структурами та моделями сприйняття реальності, залишається недостатньо опрацьованим [95]. Такий підхід дозволяє усвідомлювати смисли не як випадковий продукт інформаційного обміну, а як цінний і керований стратегічний ресурс когнітивної безпеки. Саме смислова сфера формує основу для збереження національної ідентичності, колективної стійкості та здатності до глибокої саморефлексії, критичного осмислення подій і довготривалого суспільного розвитку.

Сьогодні відсутнє уніфіковане трактування поняття «когнітивна безпека», що зумовлює потребу в систематизації та дослідженні наявних інтерпретацій цієї категорії. Аналізуючи представлені вище дефініції, можемо констатувати, що когнітивна безпека являє собою інтегрований підхід до забезпечення захисту особистості та соціуму від інформаційно-психологічних маніпуляцій. Зазначений концепт охоплює систему заходів та методик, орієнтованих на збереження когнітивних функцій, розумової діяльності та психічного здоров'я в контексті посилення ролі цифрових платформ та віртуального простору. Когнітивна безпека концентрується на виявленні, вивченні та нейтралізації ризиків, що стосуються втручання в когнітивні механізми: мислення, перцепцію, концентрацію та процес вибору рішень. Її призначення полягає в забезпеченні достовірності та захищеності інтелектуальних систем, профілактиці зловживань та протиправних дій, а також підтриманні довіри та відкритості у сфері застосування штучного інтелекту та його соціального впливу. Актуальність цього поняття зумовлена щораз більшим технологічним впливом на наші пізнавальні здібності та методи обробки інформації.

Когнітивна безпека в сучасних реаліях спрямована на охорону когнітивних механізмів розумової активності та психологічного комфорту окремих осіб і спільноти від впливів, здатних деформувати бачення та судження, провокувати маніпулятивні дії та зловживання інформаційними ресурсами. Реалізація когнітивної безпеки здійснюється через формування аналітичного мислення, підвищення поінформованості про маніпулятивні та дезінформаційні технології,

а також усвідомлення психологічних принципів впливу на сприйняття та вибір рішень.

У контексті експансії цифрових технологій та зростання обсягів доступної інформації когнітивна безпека перетворюється на критично важливий компонент системи інформаційної безпеки держави. Вона гарантує свідоме та обґрунтоване поводження з інформацією, а також адекватну відповідь на виклики та ризики психологічного та інформаційного характеру.

У сучасних умовах співвідношення когнітивної та національної безпеки набуває фундаментального значення. Стійкість національної безпеки дедалі більше залежить не лише від захищеності кордонів, збройного потенціалу чи кіберсистем, а передусім – від стабільності, захищеності та цілісності когнітивного простору держави. Людська свідомість, мислення, емоції та здатність до ухвалення рішень стали не лише об’єктом інформаційного впливу, а й новим полем бойових дій, що об’єднує як внутрішні, так і зовнішні виклики національній безпеці.

Когнітивна безпека в цьому ключі виконує роль стратегічного щита, захищаючи суспільство від маніпуляцій, інформаційного тиску та психологічного терору. Саме вона запобігає деструктивним процесам, які можуть призвести до дестабілізації держави без жодного пострілу: розкол суспільства, зневіра в державних інституціях, паніка, хаос і втрата керованості. На відміну від традиційних загроз, що стосуються фізичного середовища, когнітивна загроза проникає безпосередньо у внутрішню тканину державності – у світогляд і свідомість громадян.

У цьому полягає принципова відмінність і водночас зв’язок: національна безпека більше не існує окремо від когнітивної. Без здатності населення критично мислити, розпізнавати дезінформацію, відрізняти реальність від маніпуляцій, жодна інша сфера безпеки не буде ефективною. Навіть найрозвиненіші армії чи кіберсистеми не здатні компенсувати наслідки втрати контролю над свідомістю.

Технологічні чинники, зокрема масове використання штучного інтелекту та дипфейків, лише підсилюють це співвідношення, адже загрози стають менш видимими, але значно більш руйнівними. Наративи, що транслюються через соціальні мережі, інформаційні атаки на вибори, маніпулятивне програмування емоцій – усе це спрямовано на одне: послабити національну єдність через злам когнітивної сфери.

Тому когнітивна безпека сьогодні не є доповненням до національної безпеки – вона її невіддільний складник, основа та передумова. Беззахисна свідомість громадян прирікає державу на вразливість у будь-якій сфері: політичній, економічній, оборонній чи інформаційній. Забезпечення когнітивної стійкості – це сучасна форма національної оборони, де головною зброєю є не ракети, а правда, критичне мислення й довіра до легітимних джерел знань.

На нижченаведеному рисунку 1.1 наочно відображено місце когнітивної безпеки в загальній структурі (системі) інформаційної безпеки.

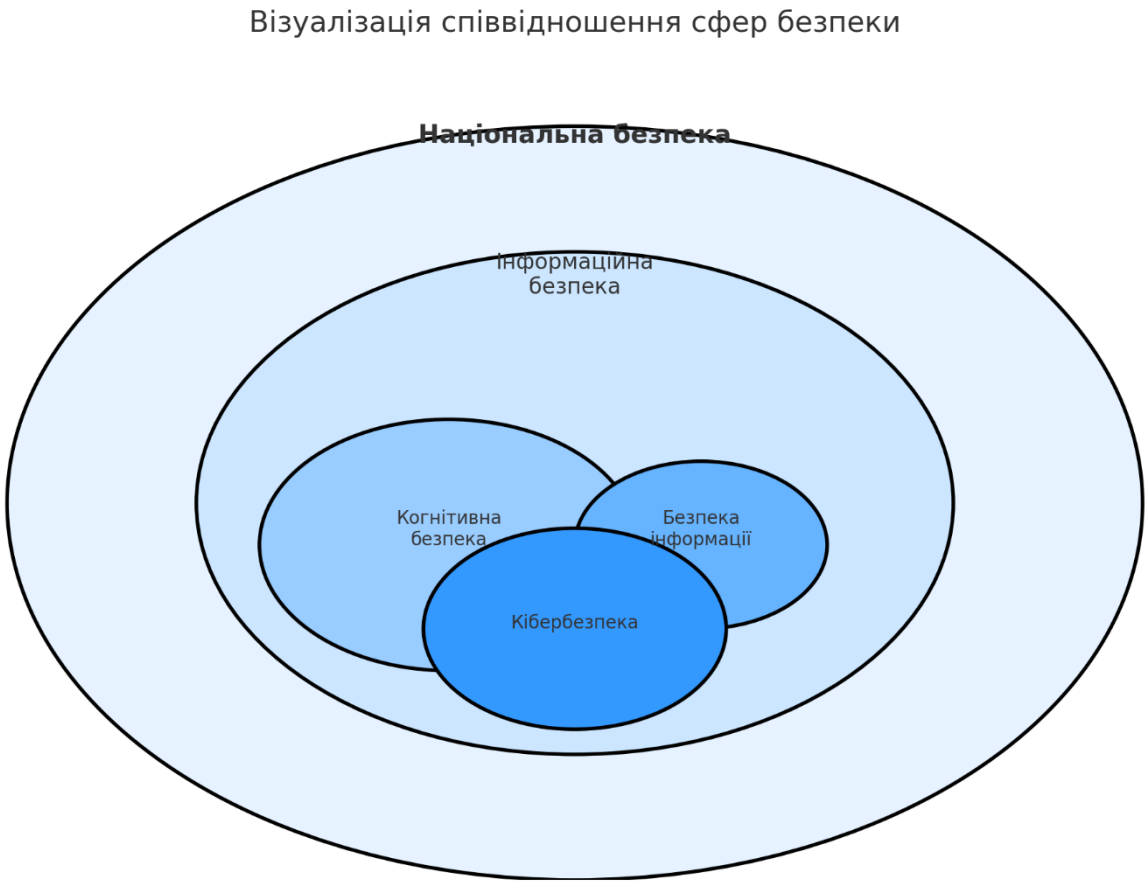


Рис. 1.1. Когнітивна безпека в структурі інформаційної безпеки [86]

Когнітивна безпека, будучи ключовим елементом інформаційної захищеності, визначає результативність та надійність усієї інформаційної екосистеми, охоплюючи також сферу кіберзахисту. Центральні напрями передбачають:

− ідентифікацію потенційних ризиків;

− боротьбу з поширенням неправдивої інформації;

− підтримання довірчих стосунків;

− зміцнення психологічної резистентності;

− запобігання наслідкам кіберінцидентів;

− підтримання ефективності кіберзахисних механізмів.

Таким чином, когнітивна безпека функціонує як фундаментальний компонент системи інформаційного захисту, орієнтований на оберігання не тільки технологічних елементів систем, а й ментального здоров'я, розумових процесів та перцептивних здібностей користувачів, гарантуючи гармонійний та стабільний прогрес соціуму в цифрову добу [78, с.278-285].

Слід зауважити, що поняття «когнітивна безпека» є багатогранним, через що виникає необхідність сегментації цієї категорії в рамках різних підходів (Рис.1.2).

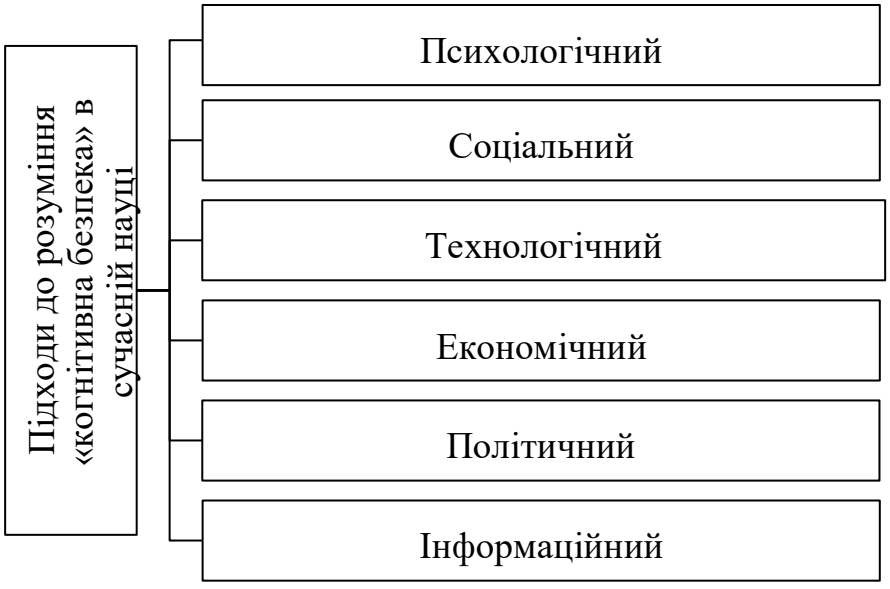


Рис.1.2. Підходи до розуміння «когнітивна безпека» в сучасній науці [78]

Психологічна перспектива розуміння когнітивної безпеки в сучасних дослідженнях зосереджується на кореляції між інформаційним впливом та ментальним станом особистості. Такий напрям орієнтований на ідентифікацію та оберігання розумових процесів від деструктивних маніпуляцій і гарантує психічну стабільність та неупереджене сприйняття даних.

Соціологічний підхід у сучасній науковій практиці досліджує вплив інформаційних потоків на соціум та міжлюдські контакти. Він вивчає роль засобів масової інформації, цифрових платформ та інших комунікативних інструментів у формуванні психологічного клімату та перцепції окремих осіб, а також їхньої спроможності впливати на суспільну свідомість. Цей напрям спрямований на осмислення кореляції між інформаційними впливами та соціальними трансформаціями, а також створення методів протидії маніпулятивним практикам та неправдивій інформації.

Технологічна концепція когнітивної безпеки в сучасних наукових розвідках підкреслює значення передових інформаційних технологій у створенні та підтриманні захисту когнітивних функцій. Ця методологія розглядає використання машинного навчання, аналітичних систем та програмних рішень для виявлення небезпек, відсіювання неправдивої інформації та розвитку цифрової компетентності. Технологічний напрям визначає способи захисту від маніпулятивного впливу в цифровому просторі та підтримує розвиток кіберзахисту з урахуванням психологічних особливостей користувачів.

Економічна перспектива в галузі когнітивної безпеки концентрується на взаємозалежності між заходами захисту розумових процесів та фінансовими чинниками. Цей підхід вивчає вплив інформаційних маніпуляцій на рівень довіри, споживацькі тенденції та інвестиційну атмосферу, а також аналізує фінансові витрати на боротьбу з інформаційними ризиками та дезінформаційними кампаніями.

Політологічна концепція когнітивної безпеки в сучасних наукових розвідках досліджує кореляцію між інформаційним впливом та державотворчими процесами. Вона вивчає функцію маніпулятивних технік та

фальшивої інформації у виборчих процесах, роль цифрових інструментів у формуванні суспільної свідомості та підтримці конкретних ідеологічних позицій. Представники політичного напряму аналізують потенціал використання інформаційного впливу для реалізації державницьких завдань, а також створює тактики захисту розумових процесів від деструктивних політичних маніпуляцій.

Інформаційна перспектива когнітивної безпеки в сучасній науці характеризується як дослідження впливу інформаційних інструментів на розумові функції та психологічний стан особистості. Цей аспект показує роль медіа, цифрових ресурсів та соціальних платформ у формуванні світосприйняття, переконань та рішень людини.

Інформаційний підхід сприяє усвідомленню того, як інформаційні впливи здатні деформувати адекватне сприйняття реальності та провокувати психологічний тиск на особистість, а також формує техніки захисту когнітивних функцій від негативного інформаційного маніпулювання.

Військовий контекст передбачає гарантування когнітивної безпеки України в умовах російської агресії і набуває критичного значення для підтримання національної незалежності та соціальної стабільності. Війна за Незалежність України активізує застосування маніпулятивних та дезінформаційних стратегій для впливу на світосприйняття, формування образу противника, мобілізації населення та дестабілізації держави. Забезпечення когнітивного захисту передбачає розвиток цифрової компетентності громадян, ідентифікацію неправдивої інформації, підвищення обізнаності щодо психологічних технік впливу. Це не тільки посилює резистентність соціуму перед інформаційними ризиками, а й сприяє збереженню національної консолідації та довіри до інформаційних ресурсів у кризових обставинах.

Отже, поняття «когнітивна безпека» тлумачиться як концептуальна система, що охоплює методи та стратегії оберігання розумових процесів та інтелектуальної активності в індивідуальному та колективному сприйнятті й переробці даних. Ця концепція наголошує на виявленні, дослідженні та нейтралізації ризиків, пов’язаних із втручанням у когнітивні механізми, що

можуть деформувати об’єктивне розуміння реальності та спровокувати психологічний вплив на людину. Призначення когнітивної безпеки полягає в забезпеченні стабільного та захищеного функціонування розумових систем, профілактиці зловживань, збереженні довіри та відкритості в інформаційному просторі.

Науковий аналіз когнітивної безпеки як ключового елемента сучасної національної безпекової політики України базується на широкому колі джерел, які охоплюють міждисциплінарні підходи з політичної науки, безпекознавства, психології, комунікативістики, соціології та інформаційних технологій. Різноманітні джерельні матеріали дозволили дисертанту здійснити комплексний аналіз когнітивного виміру безпеки, обґрунтувати авторські висновки та уникнути спрощених або однобічних трактувань динамічних процесів, що відбуваються у сфері інформаційно-психологічної безпеки.

Повномасштабна агресія російської федерації проти України, що поєднує воєнні, інформаційні, кібернетичні та когнітивні впливи, актуалізувала необхідність переосмислення традиційного розуміння національної безпеки. Виникла потреба в науковому дослідженні когнітивної безпеки як окремого домену гібридної війни та стратегічного ресурсу державної стійкості. Вивчення загроз, пов’язаних із маніпуляцією масовою свідомістю, дезінформацією, ерозією ідентичності та підривом довіри до інституцій, потребує багатовекторного аналізу як теоретичних засад, так і прикладних механізмів когнітивного впливу.

Відповідно, джерельну базу дослідження когнітивної безпеки було умовно поділено на п’ять основних груп.

Перша група – це наукові праці, у яких визначено загальнотеоретичні засади безпеки, зокрема, роботи, присвячені національній, інформаційній, кібернетичній та психологічній безпеці (В. Горбулін, О. Данільян, В. Ліпкан, М. Лібікі, В. Недбай, Ю. Радковець, Т.Семенюк, Г. Тамбер та ін.). Ці джерела забезпечили методологічне підґрунтя для формування авторської позиції щодо ролі когнітивного чинника в системі національної безпеки.

Друга група охоплює міждисциплінарні дослідження, що висвітлюють природу та структуру когнітивної війни, її відмінність від класичної інформаційної або психологічної війни, а також концепції стратегічних наративів, когнітивного впливу, резильєнтності та захисту ментального простору (Ф. Гоффман, К. Джайлз, Я. Каленський, М. Литвин, О. Мороз, Г. Почепцов, І. Рущенко, С. Фелдстайн).

Третя група складається з аналітичних доповідей, монографій та статей, що досліджують когнітивну безпеку в контексті гібридної війни, зокрема, інструменти маніпуляції свідомістю, механізми дезінформації, алгоритми розповсюдження наративів через медіа та соціальні мережі, технології дипфейків і цифрових впливів (А. Бабінська, П. Біленчук, Г. Дієм, Р. Кларк, Т. Рід, О. Семченко, А. Слободянюк, Д. Шлапак).

Четверта група джерел містить практико-аналітичні звіти, матеріали міжнародних організацій (NATO, EU StratCom, Центр протидії дезінформації при РНБО України, Hybrid CoE), що розкривають конкретні приклади когнітивних атак, ІПСО, використання соціальних мереж як інструментів впливу на політичну свідомість та емоційні стани громадян.

П’яту групу становлять емпіричні дослідження, статистичні звіти, опитування та кейси, що дають змогу оцінити рівень когнітивної стійкості українського суспільства, ефективність державної політики у сфері інформаційної протидії, а також стан розвитку критичного мислення, медіаграмотності та цифрової гігієни серед населення.

Дослідження підходів до трактування когнітивної безпеки демонструє її багатоаспектний характер та значущість у сучасному інформаційному середовищі. Психологічна перспектива зосереджується на ментальному стані особистості, соціологічна – на впливі на громадську свідомість, технологічна – на використанні машинного інтелекту, економічна – на фінансових витратах, а політична – на впливі на державотворчі процеси. Інформаційна концепція досліджує функцію інформаційних ресурсів. Ці підходи є взаємопов’язаними та

взаємодоповнюваними і формують основу для результативного забезпечення когнітивної безпеки в різноманітних сферах суспільного життя.

1.2. Політико-інформаційний складник когнітивної безпеки: теоретичні підходи та концептуалізація механізмів захисту

У сучасних умовах трансформації політичних процесів та загострення глобальних безпекових викликів інформація перестає бути лише засобом комунікації й дедалі частіше постає як інструмент влади, впливу та стратегічного протистояння. Особливого значення в цьому контексті набуває політико-інформаційний вимір когнітивної безпеки, оскільки саме в ньому відбувається формування смислів, наративів й інтерпретаційних рамок, що визначають політичну поведінку індивідів, груп та суспільства загалом. Під час гібридної війни інформаційний простір перетворюється на арену цілеспрямованого впливу на свідомість, критичне мислення та систему цінностей, що зумовлює необхідність його наукового осмислення в межах політичної науки.

Політико-інформаційний складник когнітивної безпеки охоплює сукупність процесів, механізмів й інструментів, через які здійснюється вплив на політичне сприйняття реальності, легітимацію влади, рівень суспільної довіри та стійкість демократичних інститутів. У цьому вимірі когнітивна безпека постає не лише як реакція на дезінформаційні загрози, а як стратегічний ресурс держави, спрямований на захист національного інформаційного простору, забезпечення цілісності політичного дискурсу та збереження здатності суспільства до раціонального політичного вибору.

Теоретичне осмислення політико-інформаційного складника когнітивної безпеки потребує звернення до широкого кола концепцій – від теорій політичної комунікації, стратегічних наративів і публічної сфери до підходів інформаційної, психологічної та національної безпеки. У працях сучасних дослідників дедалі частіше підкреслюється, що інформаційні впливи стають ефективними не стільки через сам факт поширення повідомлень, скільки через здатність

інтегруватися в когнітивні структури суспільства, формувати стійкі уявлення, емоційні реакції та моделі політичної лояльності чи спротиву.

З огляду на це актуалізується потреба в концептуалізації механізмів захисту когнітивного простору, які мають поєднувати нормативно-правові, інституційні, комунікативні та освітні інструменти. Політико-інформаційнний складник когнітивної безпеки передбачає не лише протидію деструктивним інформаційно-психологічним операціям, але й формування ефективної державної комунікативної політики, розвиток медіаграмотності, стратегічних комунікацій і довгострокових національних наративів. Саме ці аспекти зумовлюють необхідність детального аналізу теоретичних підходів і практичних моделей забезпечення когнітивної безпеки, що й становить предмет розгляду.

Сучасна система когнітивної безпеки детермінується необхідністю інтегрального сприйняття політичного та інформаційного складника, які в умовах гібридної війни конвергують у єдиний комплекс загроз. У контексті збройної агресії російської федерації проти України, що реалізується через поєднання мілітарних та немілітарних методів, інформаційний простір трансформувався в ключовий театр воєнних дій. Саме в цьому сегменті такі інструменти, як цілеспрямована дезінформація, ідеологічна пропаганда та кібернетичні операції, функціонують як ефективні механізми дестабілізації політичних інституцій та руйнування суспільної солідарності [13]. Еволюція гібридних загроз: від анексії Криму у 2014 році до повномасштабного вторгнення 2022 року – наочно демонструє посилення ролі інформації як стратегічного ресурсу політичного впливу та ведення війни за Незалежність України, де маніпуляція суспільною свідомістю через канали масової комунікації стала невід’ємним елементом агресії.

Предметом наукового аналізу в такому контексті виступає політико-інформаційний складник когнітивної безпеки, який концептуалізовано як комплексну систему, спрямовану на забезпечення захищеності політичної системи, конституційного ладу та колективної ідентичності від деструктивних інформаційних впливів. Ця концепція синтезує традиційні політико-правові

підходи до національної безпеки, онтологічно закріплені в Конституції України (ст. 17), з викликами, детермінованими суспільними відносинами, де контроль над інформаційними потоками безпосередньо зумовлює динаміку політичних процесів [83]. В її семантичне поле інкорпоровано як технократичні аспекти кібербезпеки, так і заходи протидії інформаційно-психологічним маніпуляціям та ідеологічній пропаганді.

Наукова проблема полягає в недостатній розробці концептуальних моделей та механізмів протидії асиметричним загрозам, серед яких пріоритетними є стратегічна дезінформація, інформаційно-психологічні операції та кібератаки на критичну інформаційну інфраструктуру. Незважаючи на те, що Закон України «Про національну безпеку України» (2018) [145] імперативно визначає інформаційну безпеку як структурний елемент національної безпеки, недостатня теоретична розробленість цього поняття зумовлює наявність практичних прогалин. До них, зокрема, належить неефективність моніторингу та нейтралізації пропагандистських кампаній у сегменті соціальних медіа. Ескалація цих загроз в умовах правового режиму воєнного стану, що регулюється Законом України «Про правовий режим воєнного стану» (2015) [148], актуалізує потребу в розробці проактивної багаторівневої стратегії захисту політико-інформаційного простору держави.

Концептуалізація політико-інформаційного складника когнітивної безпеки як об’єкта наукового аналізу вимагає методологічного синтезу, що інтегрує класичні теорії національної безпеки із сучасними парадигмами інформаційного суспільства та гібридної війни. В умовах трансформації інформаційного простору в ключовий театр асиметричних конфліктів, традиційні реалістські підходи, сконцентровані на військових та економічних детермінантах безпеки, потребують доповнення комунікативними, інституційними та владними теоріями. Такий синтез дозволяє реконцептуалізувати політико-інформаційний складник не як статичний компонент, а як динамічну систему, у якій класичні рамки (наприклад, реалістична теорія безпеки) продуктивно інтегруються з постмодерністськими концепціями мережевої організації суспільства.

М.Кастельс онтологізує сучасне суспільство як мережеву структуру, організовану навколо миттєвих потоків інформації, капіталу та культурної комунікації, що істотно обмежує ефективність традиційних національно-державних механізмів регулювання [207].

Подібний методологічний плюралізм забезпечує комплексність у розкритті природи гібридних загроз, які трактуються як синергетичне поєднання інформаційно-психологічних операцій та високотехнологічних кібератак.

Політико-правовий підхід ґрунтується на аналізі політико-інформаційного складника національної безпеки через категорії національних інтересів, державного суверенітету та конституційних норм. Стаття 17 Конституції України імперативно визначає захист суверенітету, територіальної цілісності та інформаційної безпеки як пріоритетну функцію держави та справу всього українського народу [83]. Б. Бідова, Г. Бєляєва, М. Яхіяєва концептуалізують національні інтереси як об’єктивні, багатовимірні потреби особи, суспільства та держави в забезпеченні стабільного розвитку, що відображено в офіційній політиці держави [202]. Ю. Руохонен пропонує інноваційне прочитання цифрового суверенітету, зміщуючи акцент із територіальних аспектів на здатність держави до ефективного управління цифровим простором, що має ключове значення для забезпечення індивідуальної автономії в інформаційному середовищі [265]. Дж. Беверлі та Д. Лімбо, аналізуючи складність дефініції державного суверенітету через відсутність універсальної юрисдикції в міжнародному праві, обґрунтовують доцільність онтологічного підходу до його моделювання, який інкорпорує суперечливі дані та визнає нормативну вагу актів визнання [200]. Таким чином, політико-правовий підхід актуалізує правове регулювання інформаційного простору як інструмент забезпечення політичної стабільності, де національні інтереси виступають основним орієнтиром у протидії зовнішнім деструктивним впливам.

Комунікативний підхід розширює методологічні горизонти дослідження, концептуалізуючи інформацію як стратегічний ресурс влади та поле символічної боротьби. М. Фуко, аналізуючи владу як продуктивну мережу знань і дискурсів,

демонструє, як дисциплінарні практики (спостереження, нормалізація) формують механізми соціального контролю, що є ключовим для розуміння маніпулятивного потенціалу дезінформації в гібридних конфліктах [226]. Концепція публічної сфери Ю. Габермаса як простору раціонально-критичного дискурсу, де, на його думку, «поняття комунікативної дії стосується взаємодії щонайменше двох суб'єктів, здатних до мовлення та дій, які встановлюють міжособистісні відносини» [229, с. 86], надає нормативну основу для аналізу відхилень від ідеалу раціональної комунікації. Емпіричне дослідження С. Монті, Л. Аєлло, Г. Де Франчіскі Моралеса, Ф. Бончі верифікують актуальність габермасіанської теорії, демонструючи, що комунікація, орієнтована на соціальні виміри (знання, подібність, довіра), є на 77% ефективнішою для модифікації суспільних думок в онлайн-середовищі, що вказує на роль ілукційної (іллокутивної) сили в цифровому просторі [249]. У контексті гібридної війни ці теоретичні рамки розкривають механізми, за допомогою яких дезінформація трансформує комунікацію з інструменту консенсусу в інструмент домінування.

Структурно-функціональний та неоінституційний підходи зосереджуються на аналізі інституційних детермінант політико-інформаційної безпеки. Перший із них, ґрунтуючись на теорії соціальних систем Т. Парсонса, досліджує функції ключових політичних інститутів (парламенту, уряду, РНБО, спецслужб) у забезпеченні інформаційної безпеки через призму їхньої ролі в адаптації, досягненні цілей, інтеграції та латентному підтриманні норм [260].

Неоінституційний підхід доповнює цю перспективу, зосереджуючись на аналізі формальних (закони, стратегії) та неформальних правил гри, що формують практику інституційної поведінки в умовах гібридних викликів, і бере до уваги шляхи їхньої еволюції та адаптації [113].

Дослідження Дж. Поле акцентує на необхідності системного аналізу загроз інформаційній безпеці, аргументуючи, що соціальні мережі (Facebook, Google+, X) загрожують не лише індивідуальній приватності, але й функціональній диференціації суспільства в цілому через централізоване збирання даних із

різних соціальних систем [262]. Він зазначає, що, за відсутності структурних обмежень на використання цих даних, соціальні мережі можуть трансформуватися в серйозну загрозу для автономії особистості та свободи в західних суспільствах.

У сукупності зазначені методологічні підходи формують комплексну теоретико-методологічну основу для багаторівневого аналізу та проактивної протидії загрозам у політико-інформаційній сфері.

Генеза концепту «інформаційно-політичний складник когнітивної безпеки» в українському та міжнародному політологічному дискурсі демонструє його парадигмальну трансформацію – від технократичної моделі, орієнтованої на захист інформаційних систем, до інтегративної парадигми, що синтезує політичні, соціальні та технологічні виміри. Ця еволюція репрезентує адаптацію теоретико-правових рамок до викликів гібридних загроз, у яких інформаційний простір функціонує як стратегічний інструмент політичного впливу та інституційної дестабілізації. Філософсько-стратегічні витоки поняття сягають античних практик, зокрема трактату Сунь-цзи «Мистецтво війни» (V ст. до н.е.), де інформаційна перевага концептуалізувалася як детермінанта перемоги, що стало прототеоретичною основою для сучасних доктрин інформаційного протиборства [127, с. 39].

В українському науковому полі еволюція дефініції реконструюється через історико-порівняльний аналіз ключових нормативних актів, що дозволяє ідентифікувати зміщення акцентів від технічного захисту даних до системного забезпечення національної безпеки.

Перший етап інституціоналізації концепції відтворений у Законі України «Про основи національної безпеки України» №964-IV від 19 червня 2003 року, який втратив чинність 8 липня 2018 року. Вказаний акт трактував інформаційну безпеку як складову національної безпеки, що охоплює захист життєво важливих інтересів людини, суспільства і держави від загроз у сферах, зокрема забезпечення свободи слова та інформаційної безпеки (ст. 1, абзац другий, зі змінами від 01.07.2010 № 2411-VI) [146]. Нормативний аналіз свідчить про

домінування технократичного дискурсу: пріоритетом виступає захист інформаційних ресурсів, систем і мереж від негативного впливу, без операціоналізації соціально-політичних маніпуляцій. Ця дефініція репрезентує контекст раннього пострадянського періоду, коли фокусувалася на економічних й оборонних аспектах, а інформаційно-психологічні операції залишалися периферійними.

Другий етап детермінований ухваленням Закону України «Про національну безпеку України» № 2469-VIII від 21 червня 2018 року, що імплементував нову концептуальну модель. Цей акт радикально розширює семантичні рамки поняття, виокремлюючи інформаційну безпеку як окремий сектор національної безпеки (ст. 3 ч. 4) поряд із воєнним, економічним і гуманітарним [145]. Хоча легальна дефініція «інформаційної безпеки» в ст. 1 відсутня, її зміст інтерпретується через секторальний підхід, що інкорпорує захист від маніпуляцій громадською свідомістю, ескалації соціальних конфліктів і дестабілізації політично-економічної системи. Ця парадигмальна трансформація зумовлена операціональним досвідом гібридної агресії росії проти України з 2014 року, що актуалізувало переорієнтацію з технічних аспектів на соціально-політичні загрози. Окремо конституціонується «кібербезпека» (п. 21 ст. 1) як стан захищеності від кіберзагроз, що ілюструє категоріальну диференціацію в нормативному полі.

Для подолання термінологічної полісемії в політологічному аналізі необхідна чітка демаркація суміжних категорій. «Інформаційна безпека» охоплює загальний стан захищеності інформаційного простору від негативних впливів, охоплюючи маніпуляції та пропаганду, як це концептуалізовано в Доктрині інформаційної безпеки України 2017 р., де ідентифіковано загрози, зокрема спеціальні інформаційні операції, спрямовані на підрив обороноздатності та дестабілізацію суспільства [142]. «Кібербезпека», згідно зі Стратегією кібербезпеки України 2021 р., фокусується на протекції від цифрових загроз, таких як хактивізм чи компрометація критичної інфраструктури, і трактуєце як імператив стримування агресії [152]. Ширше поняття «безпека

інформаційної сфери», артикульоване в Стратегії інформаційної безпеки України 2021 р., інтегрує не лише протекційні, а й розвиткові аспекти інформаційного середовища, передбачаючи медіарегулювання та протидію дезінформації [151]. Г. Гончаренко аргументує необхідність термінологічної уніфікації для прецизійного правового регулювання, акцентуючи на міждисциплінарному підході до сучасних викликів [38, с.467].

Історичний контекст формування вказаних концепцій реконструюється через Доктрину інформаційної безпеки України 2009 р. [141], що деномінована у 2014 р., та її субституцію у 2017 р. [142], доповнену Стратегією 2021 р. Окрім цього, правове регулювання інформаційної безпеки забезпечується через систему спеціальних законів, серед яких провідну роль відіграє Закон України «Про інформацію». Він встановлює правові засади доступу до інформації, визначає механізми її захисту та класифікації, а також унормовує обіг інформації в суспільстві [143]. Ці документи відображають еволюцію від реакції на локальні загрози до системної, детермінованої зовнішньою агресією протидії інформаційним операціям.

На підставі проведеного аналізу пропонуємо розглядати / кваліфікувати концепт *«політико-інформаційний складник когнітивної безпеки»* як стан захищеності політичної системи та суспільних інститутів від інформаційних загроз, спрямованих на підрив суверенітету, дестабілізацію та маніпуляцію політичною волею. Ця категорія синтезує онтологічні підходи до суверенітету, де він концептуалізується як динамічна взаємодія визнання та претензій [200], і системні теорії, що індикують ризик централізованих даних для функціональної диференціації суспільства [261].

В українському контексті це поняття набуває емпіричної релевантності, забезпечуючи методологічну основу для протидії гібридним загрозам через інтеграцію правового регулювання, технологічних рішень і комунікаційних стратегій. Г. А. Таердоост диференціює «кібербезпеку» (протекція від цифрових загроз) й «інформаційну безпеку» (ширший спектр загроз, охоплює нецифрові), що консолідує теоретичну обґрунтованість запропонованої категорії [270].

Еволюція поняття «когнітивна безпека» репрезентує парадигмальний зсув у політичній науці та праві з акцентом на адаптацію до гібридних викликів. Конституціонування «політико-інформаційного складника когнітивної безпеки» як аналітичної категорії відкриває нові перспективи для дослідження стійкості політичних систем у цифрову епоху, вимагаючи подальшого емпіричного аналізу та міждисциплінарної інтеграції.

Сучасна війна за Незалежність України демонструє парадигмальну трансформацію характеру війни, у якій інформаційний простір став органічним складником тотального протистояння. Початкова концепція гібридної війни, яку розуміли як альтернативу повномасштабному збройному конфлікту [42], в умовах відкритої агресії з лютого 2022 року еволюціонувала. Сьогодні ми спостерігаємо не заміщення, а синергетичне поєднання методів: класичні бойові дії посилюються потужними інформаційно-психологічними операціями, що перетворює війну за Незалежність України на багаторівневе протистояння. Інформація в цьому контексті втратила статус винятково «м'якої сили» та перетворилася на прямий інструмент ведення бойових дій, що впливає на оперативну обстановку, моральний стан військ та суспільну свідомість.

Аналіз сучасних загроз вимагає переосмислення теоретичного базису в контексті актуального воєнного досвіду. Якщо до 2022 року гібридні методи розглядалися переважно як спосіб уникнення відкритої конфронтації, то тепер вони стали невід'ємною частиною повномасштабної війни і посилили ефект від застосування збройних сил. Ця логіка відображена в українській нормативній базі, зокрема в Стратегії воєнної безпеки України [150], яка, хоч і була ухвалена до повномасштабного вторгнення, концептуалізує комбінацію різних інструментів впливу. Однак сьогодні ця комбінація набула нового значення: інформаційні атаки проводяться не замість військових, а разом із ними, утворюючи єдиний потік впливу. Наприклад, кібератаки на системи зв'язку та енергетику безпосередньо підтримують наступальні операції противника, а пропагандистські наративи про «денацифікацію» слугують легітимацією воєнних злочинів.

Синтез теоретичних напрацювань (на кшталт концепції мережевого суспільства Кастельса) з практичним досвідом дозволяє зробити висновок: інформація в сучасній війні перестала бути лише супутнім явищем. Вона стала повноцінним боєприпасом, що застосовується в реальному часі для безпосередньої підтримки воєнних цілей, що вимагає від України та її союзників розробки не просто оборонних, а проактивних стратегій інформаційної безпеки, що передбачають швидке виявлення і розвінчання ворожих наративів, а також протидію їм на всіх рівнях – від тактичного до глобального. Майбутні дослідження мають бути спрямовані на моделювання сценаріїв розвитку інформаційної війни та розробку нових методів захисту суспільної свідомості в умовах тривалої війни за Незалежність України.

Забезпечення політико-інформаційного складника когнітивної безпеки України в умовах тривалої гібридної агресії потребує системного аналізу інституційно-правових механізмів, спрямованих на нейтралізацію політично детермінованих інформаційних загроз. Сучасна система ґрунтується на еволюційному розширенні нормативно-правового поля, що відображає парадигмальний зсув від технократичного захисту інформаційних систем до інтегративної моделі, орієнтованої на протидію соціально-політичним маніпуляціям. Стратегічні рамки визначені низкою ключових документів: Стратегія інформаційної безпеки України (2021) актуалізує протидію дезінформації та розвиток медіарегулювання [151], тоді як Стратегія кібербезпеки України (2021) фокусується на захисті критичної інформаційної інфраструктури [152].

Знаковим досягненням стало ухвалення Закону України «Про медіа» [144], який інституціалізує захист національного інформаційного простору від зовнішніх деструктивних впливів, зокрема, шляхом заборони пропаганди агресії та впровадження механізмів обмеження ретрансляції ворожих інформаційних ресурсів. В умовах правового режиму воєнного стану держава отримує додаткові повноваження для оперативного реагування, що, однак, породжує напругу між

безпековими імперативами та дотриманням демократичних стандартів (Закон України «Про правовий режим воєнного стану», 2015).

Емпіричні дані свідчать про низку вагомих досягнень. Діяльність Центру протидії дезінформації при РНБО дозволила систематизувати виявлення та спростування пропагандистських кампаній. Дослідження підтверджують, що посилення кіберрезильєнтності дозволило українським структурам відбити значну частину російських кібератак, що доводить ефективність інтеграції міжнародних стандартів у національну стратегію безпеки [235]. Активізація волонтерських ініціатив, наприклад, IT Army [208], та партнерства з міжнародними технологічними компаніями (Microsoft, 2022) ілюструють реалізацію принципу «справа всього народу», закріпленого в Конституції України (1996), та демонструють здатність до нестандартних рішень у протидії асиметричним загрозам.

Проте, незважаючи на прогрес, аналіз показує низку системних прогалин, що обмежують потенціал повноцінного забезпечення політико-інформаційної безпеки. Перш за все, це нормативно-термінологічна полісемія. Відсутність єдиного концептуального апарату та чіткої демаркації понять «інформаційна безпека», «кібербезпека» та «політико-інформаційна безпека» призводить до фрагментації правового поля та ускладнює координацію між інституціями [13; 39; 270]. По-друге, існують значні ресурсні та технологічні обмеження.

По-третє, маніфестуються комунікативні дисфункції. Відхилення від моделі раціональної комунікації в цифровому просторі посилює ефект «ілллокуційної сили» дезінформації [229], тоді як брак проактивних контрнаративів обмежує здатність держави до символічного протистояння в міжнародному інформаційному полі.

Крім того, існують онтологічні виклики суверенітету. Концептуалізація суверенітету як динамічної взаємодії вказує на ризик, коли централізоване збирання даних глобальними платформами підриває функціональну диференціацію суспільства [261] та обмежує реальний цифровий суверенітет держави [265], що демонструє потребу не лише в технічних рішеннях, але й у

глибокому теоретичному осмисленні природи влади та контролю в мережевому суспільстві [226].

Перехід від реактивної до проактивної парадигми забезпечення політико-інформаційної безпеки є імперативом. Він вимагає реалізації комплексу заходів: нормативної консолідації шляхом ухвалення спеціалізованого законодавства; інституційної оптимізації для підвищення міжвідомчої координації; технологічної модернізації через інвестиції в системи моніторингу; комунікативної проактивності, спрямованої на відновлення раціонального дискурсу. Лише синтез політико-правових, комунікативних та структурно-функціональних підходів може забезпечити стійкість національної безпеки України в умовах тривалої гібридної війни.

Крізь призму гібридної агресії інституційна архітектура національної безпеки зазнає парадигмальної трансформації, де політичні інституції та структури громадянського суспільства формують комплементарну систему протидії інформаційним загрозам. Ефективність цієї системи детермінується здатністю до синергетичної взаємодії між формальними механізмами державного регулювання та горизонтальними мережами громадянської активності [133]. Політико-інституційний підхід у в такому випадку реалізується через створення комплексних рамок координації, що інтегрують правові норми, інституційні практики та стратегічні комунікації для нейтралізації дезінформаційних впливів.

Державні інституції формують вертикальну вісь системи протидії, забезпечуючи стратегічне планування, нормативно-правове регулювання та оперативне реагування. Ключову роль відіграє РНБО, що координує міжвідомчі заходи моніторингу інформаційних загроз та захисту критичної інфраструктури. Законодавча влада імплементує норми медіарегулювання, спрямовані на нейтралізацію інформаційно-психологічних операцій, тоді як силові структури (Служба безпеки України, Державна служба спеціального зв’язку та захисту інформації) реалізують оперативні заходи з виявлення та спростування

дезінформаційних кампаній, що дозволяє знижувати їхній вплив на 30–40% у сегменті соціальних медіа [197].

В умовах воєнного стану інституційний механізм доповнюється спеціальними повноваженнями щодо блокування ворожих інформаційних ресурсів, що актуалізує проблему балансу між безпековими імперативами та гарантіями свобод. Цей баланс забезпечується через гармонізацію національного законодавства з європейськими стандартами (Digital Services Act, European Democracy Action Plan). Національна рада України з питань телебачення і радіомовлення як медіарегулятор здійснює ліцензування та моніторинг контенту для ідентифікації мови ворожнечі, а Міністерство культури та інформаційної політики формує стратегічні засади інформаційної безпеки, впроваджуючи лінгвістичну експертизу для аналізу маніпулятивних практик на тимчасово окупованих територіях.

Громадянське суспільство виступає горизонтальною складовою системи національної безпеки, реалізуючи принцип “емансипаторної безпеки” через активізацію суспільної участі та збереження колективної ідентичності [238]. Волонтерські ініціативи демонструють високу ефективність у заповненні інституційних прогалин: благодійні фонди («Повернись живим», Фонд Сергія Притули) мобілізують фінансові ресурси для забезпечення армії, громадські організації (InformNapalm) реалізують розслідувальні функції, а координаційні центри (Схід SOS, Save Ukraine) забезпечують гуманітарну допомогу та евакуацію населення.

Особливого значення набувають технологічні ініціативи громадянського суспільства. IT Army України реалізує децентралізовану кібероборону через координацію DDoS-атак та контркампаній, а фактчекінгові платформи (StopFake) забезпечують верифікацію інформації та підвищення медіаграмотності на 25%. Партнерства з технологічними компаніями дозволяють заповнювати прогалини в моніторингу кіберзагроз, протидіючи фішинговим атакам та поширенню шкідливого програмного забезпечення (далі – ПЗ) [201].

Ефективність протидії інформаційним загрозам забезпечується через гібридні моделі координації, що поєднують державне регулювання з громадянськими ініціативами. Яскравим прикладом є платформа Digital Threat Landscape для виявлення кібератак, що функціонує на засадах публічно-приватного партнерства. Проте, недостатній рівень інституційної координації призводить до дублювання функцій, що показує потребу в створенні спеціалізованих центрів обміну інформацією.

Міжнародний досвід (наприклад, Естонія з Cyber Defence League) демонструє ефективність інтеграції цивільного сектору в систему тотальної оборони без порушення демократичних стандартів (Open Government Partnership, n.d.). В українському дискурсі це передбачає розвиток механізмів взаємодії Міністерства культури та інформаційної політики і Центру протидії дезінформації з громадськими організаціями та міжнародними партнерами (NATO StratCom COE).

На підставі аналізу інституційної взаємодії пропонуємо концептуальну модель політико-інформаційного складника когнітивної безпеки, що базується на чотирьох взаємопов’язаних компонентах:

Нормативна консолідація – ухвалення єдиного законодавчого акту про протидію гібридним загрозам із чіткою демаркацією понятійного апарату та гармонізацією з європейськими нормами, зокрема, положеннями про суспільну безпеку для інституціоналізації участі громадянського суспільства.

Інституційна оптимізація – створення міжвідомчих хабів з інтеграцією штучного інтелекту для моніторингу загроз, формалізація статусу волонтерських резервів та впровадження єдиної системи координації.

Комунікативна проактивність – розробка контрнаративів на засадах раціонального дискурсу, реалізація кампаній медіаграмотності та системна координація стратегічних комунікацій для проактивної трансляції єдиних повідомлень.

Онтологічне переосмислення – диверсифікація інформаційних потоків для забезпечення цифрового суверенітету, розвиток міжнародних альянсів проти зовнішнього втручання та інтеграція в євроатлантичний простір безпеки.

Запропонована модель трансформує інформаційний простір з арени загроз у платформу стратегічних можливостей, забезпечуючи основу для подальших досліджень синергії інституційних механізмів у поствоєнний період. Верифікація її ефективності потребує імітаційного моделювання сценаріїв розвитку гібридних загроз до 2030 року з урахуванням динаміки інституційних трансформацій.

Отже, проведене дослідження доводить: сучасна система національної безпеки формується під впливом парадигмального зсуву, у результаті якого політико-інформаційний складник перетворюється на центральний елемент стійкості держави в умовах гібридних конфліктів. Цей перехід від фрагментарного технократичного захисту цифрових систем до інтегративної моделі політико-інформаційної безпеки означає трансформацію інформації з інструменту комунікації в стратегічний ресурс влади, що визначає динаміку політичних процесів через боротьбу за вплив на суспільну свідомість. Методологічна інновація дослідження полягає в обґрунтуванні ефективності плюралістичного виміру, що інтегрує політико-правовий, комунікативний та структурно-функціональний інструментарії. Синтез цих підходів дозволяє аналізувати національну безпеку не як статичну систему, а як динамічну мережу, здатну до адаптації в умовах асиметричних викликів, і поєднує традиційні теорії безпеки із сучасними концепціями мережевого суспільства. Інституційна трансформація системи безпеки проявляється у формуванні гібридної моделі взаємодії, де державні інституції забезпечують вертикальну координацію, а структури громадянського суспільства – горизонтальну мобілізацію ресурсів. Така симбіотична система тотальної оборони перетворює потенційні вразливості на джерела інноваційної стійкості, роблячи участь суспільства конститутивним елементом національної безпеки.

Емпіричний аналіз виявив синергетичний характер сучасних гібридних загроз, де поєднання кібератак, дезінформаційних кампаній та психологічних операцій створює системну вразливість. Централізація даних у глобальних мережах формує онтологічну загрозу цифровому суверенітету, а нормативно-правові прогалини, зокрема, термінологічна полісемія та відсутність єдиного законодавства про гібридні загрози, обмежують можливості проактивного реагування. Контури нової парадигми політико-інформаційної безпеки базуються на чотирьох взаємопов'язаних компонентах: нормативній консолідації, інституційній оптимізації, комунікативній проактивності та онтологічному переосмисленні. Ця модель забезпечує перехід від реактивної оборони до стратегії проактивного впливу, перетворюючи інформаційний простір із зони ризику на платформу стратегічної переваги.

У результаті аналізу теоретичних підходів до політико-інформаційного складника когнітивної безпеки встановлено, що в умовах гібридної війни інформаційний простір перестає бути нейтральним середовищем обміну повідомленнями та трансформується в ключовий інструмент політичного впливу, боротьби за легітимність і контроль над процесами суспільного мислення. Політико-інформаційний вимір когнітивної безпеки безпосередньо пов'язаний із формуванням наративів, інтерпретаційних рамок, ціннісних орієнтацій і моделей політичної поведінки, що визначають рівень стійкості суспільства до деструктивних інформаційно-психологічних впливів.

Когнітивна безпека має багаторівневу та структурно складну природу й охоплює взаємопов'язані компоненти: індивідуальний (рівень сприйняття, критичного мислення та психологічної стійкості особи), суспільний (колективні уявлення, ідентичність, довіра до інститутів) та інституційний (державна політика, стратегічні комунікації, нормативно-правове регулювання). Політико-інформаційний складник посідає в цій структурі системоутворювальне місце, оскільки саме через нього здійснюється вплив на всі інші рівні когнітивної безпеки.

Політико-інформаційний складник когнітивної безпеки виконує подвійну функцію: з одного боку, він є каналом поширення загроз у формі пропаганди, дезінформації та маніпулятивних наративів, а з іншого, – виступає ключовим інструментом захисту, через який держава і суспільство можуть формувати механізми протидії когнітивним атакам. Саме в цій площині відбувається боротьба за смисли, довіру та політичну лояльність, що зумовлює її особливе значення для забезпечення національної безпеки.

Ефективна система когнітивної безпеки неможлива без цілеспрямованої інформаційної політики, яка поєднує стратегічні комунікації, розвиток медіаграмотності, захист інформаційного суверенітету та формування стійких національних наративів. Таким чином, політико-інформаційний складник виступає не допоміжним елементом, а ядром когнітивної безпеки, від ефективності якого залежить здатність держави зберігати цілісність політичного простору, демократичну легітимність і стійкість суспільства в умовах гібридних загроз.

Теоретико-концептуальне обґрунтування феномену когнітивної безпеки постає інтегральною складовою сучасної політичної науки, безпекових студій та стратегічних комунікацій. Когнітивна безпека формується на перетині політичної психології, інформаційної безпеки, соціальної когнітології, філософії свідомості та комунікаційних технологій.

Аналіз наукової літератури показав, що в умовах гібридної війни когнітивна безпека стає критично важливим інструментом для збереження національного суверенітету, цілісності інформаційного простору та соціальної єдності. Основними загрозами виступають інформаційні атаки, маніпуляція громадською думкою, поширення дезінформації, підміна історичних наративів, фрагментація колективної ідентичності. Під впливом цих чинників відбувається ерозія критичного мислення, зниження довіри до державних інституцій та поляризація суспільства.

Узагальнення сучасних теоретичних підходів дозволяє виокремити основні напрями дослідження когнітивної безпеки**:**

- аналіз когнітивних загроз у політичних процесах;
- вивчення механізмів формування когнітивної стійкості в громадян;
- дослідження стратегічних наративів і контрнаративів як інструментів захисту;
- розробка індикаторів когнітивної вразливості суспільства;
- роль державної комунікації та медіаосвіти в протидії маніпулятивному впливу;
- створення моделей когнітивного моніторингу в системі національної безпеки.

Таким чином, когнітивна безпека розглядається не лише як захист від інформаційного впливу, а як стратегічний ресурс – запорука стабільності демократичного устрою, ефективного державного управління та самозбереження суспільства в умовах цифрової доби.

РОЗДІЛ 2. КОГНІТИВНА БЕЗПЕКА УКРАЇНСЬКОГО СУСПІЛЬСТВА В УМОВАХ ГІБРИДНОГО ПРОТИСТОЯННЯ

2.1. Аналіз та класифікація загроз когнітивній безпеці українського суспільства

Сучасний політико-інформаційний контент, що безпосередньо впливає на свідомість людини, набуває ознак специфічного ресурсу чи навіть товару, який може бути об’єктом купівлі, продажу, маніпуляцій та злочинного використання. Така динаміка актуалізує необхідність посиленої уваги до захисту когнітивного простору особистості, своєчасного виявлення загроз когнітивній безпеці та їхньої нейтралізації. Ефективна протидія цим загрозам передбачає не лише ідентифікацію їхніх джерел, а й осмислення глибинних причин їхнього виникнення, що потребує системного підходу та розробки класифікаційних моделей.

Для упорядкування наукових підходів у досліджуваній сфері передусім необхідно уточнити зміст понять «загроза» та «загроза когнітивній безпеці». Загроза (від англ. *threat*) – це будь-які обставини чи події, що потенційно здатні порушити політику інформаційної безпеки або завдати шкоди функціонуванню автоматизованої системи. Спробу реалізації такої загрози прийнято визначати як атаку [129]. У ширшому значенні загроза розглядається як можлива подія, дія (вплив), процес чи явище, які можуть завдати шкоди чиїмось інтересам. У цьому контексті доцільним є аналіз наукових поглядів на сутність категорії «загроза» [180]. Н. Різник вважає, що загроза виникає тоді, коли негативні чинники безпосередньо впливають на безпеку об’єкта, порушуючи стан його рівноваги [160, с.118].

Дослідження динаміки загроз національним інтересам України, здійснене Л. Петренко [136], дозволило встановити низку хронологічних закономірностей їхнього формування та прояву:

- загрози мають циклічний характер і проходять кілька етапів розвитку – від початкових до завершальних, із можливістю зворотної динаміки;
- стійкість загроз полягає в їхній здатності відхилятися під впливом протидій від оптимального напряму, проте з часом повертатися до вихідного стану після зниження інтенсивності цих впливів;
- загрози реалізуються у хвилеподібному ритмі: вони посилюються у фазах внутрішньої нестабільності об'єкта й послаблюються за умов досягнення ним стабільності та здатності до опору;
- взаємодія кількох загроз може збігатися в часі, що формує глобальну мультиплікативну загрозу, спроможну зруйнувати всю систему державної безпеки.

Загрози когнітивній безпеці України в інформаційній та політичній сфері можна визначити як сукупність умов, чинників і процесів, що створюють небезпеку для життєво важливих інтересів держави, суспільства та особи шляхом негативного інформаційного впливу на свідомість і поведінку громадян, а також через можливі посягання на інформаційні ресурси та інформаційно-технічну інфраструктуру [137]. Такі загрози охоплюють як зовнішні, так і внутрішні виклики, що проявляються у формі інформаційних маніпуляцій, пропагандистських кампаній, дезінформації, кібератак та інших форм деструктивного впливу на когнітивний простір держави.

Попри виявлені закономірності їхнього розвитку та прояву, систематизація загроз когнітивній безпеці є складним завданням. Це пояснюється високим рівнем взаємозалежності між окремими загрозами, а також впливом спільних деструктивних чинників, які водночас стають джерелами їхнього виникнення. Крім того, динаміка інформаційного середовища, технологічний прогрес та гібридний характер сучасних конфліктів зумовлюють появу нових форм загроз, що потребують постійного оновлення підходів до їхньої класифікації та нейтралізації.

За оцінкою фахівців Cognitive-Security Research-Labs при Army Cyber Institute (Вест-Пойнт/West Point), забезпечення когнітивної безпеки в умовах інформаційної протидії спрямоване на збереження здатності до раціонального ухвалення рішень. Це передбачає спільне прийняття єдиної картини реальності та загальних «правил гри», які забезпечують основи для рішень, а також запобігання емоційним маніпуляціям і захист як індивідів, так і спільнот для ефективної колективної реакції на виклики.

До основних загроз когнітивній безпеці належать:

- цілеспрямований вплив на механізми ухвалення рішень людьми;
- втручання у взаємодію людини з машиною, зокрема в контексті команд «людина – машина»;
- маніпулятивний вплив на соціальну поведінку особи в групі;
- проблеми, пов'язані з формою подання інформації людині, зокрема через симбіотичні інтерфейси «людина – комп'ютер»;
- розширення взаємодії за межі традиційного HMI до HME («людина – машина – екосистема»);
- використання так званих «збройних наративів» як інструменту впливу;
- функціонування в умовах політизованого та комерціалізованого інформаційного середовища [195].

Відповідно до положень Доктрини інформаційної безпеки України (2017 р.) [142], функції з моніторингу загроз, що можуть зашкодити національним інтересам у сфері інформаційного простору, покладені на Міністерство інформаційної політики. Водночас, як підкреслюють дослідники, «залишається невирішеною проблема контентно-комунікаційної та комунікаційно-контентної взаємодії на всіх рівнях між владою і суспільством» [84, с. 165].

Стратегія інформаційної безпеки України (2021 р.) окреслює ключові глобальні виклики, серед яких:

- загроза, яку становить інформаційна політика рф не лише для України, але й для інших демократичних держав;

- трансформація соціальних мереж у самостійних суб'єктів впливу в інформаційному середовищі;
- низький рівень медіаграмотності населення на тлі стрімкого розвитку цифрових технологій [151].

В умовах сучасних геополітичних та суспільно-політичних трансформацій інформаційна безпека Української держави та її громадян опинилася під реальною прямою загрозою. Широкий спектр таких загроз був зафіксований у Законі України № 964-IV «Про основи національної безпеки України» від 19 червня 2003 року. Згідно зі статтею 7 (у редакції, зміненій Законом № 1170-VII від 27 березня 2014 року), серед основних загроз національним інтересам у сфері інформаційної безпеки визначаються обмеження свободи слова й доступу до публічної інформації; поширення насильства, жорстокості та порнографії через засоби масової інформації; комп'ютерна злочинність і кібертероризм; розголошення державної таємниці або іншої інформації з обмеженим доступом, яка має важливе значення для національних інтересів; а також маніпулятивний вплив на суспільну свідомість через поширення недостовірної, викривленої чи неповної інформації [146].

Актуалізований перелік таких загроз, хоча й потребує подальшого доповнення, детально подано в «Стратегії національної безпеки України», затвердженій Указом Президента України від 14 вересня 2020 року [154]. Основна увага в документі приділена таким формам інформаційного впливу, як інформаційно-психологічна війна, знецінення української мови й культури, фальсифікація національної історії, а також створення альтернативної реальності через викривлену інформаційну картину світу, що транслюється російськими масмедіа. Серед додаткових викликів названо ведення цілеспрямованої інформаційної війни проти України, відсутність цілісної державної комунікативної політики, низький рівень медіакультури в суспільстві. Стратегія також окреслює загрози у сфері кібербезпеки, а саме: вразливість критичної інфраструктури та державних інформаційних ресурсів до кібератак; моральну й технічну застарілість систем захисту державної таємниці й інших видів

інформації з обмеженим доступом. Окремими розділами визначено пріоритети державної політики у сфері забезпечення як інформаційної, так і кібербезпеки.

У межах інформаційного підходу до вивчення когнітивної безпеки важливим є розуміння того, як саме можна класифікувати загрози, що виникають у цій сфері. Така класифікація дозволяє не лише точніше оцінити потенційну шкоду, а й розробити більш ефективні механізми протидії.

Передусім загрози розрізняються *за характером їхньої реалізації*. До *реальних загроз* належать ті, які вже мають активну деструктивну силу або її активізація неминуча: вони не обмежені в просторі та часі. *Потенційні загрози* виникають за певних умов середовища, наприклад, у разі послаблення інституційних механізмів. *Здійснені* загрози вже були реалізовані, тобто негативні наслідки настали. Натомість *уявні* загрози є умовними: вони можуть нагадувати реальні загрози, але фактично такими не є, часто мають залякувальний або маніпулятивний ефект.

Ще одним важливим критерієм є *ступінь гіпотетичної шкоди*, яку може завдати загроза. *Загрозливі дії* – це як помітні, так і потенційні прояви, що можуть перешкоджати реалізації національних інтересів у сфері інформаційної безпеки. Вони можуть впливати на функціонування системи управління безпекою, а також загрожувати її ключовим елементам. Зі свого боку, *небезпечні загрози* мають більш радикальний характер: вони прямо дестабілізують безпекову систему.

Існує кілька категорій щодо *ймовірності реалізації. . Вірогідні загрози* – це ті, які з великою ймовірністю настануть за певного збігу обставин. Наприклад, інформаційна атака на ресурси державних структур часто передує основному наступу. *Неможливі загрози*, навпаки, не можуть бути реалізовані навіть у теорії: вони більше нагадують пропагандистські вкиди або спроби залякати. І нарешті, *випадкові загрози* залежать від конкретного контексту та аналізуються за допомогою певних інструментів, таких як теорія ймовірностей чи теорія ігор, що дозволяє передбачати варіативність поведінки у випадкових ситуаціях. Окремо варто звернути увагу на *рівень детермінованості загроз*. *Випадкові загрози*

можуть або виникнути, або ні, наприклад, раптова хакерська атака на інформаційну систему органів влади. Натомість *закономірні загрози* мають постійний, повторюваний характер. Вони формуються під впливом сталих, об'єктивних умов функціонування та розвитку системи інформаційної безпеки й часто є результатом тривалих тенденцій або структурних вразливостей [184, с.285-286].

Джерела загроз безпеці можуть мати як суб'єктивне походження, коли вони пов'язані з діями окремої особистості, так і об'єктивний характер, зумовлений зовнішніми чи природними чинниками. Усі джерела загроз за характером виникнення умовно поділяють на три основні категорії [180]:

1. Антропогенні загрози – це ті, що виникають унаслідок діяльності людини. Вони можуть бути спричинені як навмисними (саботаж, кібератаки), так і ненавмисними діями (помилки персоналу, недбалість, нехтування правилами безпеки). Цей тип загроз вважається наймасштабнішим і таким, що має ключове значення для організації захисту, оскільки поведінку суб'єктів можна аналізувати, прогнозувати та враховувати при формуванні захисних заходів. Важливо, що ці загрози часто керовані, тобто на них можна впливати через регламенти, контроль доступу, навчання тощо. Суб'єктом антропогенної загрози може бути як внутрішня особа (працівник із санкціонованим доступом), так і зовнішній агент, що діє несанкціоновано.

2. Техногенні загрози пов'язані з використанням і розвитком технічних засобів. Вони виникають у результаті збоїв у роботі обладнання, програмного забезпечення, інфраструктурних систем тощо. Такий тип загроз є похідним від цивілізаційного прогресу: що складніші технології ми створюємо, то вищим стає ризик їхнього виходу з-під контролю.

3. Стихійні загрози, або загрози природного походження, об'єднують ситуації, що є проявами непереборної сили (форс-мажору). До них належать стихійні лиха: повені, землетруси, пожежі, урагани, а також інші події, які неможливо передбачити або яким не можна запобігти. Навіть у разі, коли загроза передбачувана, часто бракує технологій або ресурсів для її ефективного

стримування. Відповідно, ці загрози вважаються об'єктивними та універсальними, адже вони можуть загрожувати незалежно від людської волі чи поведінки.

У межах американської дослідницької традиції, що тяжіє до кібернетичного й технологічного підходу, особливу увагу сьогодні приділяють викликам, пов'язаним із впровадженням технологій штучного інтелекту (далі – ШІ). Хоча ці технології відкривають значні можливості для вдосконалення управлінських, аналітичних і комунікаційних процесів, водночас вони несуть реальні ризики для когнітивної безпеки як окремих осіб, так і цілих суспільств.

Нижче подано основні загрози, які постають унаслідок використання ШІ в інформаційному та когнітивному просторах:

1. Deepfakes. Це технологія створення фальшивих, але дуже реалістичних зображень, відео- чи аудіофайлів за допомогою нейромереж. Візуальна й звукова достовірність таких матеріалів дозволяє легко вводити аудиторію в оману. Deepfakes можуть використовуватися для дискредитації політичних лідерів, створення фальшивих новин, шантажу або втручання у виборчі процеси. В умовах високої довіри до візуального контенту вони стають надзвичайно ефективним інструментом когнітивного впливу.

2. Дезінформація, поширювана ШІ. Сучасні алгоритми штучного інтелекту здатні генерувати великі обсяги контенту з фейковими наративами та розповсюджувати їх у мережі за лічені хвилини. Автоматизовані акаунти (боти) та системи генерації текстів (на кшталт GPT) здатні моделювати переконливі повідомлення, які маніпулюють емоціями, викликають паніку або підривають довіру до інституцій. Це особливо небезпечно в кризових ситуаціях, коли швидкість і точність інформації є критично важливими.

3. Упередженість у системах ШІ (algorithmic bias). ШІ навчається на основі великих масивів даних, які часто відображають наявні соціальні чи культурні упередження. Унаслідок цього система може відтворювати дискримінаційні моделі, наприклад, у прийомі на роботу, визначенні ступеня загрози особи,

доступі до послуг тощо. Це поглиблює соціальну нерівність і формує недовіру до технологій.

4. Порушення конфіденційності. Системи ШІ здатні обробляти гігантські обсяги персональних даних включно з фото, голосами, поведінковими характеристиками. Зокрема, технології розпізнавання обличчя і відстеження пересувань можуть застосовуватися для незаконного спостереження, стеження або контролю за громадянами без їхньої згоди. Це створює загрозу масового порушення прав людини.

5. Маніпуляція поведінкою через персоналізований контент. ШІ все точніше «вгадує» інтереси користувача і формує для нього індивідуалізований інформаційний простір («інформаційна бульбашка»). Через це людину можна системно підштовхувати до певних рішень, змін у переконаннях або навіть радикалізації, що особливо небезпечно в політичних кампаніях, питаннях національної ідентичності чи безпеки.

6. Кібератаки на основі ШІ. Штучний інтелект дозволяє розробляти нові, більш складні та адаптивні види кібератак – від автоматизованих фішингових повідомлень до атак на інфраструктури. Такі атаки важче виявити, а швидкість реагування людини може бути недостатньою для протидії. У майбутньому можна очікувати появу повністю автономних систем кібернападу.

7. Змагальні (адверсарні) атаки. Цей тип атак спрямований безпосередньо на алгоритми ШІ: злочинець навмисне змінює вхідні дані так, щоб система неправильно їх обробила. Наприклад, розпізнавання обличчя або об’єктів може давати помилкові результати через приховані маніпуляції із зображенням. Такі атаки можуть бути використані проти систем безпеки, автономного транспорту чи цифрового нагляду.

8. Залежність від ШІ. Зі зростанням ефективності та зручності ШІ-систем зростає й ризик надмірної довіри до них. Це може призвести до зниження критичного мислення, знецінення людської експертизи та втрати здатності діяти в разі технічних збоїв або помилок системи. Людина перестає самостійно аналізувати інформацію, покладаючись на автоматизовані висновки.

9. Зменшення людської автономії. Що більше когнітивних функцій делегується штучному інтелекту, то менше простору залишається для самостійного людського мислення, ухвалення рішень і моральної відповідальності. Це породжує не лише технологічні, а й етичні загрози, адже рішення, що ухвалюються за участі ШІ, можуть впливати на долі людей і спільнот.

Таким чином, розгляд когнітивної безпеки в контексті впровадження ШІ потребує комплексного аналізу – не лише технічного, а й соціального, психологічного та етичного. Відповідь на ці виклики вимагає міждисциплінарного підходу та перегляду наявних стратегій інформаційного та політичного складника національної безпеки.

Сучасні генеративні системи на основі штучного інтелекту, зокрема ChatGPT від OpenAI, значно просунулися у сфері створення текстового контенту, який за структурою, стилістикою та логікою побудови все більше наближається до людського мовлення. Ці системи здатні не лише відтворювати складні мовні конструкції, а й формувати переконливі наративи, що потенційно впливають на переконання, емоції та поведінку користувачів. Така здатність, попри очевидні переваги у сферах освіти, науки, бізнесу чи державного управління, водночас становить серйозну загрозу для когнітивної безпеки в інформаційному середовищі [231].

Моніторинг інформаційного простору охоплює лише частину актуальних загроз через дефіцит високотехнологічних інструментів на основі штучного інтелекту та кваліфікованих кадрів, що, зі свого боку, обмежує повноту й оперативність виявлення деструктивних інформаційних впливів. За таких умов виникають прогалини в аналітичному супроводі, які відкривають простір для оперативних інформаційно-психологічних операцій противника та ускладнюють своєчасну реакцію на них. Емпірична специфіка загроз, що впливають на громадянське суспільство та медіа, може бути структуровано представлена для наочності, оскільки систематизація проявів і характеристик впливів сприяє більш чіткому їх окресленню та розумінню. Такий підхід дозволяє впорядкувати

наявні спостереження, узагальнити практичні прояви ризиків і представити їх у формі, придатній для подальшого аналізу (Табл. 2.1).

Таблиця 2.1

Класифікація емпіричних цифрових загроз для громадянського суспільства та медіа в Україні

Тип загрози	Вектор атаки	Задокументований вплив	Емпіричний приклад
Фішингові кампанії	Email/SMS зі шкідливими посиланнями	Витік даних активістів, компрометація комунікацій	Атака за допомогою Remcos RAT на організації громадянського суспільства
Шкідливе ПЗ (Malware)	Інфіковане програмне забезпечення	Компрометація мереж, ескалація цифрового шпигунства	Активність групи Gamaredon проти державних установ
DDoS-атаки	Перевантаження серверів	Тимчасове блокування доступу до інформаційних ресурсів	Координовані атаки на новинні портали під час кризових подій
Координована дезінформація	Боти та фейкові акаунти в соцмережах	Підрив довіри до інституцій, розкол суспільства	Кампанії із заперечення воєнних злочинів або дискредитації волонтерських ініціатив

Таблиця створена автором на основі аналізу літературних джерел представлених у списку джерел дисертаційного дослідження [208] [218,] [225], [230].

Серед фахівців існує консенсус, що ефективне реагування на ці виклики потребує мультидисциплінарного підходу, який поєднує технологічні рішення, нормативно-правові механізми та міжнародну кооперацію. Лише скоординовані дії урядових структур, технологічних компаній та наукової спільноти можуть

забезпечити етичне, прозоре та контрольоване впровадження ШІ, що відповідатиме інтересам безпеки й розвитку.

Власне когнітивна безпека, на відміну від традиційної кібербезпеки, яка здебільшого фокусується на захисті інформаційної інфраструктури, охоплює захист ментального простору особистості та колективної свідомості. Вона передбачає запобігання інформаційному впливу, здатному маніпулювати, дезорієнтувати або підривати здатність до критичного мислення. Досягнення когнітивної безпеки в контексті подолання базових загроз ґрунтується на трьох ключових елементах:

1. Підвищення стійкості (резильєнтності) до маніпуляцій. Першим і, безумовно, фундаментальним напрямом досягнення когнітивної безпеки є формування індивідуальної та колективної стійкості до маніпулятивного впливу. Це передбачає насамперед:

– розвиток критичного мислення та медіаграмотності через впровадження відповідних освітніх програм у школах, університетах, системах підвищення кваліфікації;

– створення інструментів виявлення дезінформації в реальному часі, таких як програми для виявлення deepfake-контенту або автоматизовані механізми перевірки фактів;

– адаптацію таких інструментів до швидкості та обсягів інформаційного потоку в Інтернеті, аби забезпечити адекватну реакцію на інформаційні атаки.

Таким чином, ідеться про формування свідомої аудиторії, здатної самостійно оцінювати достовірність інформації, розрізняти пропаганду та захищатися від деструктивного контенту.

2. Забезпечення ситуаційної обізнаності. Другий елемент когнітивної безпеки пов’язаний з оперативним розумінням інформаційної ситуації, її змін і потенційних загроз, що означає:

– виявлення шкідливих інформаційних кампаній, які поширюються через соціальні мережі, месенджери, відеохостинги тощо;

– аналіз структури, каналів і цільових груп впливу, а також характеристик джерел дезінформації;

– впровадження віртуальних асистентів та аналітичних систем, які здатні відстежувати, категоризувати й передавати сигнали про загрози в реальному часі.

Таким чином формується інформаційна спроможність суспільства – не лише реагувати, а й передбачати та нейтралізовувати потенційні маніпулятивні впливи ще на ранніх етапах їхнього прояву.

3. Розробка інструментів когнітивної взаємодії. Третім напрямом є створення ефективних й етичних інструментів взаємодії в цифровому середовищі, які дозволяють протистояти шкідливим впливам з боку бот-мереж, програмних агентів, фейкових акаунтів та інших автоматизованих засобів інформаційної атаки. Сюди належать:

– виявлення автоматизованої поведінки в соціальних мережах;

– автентифікація контенту та його джерел;

– розробка протоколів етичного впровадження ШІ в системи комунікації та інформаційної взаємодії.

Ці технології мають не лише блокувати маніпулятивний контент, але й сприяти збереженню прозорого, етичного й відкритого цифрового простору.

Систематизація сучасних політико-інформаційних загроз у російсько-українській війні дозволяє виокремити кілька ключових типів, які демонструють свою ефективність на практиці:

Стратегічна дезінформація та пропаганда. Цей тип загрози спрямований на формування хибної картини світу як всередині країни-агресора, так і на міжнародній арені. Ключовою рисою такої загрози є створення альтернативної реальності, де агресія представлена як «спеціальна воєнна операція», а збройний опір – як активність «неонацистського режиму». Яскравими прикладами є масована кампанія в російських державних медіа та соцмережах, що експлікує заперечення воєнних злочинів у Бучі чи Маріуполі, а також наративи про «біологічну зброю», розроблену в українських лабораторіях. Мета –

деморалізувати українське суспільство, підірвати довіру до влади та заблокувати міжнародну підтримку.

Оперативні інформаційно-психологічні операції (ІПО). Від стратегічної пропаганди ІПО відрізняються тактичним характером і прив'язкою до конкретних подій на фронті. Вони проводяться для впливу на моральний стан українських військовослужбовців та цивільного населення в прифронтових регіонах. Сюди належать фейкові повідомлення про «оточення» ЗСУ, «масове дезертирство» або «здачу міст», що поширюються через Telegram-канали та соцмережі. Ефективність цих операцій полягає в їхній швидкості та здатності експлуатувати інформаційну невизначеність в умовах бойових дій.

Кібератаки на критичну інфраструктуру та системи управління. Цей тип загроз перетворився з інструменту шпигунства та дискредитації на засіб ведення бойових дій. Масовані атаки на енергосистему України взимку 2022-2023 років мали ціллю не лише деморалізувати цивільне населення, але й підірвати економічний та логістичний потенціал країни, ускладнивши роботу промисловості та ЗСУ. Зазначені дослідження [235] підтверджують, що, незважаючи на масштабність, багато атак було відбито завдяки високому рівню кіберстійкості, що свідчить про критичну важливість резильєнтності, а не лише захисту.

Цифрове втручання для міжнародної дестабілізації. росія активно використовує інформаційні канали для впливу на громадську думку в країнах-союзницях України. Мета – послабити єдність міжнародної коаліції, спровокувати соціальну напругу та популяризувати ізоляціоністські настрої. Інструментами такого типу загроз є фінансування політичних сил, створення мереж псевдоекспертних центрів та координовані кампанії в соцмережах, що експлуатують теми енергетичної кризи, інфляції та втоми від війни.

Таким чином, когнітивна безпека є соціотехнічною категорією, що передбачає тісну інтеграцію соціальних, гуманітарних і технічних знань. Її ефективне забезпечення та подолання загроз можливе лише за умови співпраці держави, приватного сектору, академічної та громадянської спільноти, які мають

об’єднати зусилля для створення стійкої екосистеми захисту свідомості людини в умовах стрімкої цифрової трансформації.

2.2. Гібридна війна як загроза когнітивній безпеці сучасного суспільства

Під час воєнно-політичного та інформаційного протистояння особливого значення набуває феномен гібридної війни, яка поєднує традиційні військові засоби із широким спектром немілітарних інструментів впливу. Однією з ключових цілей гібридної агресії є когнітивний простір суспільства, у межах якого здійснюється вплив на свідомість, емоційні стани, ціннісні орієнтації та поведінкові установки населення. Гібридна війна спрямована не лише на фізичне послаблення противника, а насамперед на підрив його здатності до раціонального мислення, колективної дії та стратегічного ухвалення рішень. Через використання інформаційних операцій, пропаганди, дезінформації та психологічного тиску формується викривлене сприйняття реальності, що істотно підвищує вразливість когнітивної безпеки. За таких умов когнітивний вимір безпеки перетворюється на один із визначальних факторів стійкості держави та суспільства в умовах тривалого воєнного протистояння.

Із розвитком та поширенням цифрових технологій у всіх сферах суспільної діяльності почала наростати залежність від інформації. Сучасні конфлікти все частіше мігрують у медіа- та кіберпростір, що дає змогу оперативно поширювати дезінформацію, модифікувати перцепцію подій. Значні прояви маніпуляцій та використання інформації як одного із засобів ведення війни щоденно простежуються і у війні росії проти вільної та незалежної України (лютий 2022 року), ХАМАС-у та Ізраїлю (жовтень 2023 року), мали місце в П’ятиденній війні росії та Грузії (серпень 2008 року) тощо. У світлі зазначеного зауважимо, що концепт когнітивної безпеки наразі посідає майже рівноцінне місце з безпекою фізичною, особливо в умовах гібридної війни.

Характерно, що гібридна війна як феномен має далеко не тимчасовий характер, а поетапно стає складною стратегією, яка використовується на

постійній основі. У зв'язку із зазначеним додамо: питання когнітивної безпеки – це не лише внутрішня проблема певної країни, а проблематика міжнародного значення, яке зумовлює ухвалення консолідованих рішень задля протидії відповідним загрозам.

Феномен гібридної війни в контексті політологічних досліджень набуває особливої популярності після політичних дебатів американських військових спеціалістів (морська піхота США), які публікують спільну статтю, присвячену зростанню кількості гібридних воєн, першопричини яких вони бачать у «домінантній ролі людського виміру у війні». У публікації ідеться про звичайні та особливі стратегії, які застосовуються в ході ведення сучасних воєн, переважно засновані на методах психолого-інформаційного впливу [246]. Удруге глобально за новий тип війни почали говорити з квітня 2014 року, коли росія несанкціоновано ввела регулярні війська на територію України, а за тим здійснила анексію Криму. Довготривала, багаторічна кампанія агресора, особливо на території Донецької та Луганської областей, де превалює кількість російськомовного населення, багато в чому виправдала себе через використання соціально-політичної поляризації, потужного економічного впливу, озброєння сил, інформаційної пропаганди. На щастя, цих заходів виявилося недостатньо з початком повномасштабного вторгнення в лютому 2022 року, тому концепція «візьмемо Київ за три дні» зазнала фіаско [181].

На думку В. Гулая, у межах гібридної війни комунікаційна діяльність передбачає масований психологічний вплив, що здійснюється переважно через емоційний, а не логічний спосіб подачі інформації, із перенесенням акценту з сутності повідомлення на форми комунікаційної взаємодії, які забезпечують пошук ефективних способів подачі, формування потрібних асоціацій та образів і поширення відомостей, здатних завдати політичної шкоди державі; у зв'язку з цим інформаційний фронт гібридної війни Російської Федерації проти України розгортається одночасно на кількох напрямах: серед населення в зоні конфлікту, серед населення держави-жертви поза безпосередньою зоною бойових дій, серед громадян країни-агресора та серед міжнародного співтовариства [47, с.233].

Явище гібридної війни має два головні модуси існування – матеріальний (фізичний) і дискурсивний. Вони є асиметричні. У військовому (матеріальному) вимірі війна за Незалежність України є локалізованою, оскільки охоплює частину території України, натомість дискурс цієї гібридної війни набув глобального масштабу [187, с. 47]. У широкому розумінні гібридну війну розуміють як специфічний вид збройного конфлікту, у якому слабший проти сильного прагне нівелювати його конвенційні переваги. Тобто в цій ситуації спостерігаємо зіткнення симетричних та асиметричних дій [54, с. 10]. Слушною також є думка інших науковців, які розкривають цей тип війни через її структурну природу. Так, гібридна війна є формою асиметричної війни і використовує кілька інструментів влади вздовж горизонтальної та вертикальної осі. Дії недержавних акторів проти державних є зазвичай асиметричними. Вони використовують методи, не характерні для регулярних військ держав. Тому війни державних і недержавних суб'єктів є асиметричними війнами [42, с. 25].

Для С. Дерев'янка вихідним в дослідженні гібридних війн є розуміння їх як політико-правового феномену [56, с. 11-12]. Чинне законодавство України наразі не містить чіткого визначення терміна «гібридна війна». Водночас певне уявлення про зміст цього поняття можна отримати, звернувшись до формулювань, поданих у новій редакції «Воєнної доктрини України» 2015 року. У документі серед ключових тенденцій, що впливають на трансформацію глобального безпекового середовища, виокремлене зростання ролі асиметричного застосування воєнної сили з боку незаконних збройних формувань, а також акцентовано на комплексному використанні як воєнних, так і невоєнних засобів впливу, наприклад, економічних, політичних, інформаційно-психологічних тощо, що суттєво змінює природу збройної боротьби (п. 6) [24]. Однак, у 2021 році зазначена доктрина була скасована й замінена новим стратегічним документом – «Стратегією воєнної безпеки України» [150]. У Стратегії прямо зазначено, що головною загрозою у воєнній сфері національного рівня залишається гібридна війна, яку веде проти України російська федерація. Вона характеризується поєднанням різноманітних форм агресії, включно з

прихованим використанням регулярних збройних сил, незаконних формувань і терористичних організацій, а також із застосуванням пропаганди, диверсій, терористичних актів, саботажу та цілеспрямованим завданням шкоди громадянам, юридичним особам і державній інфраструктурі України.

Відповідно, створюється особливий дискурс гібридних війн зі своїми засобами породження смислів. Зокрема, в аспекті комунікацій завдання гібридної війни полягає не в досягненні порозуміння, а у створенні численних непорозумінь і хаосу мислення, продукуванні різних версій подій, які однаково претендують на істинність. Аналогічно збройні операції здійснюються так, щоб не було зрозуміло, хто за ними стоїть і яку мету вони мають. Відмова від фізичного насильства не означає відмови від насильства когнітивного – емоційного та інтелектуального, коли сторони «м'якими» засобами намагаються нав'язати противникові власні уявлення про устрій реальності, присвоїти свої імена речам, представити свою логіку міркувань як єдино правильну.

Колишній міністр оборони США Р. Гейтс характеризував гібридну війну як поєднання сучасних технологій і архаїки, сукупність застосування потенціалу збройних сил держави з фанатичним і невичерпним прагненням інсургентів, які ведуть «партизанські» бойові дії, а також спільне використання продукції компанії «Microsoft» та технологій «STELS», керованих камікадзе [226]. Узагальнюючи вказане, зауважимо, що «гібридність» в такому трактуванні ідентифікується через симбіоз форм економічного, культурного, інформаційного, збройного впливу на суб'єкт, обраний як ціль для захоплення. Про такий тип війни як динамічне явище напише директор Інституту зовнішньої політики Дипломатичної академії України Г. Перепелиця. Він зазначає, що вона охоплює активні бойові дії, переговори, миротворчі дії, ескалацію конфлікту та перемир'я, адже в такому мутованому вигляді війни розмитою стала лінія між війною та миром. Досить часто, навіть по завершенню мирних переговорів або оголошенню остаточного перемир'я, гібридна війна продовжує тривати, але з меншою інтенсивністю (на інформаційному, культурному, інших фронтах) [135, с. 34].

Постає цілком логічне питання: які «переваги» ведення саме гібридної війни у порівнянні з її класичним варіантом? Передусім, як транслює російська пропаганда, це сам факт заперечення війни або використання дефініцій, що за своїм змістовим наповненням не відповідають фактичному стану подій (збройний конфлікт, тимчасова операція, антитерористичні заходи і т.д.). У такий спосіб затягується процес притягнення до відповідальності країни-загарбника за порушення територіальної цілісності й миру в іншій суверенній країні; світова спільнота залишається певний час дезорієнтованою, перебуває в пошуку оптимальних та правомірних засобів впливу на агресора.

У той же час, як зазначено на офіційному сайті НАТО, хоча сучасні конфлікти ведуться новими, інноваційними та радикально різними методами, вони все менше стосуються безпосередньої участі збройних сил, сама природа міжнародної безпеки та міжнародних конфліктів залишається незмінною. Сталими є закономірності, яким підпорядковуються міжнародні відносини, наприклад, «гра з нульовою сумою», де перемога однієї сторони означає поразку іншої; неминучість збройних конфліктів, збереження дилеми безпеки та балансу сил [203]. У зв'язку з цим можемо навести приклади технологій «кольорових революцій» (із комплексним використанням можливостей єдиного інформаційного простору та сучасних інформаційних технологій), що в поєднанні з політичним та економічним впливом дозволяють досягти мети без військового втручання, за потреби – з точковою ліквідацією представників політичної та економічної еліти, правоохоронних органів.

Після багатьох років пропаганди рф наратив про «братні народи» змінився закликом «звільнити населення України від фашистів, націоналістів та бандерівців, захистити російськомовне населення». Нацистів так і не знайшли, а російськомовне населення, як і україномовне, стало на захист своїх міст/сіл, своїх будинків та сімей від непроханих «визволителів». Для українців, як і для будь-якої іншої нації, мова – дім життєдайного буття, духовний, світоглядний, націєтворчий корінь. Теза, яку цілеспрямовано нав'язують: «Яка різниця, якою мовою говорити», – у сучасних умовах цинічно фальшива. Вона є формою

нинішнього повзучого, так званого м'якого зросійщення, яке підступно висмоктує з українців національну сутність, культивує російську імперську свідомість, створює передумови нефункціональності української мови. За ігноруванням комунікативної функції мови приховано знищення інших, не менш важливих, функцій: ідентифікаційної, експресивної, гносеологічної, мислетворчої, естетичної, культуроносної, номінативної тощо. Тобто питання всебічного функціонування української мови в усіх державних і суспільних інституціях – це питання життя або смерті української нації [93, с. 127]. Важливим аспектом гібридної війни також стала активна протидія курсу України на інтеграцію і членство в ЄС.

Існує також альтернативний внутрішній фронт гібридної війни: росія тривалий час масштабно поширює лозунги і наративи кремля серед своїх громадян як за допомогою транслювання специфічної інформації, так і шляхом блокування зовнішніх джерел інформації для місцевого населення. Один із найскладніших аспектів цієї кризи полягає в його оцінці ззовні. Тут варто бути обережним, оскільки те, що здається неефективною пропагандою для українців, може бути сприйняте аудиторією внутрішньо. Ця теза підтверджує ще одну особливість гібридної війни: складно вести інформаційну кампанію, коли агресор грає відкрито, тоді як латентні довготривалі маніпуляції все ж мають вплив на певну частину населення.

Вторгнення росії та жахливі сцени руйнування українських міст створили глобальну кризу і моральний консенсус, що стало надзвичайно рідкісним у цифрову епоху. Українці через резистенцію військовій агресії та єдності в бажанні жити у вільній, незалежній країні два роки невпинно розповідають світу про те, що відбувається з ними. Українська діаспора проявила потужний опір загарбницьким лозунгам кремля в соціальних мережах, світових медіа, мережі Інтернет в цілому. Слушними вважаємо міркування старшого наукового співробітника Центру Шоренштейна з питань медіа, політики та публічної політики Гарвардської школи Кеннеді щодо того того, що інтернет-аудиторія, особливо та, яка стежить за останніми новинами, з часом стала більш скептична,

ніж раніше, і краще розпізнає спроби впливу: «Ми не тільки можемо розплутати їхні операції під чужими прапорами і дезінформацію, але ми можемо показати, наскільки погано виконані ці пропагандистські спроби» [243].

Ситуація загострюється також тому, що агресивним імперським амбіціям москви піддаються лідери Угорщини, Словаччини, Сербії та інших країн. Вони проявляють агресію до української культури або незадоволення нею, перекручуючи історичні факти, доводячи їх до абсурду; у повсякденному житті часто вдаються до банальної фальсифікації, відвертої та прихованої маніпуляції, упереджених висловлень, брехні, наклепів та інших методів, щоб проводити гібридно-інформаційну війну проти України.

Однак, не лише реалії українського сьогодення слугують яскравим кейсом гібридної форми війни. З кінця 1990-х рр. Китай вивчає методи так званої «необмеженої війни», прийоми якої передбачають комп'ютерне хакерство та зараження вірусами, зрив роботи банківської системи, маніпуляції на валютних біржах, тероризм у міських умовах, дезінформацію в медіа [23, с. 99]. Поки не зрозуміло, наскільки необмежена війна стала офіційною китайською доктриною, хоча деякі елементи цієї концепції проглядаються в китайській політиці «трьох воєн» щодо територіальних претензій у Східно-Китайському та Південно-Китайському морях. Китай уникає відкритого застосування військової сили, але для досягнення своїх цілей використовує психологічні операції, медійні маніпуляції та правові претензії (так звану правову війну).

За таких умов роль і значення когнітивної безпеки значно інтенсифікується. Саме поняття визначається як концептуальна парадигма, яка охоплює механізми й стратегії для захисту когнітивних процесів та інтелектуальної діяльності в особистому та колективному сприйнятті, обробці інформації. Подібного роду ідея акцентує на виявленні, аналізі та протидії загрозам, пов'язаним із маніпуляціями когнітивними процесами, що можуть спотворити об'єктивне сприйняття дійсності і призвести до психологічного впливу на індивіда.

Очевидну перевагу в когнітивній війні отримує той, хто вчиняє перший крок і вибирає час, місце і методи наступу. Завдяки відкритості соціальних мереж противник легко переорієнтовує свою діяльність на окремих осіб, обрані групи або широку громадськість за допомогою соціального меседжингу, впливу через соціальні медіа, цільового розповсюдження документів, відеоматеріалів тощо. Засоби гібридної війни дають можливість систематично моніторити за ворогом, здійснювати хакерські атаки і відстежувати життя зацікавлених осіб у соціальних мережах. Ефективна оборона вимагає принаймні розуміння того, що когнітивна кампанія вже відбувається. Для цього необхідно мати здатність спостерігати і реагувати на ухвалення рішень. Застосування технологій може забезпечити такі умови, що допоможуть знайти відповіді на ключові питання: чи відбувається кампанія? Хто стоїть за її організацією? Які її цілі та завдання?

У світлі вищевикладеного можемо узагальнити: когнітивна безпека є комплексним підходом до забезпечення стабільності індивідів і суспільства від впливів інформаційно-психологічного характеру. Зазначена концепція передбачає заходи та стратегії, спрямовані на захист когнітивних процесів, інтелектуальних зусиль і психологічного благополуччя в умовах росту впливу цифрових технологій та онлайн-середовища. Когнітивна безпека зосереджена на виявленні, аналізі й протидії загрозам, пов’язаним із маніпулюванням когнітивними процесами, такими як мислення, сприйняття, увага, ухвалення рішень. Її основною метою є забезпечення надійності та безпеки інтелектуальних систем, запобігання зловживанням та кримінальній діяльності, а також збереження довіри й прозорості у використанні штучного інтелекту, його впливу на суспільство. Особливо актуальним це є в контексті щораз більшого впливу технологій на наші пізнавальні процеси та спосіб сприйняття інформації [78, с. 280-281].

Відповідно, постає логічне питання щодо ефективних засобів протидії атакам, які здійснюються на суспільство в рамках гібридних воєн. Як зазначалося вище, гібридна війна – це міжнародна проблема, у зв’язку з чим першочергові заходи щодо її вирішення мають бути вжиті на відповідному рівні. Доречно буде

згадати, що в період після варшавського саміту у 2016 році НАТО наголосило на потребі забезпечення громадянської готовності, щоб підвищити рівень життєстійкості населення та державних інститутів у країнах-членах альянсу шляхом співробітництва між урядовими міністерствами та цивільними організаціями, приватним сектором і громадськістю. До прикладу, країни ЄС теж активно розробляють власні заходи. Так, Концепція національної оборони Естонії, ухвалена у 2017 р., разом із військовою готовністю охоплює також заходи психологічної, громадянської та економічної оборони. Стосовно локальних ініціатив, то тут слід зауважити, що універсальних інструментів, адаптованих під кожен воєнний кейс, не існує, проте можна виділити загальні рекомендації, які базуються на досвіді російсько-української війни. Першочергово – це освіта, яка передбачає набуття hard skills та soft skills цифрової грамотності; культура поведінки в Інтернет-середовищі; «активне» сприйняття інформації, яка перебуває у вільному доступі. Важливими є територіальні та загальнодержавні програми: 13 липня 2023 року у Київській міській раді ввели в дію мораторій на публічне використання російськомовного культурного продукту; за тим ініціативу перейняли у Львівській, Чернівецькій, Вінницькій, Запорізькій міськрадах; декілька останніх років успішно функціонує проєкт “Дія.Цифрова освіта” (реалізований Міністерством цифрової трансформації України); академічна протидія тощо.

Ми солідарні з думкою Г. Яворської, яка наголошує, що, коли не вистачає ресурсів для безумовної військової перемоги, яка до того ж обернеться величезною кількістю жертв, здобути перемогу в гібридній війні можна лише невиконанням набору політичних вимог агресора, незмінних протягом усього періоду війни. Таким чином, перемога України на когнітивному рівні полягатиме в тому, щоб унеможливити виконання вимог рф і продовжувати зберігати себе як самостійну державу [187, с. 47].

Отже, за результатами проведеного аналізу дійшли до висновку, що гібридна війна не змінює саму природу війни. Тиск залишається в центрі гібридної війни, як і в будь-якій іншій її формі; мета – попередньою, а саме

отримання психологічних чи фізичних переваг перед суперником. Гібридна війна характеризується складною динамікою конфлікту не лише тому, що вона пропонує широкий спектр інструментів для підриву супротивника, а й через можливість одночасного його ураження з різних напрямків (відображає загальну мету гібридної війни). На передовій використовуються слабкі сторони в політичній, військовій, економічній, соціальній та інфраструктурній сферах держави, яка стала об'єктом атаки, настільки, наскільки вони фізично й функціонально зазнали ослаблення. Інший фронт – інформаційний, головне завдання якого – поставити під сумнів легітимність чинної влади. Безперечно, для служб, відповідальних за національну безпеку, боротьба із широким колом загроз, які мають назву «гібридна війна», становить значну проблему. Водночас питання протидії потенційним і фактичним загрозам, а також забезпечення стану когнітивної безпеки – це індивідуальна справа і задача кожної свідомої людини. Перспективи подальших наукових пошуків вбачаємо в комплексному аналізі стратегій і тактик інформаційної війни.

2.3. Когнітивна війна як інструмент гібридного протистояння: виклики для когнітивної безпеки

У нинішніх реаліях гібридної агресії проти України когнітивна війна відіграє роль стратегічного інструменту дестабілізації, у межах якого агресор, зокрема росія, цілеспрямовано атакує не лише фізичну інфраструктуру, а й колективну свідомість нації, перетворюючи людський розум на стратегічне поле бою [232; 254; 251]. Така еволюція від традиційних до когнітивних доменів війни відображає суттєвий парадигмальний зсув: якщо фізичні атаки обмежені матеріальними втратами, то маніпуляція когнітивними процесами спричиняє глибоку ерозію соціальної когезії та національної ідентичності, створюючи умови для саморуйнівних реакцій суспільства без прямого військового втручання [254].

З іншого боку, когнітивна безпека тісно пов’язана з концепцією когнітивної війни (*cognitive warfare*), яка визначається як стратегія, спрямована на зміну способу мислення та відповідно поведінки цільової популяції, часто з метою дестабілізації суспільних інститутів та підриву довіри до влади.

На відміну від традиційної інформаційної, когнітивна війна робить акцент не на поширенні окремих фейків, а на системному впливі на свідомість через складні психологічні техніки маніпулювання, використання соціальних мереж та створення ехокамер, що ведуть до поляризації суспільства. НАТО визначає когнітивну війну як діяльність, що проводиться в поєднанні з іншими інструментами для впливу на ставлення та поведінку цільових аудиторій шляхом маніпуляції, захисту або погіршення індивідуального та групового судження з метою отримання переваги над противником. Ця концепція підкреслює культурні та емоційні виміри ухвалення рішень, вказуючи на те, що зосередження лише на дезінформації та фейкових новинах ігнорує широкий спектр стратегій, які можуть бути використані в інформаційному та медійному просторі.

Когнітивна війна, спрямована на підрив фундаментальних засад суспільства: колективної свідомості, довіри до інституцій та здатності до консолідованого спротиву, дедалі виразніше постає як системна загроза національній безпеці. На відміну від традиційної інформаційної війни, яка фокусується переважно на контролі потоків інформації, когнітивна націлена на вплив на когнітивні процеси: мислення, ухвалення рішень і поведінку як окремих індивідів, так і цілих соціальних груп. Її мета полягає не в переконанні, а в дезорієнтації, розколі та демобілізації через експлуатацію емоційних станів, когнітивних упереджень і підсвідомих реакцій.

З 2021 року Центр інновацій НАТО активно досліджує концепцію так званої «когнітивної війни», яка репрезентує новий підхід до ведення глобального конфлікту. Основна стратегічна мета цього типу війни полягає у впливі на процеси людського пізнання, мислення та формування поведінкових моделей. Очікувалося, що повноцінну презентацію концепції буде здійснена наприкінці

2024 року, це засвідчить переосмислення природи сучасних загроз і принципів ведення війни в умовах інформаційного суспільства [9, с. 12].

Згідно з експлоративною концепцією NATO Allied Command Transformation, когнітивна війна визначається як діяльність, що проводиться синхронізовано з іншими інструментами влади для впливу на ставлення та поведінку шляхом впливу, захисту або порушення індивідуального та групового пізнання з метою отримання переваги над супротивником [216]. У ширшому сенсі її можна розглядати як новий домен конфлікту, де людський розум стає полем бою [209; 210] поряд із традиційними середовищами (земля, море, повітря, космос) та кіберпростором. На відміну від поверхневих маніпуляцій інформаційними потоками, когнітивна війна здійснює глибоке втручання в механізми сприйняття, спрямоване на деградацію здатності пізнавати, інтерпретувати та чинити опір інформаційним впливам.

Якщо на екзистенційному рівні війна є збройним зіткненням значних людських угруповань, організованих у військо, то в когнітивному сенсі війна породжується неможливістю порозуміння через розрив у ланцюжках комунікації, зумовлений різними уявленнями про соціальний порядок і владні відносини. Відповідно, мир означає як припинення збройних зіткнень, так і відновлення комунікацій та встановлення порозуміння. Проте сучасні війни не визнають себе обмеженими міжнародним правом. Вони прагнуть до маскування під різного типу «військові операції» та відбуваються в специфічний спосіб війн гібридних або терористичних, які практично є поєднанням воєнних дій і таємних операцій.

Прагнення емоційно-психічної зверхності – одне з істотних виявів волі до влади, тобто встановлення відносин панування та підкорення. Воно є тим небезпечнішим, що більше за пропозицією діалогу та мирного обміну думками приховано прагнень встановити свій контроль над свідомістю та волею іншого, а через це – оволодіти його матеріальними й ментальними ресурсами, соціальним капіталом тощо.

У фокусі таких атак перебувають нейропсихологічні вразливості, зокрема активація центрів страху та тривоги, які пригнічують виконавчі функції мозку й порушують раціональне мислення, що створює когнітивно-емоційний конфлікт, у межах якого цільова аудиторія стає більш сприйнятливою до нав'язаних наративів [211]. На відміну від інформаційних кампаній, де когнітивна реакція є побічним наслідком, у когнітивній війні саме вплив на внутрішню обробку інформації виступає первинною ціллю [210].

Когнітивні операції інтегруються в широкий спектр гібридних дій, використовуючи комбінацію кібер-, інформаційних, психологічних та соціально-інженерних інструментів. Вони таргетують як лідерів думок, так і пересічних громадян через соціальні медіа, месенджери та цифрові екосистеми, що дозволяє досягати когнітивної переваги – домінування в знаннях, довірі та процесах ухвалення рішень.

З початку повномасштабного вторгнення у 2022 р. зафіксовано масштабні дезінформаційні кампанії, спрямовані на підрив довіри до державних інституцій та посилення внутрішніх розколів [232].

Погоджуємося з думкою Т. Бевз про те, що в контексті сучасної війни російська федерація застосовує не лише збройні засоби впливу, а й активно веде багатовимірну когнітивну війну, основною метою якої є маніпуляція свідомістю, підрив критичного мислення, поширення дезінформації та формування викривленої картини реальності. Такий підхід спрямований на деморалізацію українського суспільства, послаблення національної ідентичності та зменшення рівня його стійкості перед зовнішніми загрозами.

Когнітивна війна постає як новітня форма інформаційно-психологічного протистояння, головним завданням якої є вплив на переконання, поведінку та ідентичність населення без прямого застосування фізичного насильства. Цей тип впливу є одним із найбільш загрозливих складників гібридних війн, оскільки спрямований на встановлення контролю над мисленням, емоційним станом та процесом ухвалення рішень [9, с.13].

Таким чином, когнітивна війна постає як нетрадиційна форма збройного протистояння, що ґрунтується на використанні кіберінструментів і інформаційно-психологічних технологій з метою впливу на когнітивні процеси супротивника. Її завданням є не лише порушення раціонального мислення через експлуатацію ментальних упереджень і рефлексивних реакцій, а й викривлення сприйняття реальності, маніпуляція механізмами ухвалення рішень і гальмування ефективної поведінки. Наслідки таких впливів є критичними як на індивідуальному, так і на колективному рівнях, оскільки нівелюють довіру, солідарність, внутрішню стійкість та ідентичність спільноти.

Глибше розуміння сутності російсько-українського конфлікту в цьому контексті пропонує ізраїльський військовий експерт Ш. Шай, який розглядає сучасну агресію як інтенсивне застосування інформаційної та психологічної війни – компонентів ширшого явища когнітивного протистояння. За його словами, головна стратегічна мета когнітивної війни полягає у веденні наступу проти уявлень, цінностей і переконань ворожої спільноти через цілеспрямовану зміну її уявлення про дійсність [253].

Таким чином, сучасне понятійний апарат, що охоплює такі терміни, як «гібридна війна», «когнітивна війна», «інформаційна війна», «екзистенціальна загроза», насправді є різними проявами одного й того ж процесу – багаторівневого інформаційно-психологічного вторгнення, сконцентрованого на сфері свідомості. Особливо чітко це простежується в українському контексті, де людський розум і колективна уява стали повноцінним «полем бою».

У зв’язку з цим надзвичайно важливим є розуміння цілей, досягнення яких ставить собі за мету когнітивна агресія. Військові аналітики й дослідники вказують на такі ключові завдання когнітивної війни:

1. Руйнування суспільної свідомості через деструкцію наративної цілісності та колективної ідентичності.

2. Маніпуляція громадською думкою з метою дезорієнтації населення, викривлення уявлень про реальність, формування песимістичних або фаталістичних установок.

3. Підрив комунікаційних зв’язків на різних рівнях: між політичними лідерами, військовими структурами, родинами, державами-партнерами, зокрема представниками Європейського Союзу.

У межах сучасної когнітивної науки людина розглядається не лише як об’єкт інформаційного впливу, а як динамічний носій смислів і системи орієнтацій. Саме тому когнітивна війна – це передусім битва за структурування реальності в межах ментального простору індивідів і спільнот. В умовах російсько-українського протистояння така війна розгортається не лише на фізичних територіях, а й у сфері мислення, де вирішується питання: *хто і як має право визначати, що є правдою, цінністю та майбутнім* [32, с.76].

Когнітивна війна розглядається як концепція ведення впливових дій, спрямованих на трансформацію мислення, емоційної сфери, переконань і поведінки людини. Її сутність полягає в боротьбі за контроль над свідомістю, увагою, емоціями та уявленням про реальність. Ціль таких дій – проникнення в комунікаційне середовище противника з метою впливу на його сприйняття ситуації та процес ухвалення рішень як за допомогою сили, так і без її застосування.

Інструментарій когнітивної війни охоплює широкий спектр впливів – від поширення дезінформації й пропаганди до психологічних операцій та маніпуляцій у цифровому просторі, зокрема в соціальних мережах. Цей тип конфлікту вплетений у різноманітні сфери – від політичної пропаганди, медіапростору, мистецтва та культури до освітньої системи й наукових дискурсів.

Попри те, що когнітивна війна має риси, схожі з психологічною, вони відрізняються фокусом впливу, масштабами, методами реалізації та засобами. Когнітивна війна передбачає повний спектр ментальної діяльності людини, націлена на зміну способів осмислення інформації, формування переконань й ухвалення рішень. Для цього використовуються інформаційні технології, маніпулятивні стратегії, штучний інтелект і велика база даних для формування

викривленої, але переконливої картини дійсності. Вплив поширюється на знання, систему цінностей, культурні коди та ідентичність.

Натомість психологічна війна зосереджена переважно в емоційно-поведінковій сфері: вона спрямована на зниження морального стану, створення відчуття страху, паніки чи апатії. Такі операції реалізуються через методи психологічного тиску, залякування, поширення чуток, дезінформації та інші форми впливу на психоемоційний стан індивідуума або групи.

Когнітивна війна має глобальний масштаб, оскільки спрямована не лише на окремих осіб, а й на трансформацію свідомості цілих спільнот і суспільств через контроль над інформаційними потоками. Це дозволяє змінювати моделі поведінки та уявлення на рівні соціальних систем. У той час психологічна війна частіше орієнтується на конкретні цільові аудиторії: військових, політичну еліту чи визначені соціальні групи – з метою деморалізації або підвищення бойового духу.

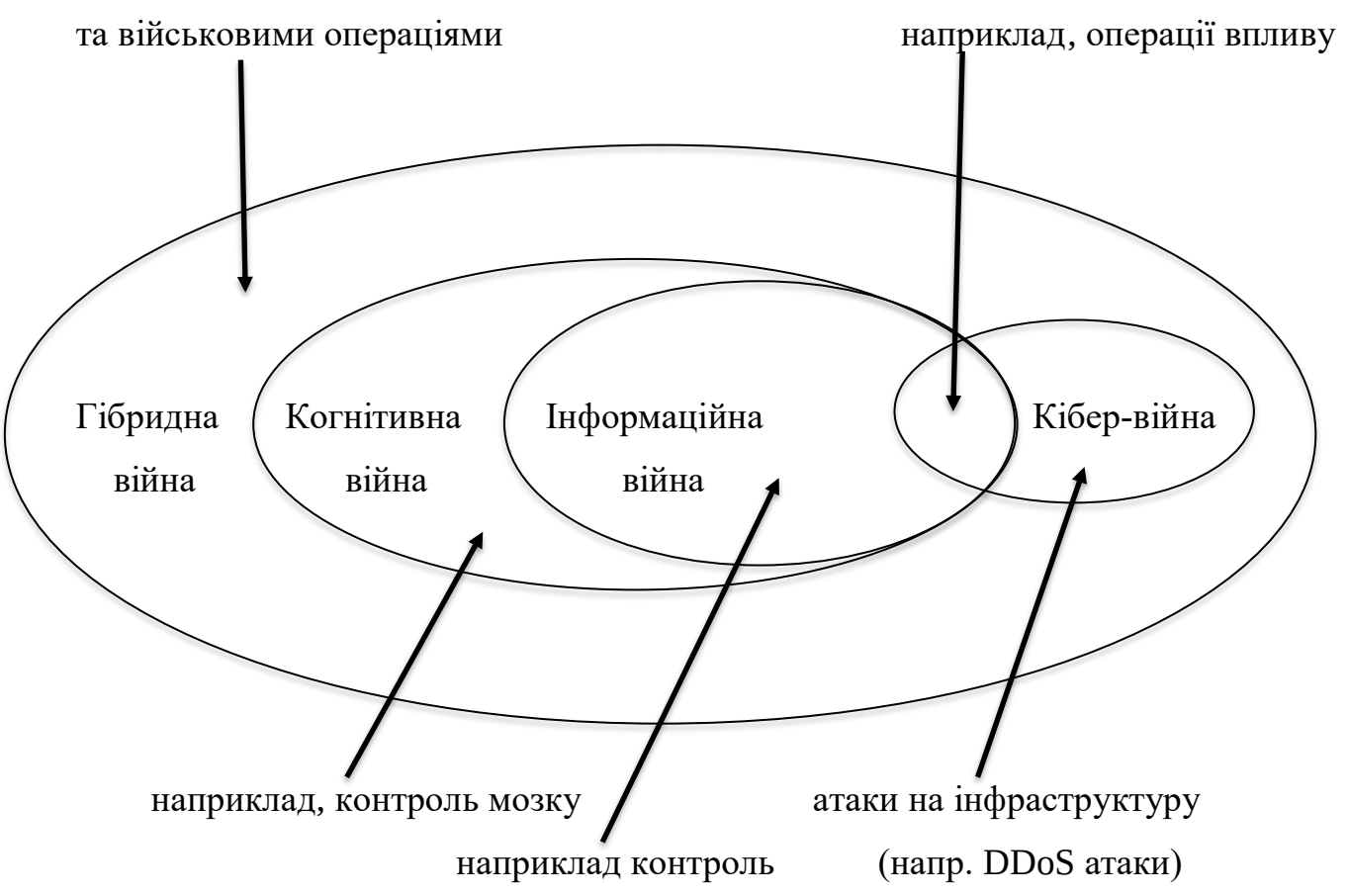
Когнітивні атаки зазвичай здійснюються із залученням цифрових технологій, соціальних мереж, штучного інтелекту, алгоритмів обробки даних, а також інструментів культурного, академічного й політичного впливу. Йдеться про контроль над інформаційними потоками в освіті, моделювання навчальних програм, які формують певний світогляд, і навіть академічні дослідження, які служать легітимації визначених наративів.

Зі свого боку,психологічна війна переважно ґрунтується на традиційних каналах: медіакампаніях, пропагандистських матеріалах, радіопередачах, листівках, прямих погрозах та інших формах емоційного тиску. Обидва види війни можуть застосовуватися окремо, але найчастіше поєднуються, створюючи ефект синергії – посилення впливу завдяки комбінованому застосуванню різних засобів.

Отже, ключова відмінність між когнітивною та психологічною війною полягає в широті впливу: когнітивна війна орієнтується на зміну мислення, світогляду та ментальних структур через інформаційні й цифрові засоби, тоді як

психологічна – фокусується на емоційному стані, мотивації та внутрішньому опорі людини.

Проблематику співвідношення понять «гібридна війна», «інформаційна війна», «психологічна війна», «когнітивна війна» та «кібероперації» подано / відображено на Рис. 2.1. Когнітивні операції в умовах збройного протистояння можуть набувати рис військових злочинів, зокрема, коли вони спрямовані на завдання шкоди або знищення противника шляхом впливу на його розум. Когнітивна війна багато в чому перегукується з так званими війнами впливу. І хоча всі згадані концепти (кібер-, інформаційна, когнітивна та гібридна війни) мають спільний елемент впливу на свідомість, саме когнітивна війна найбільш виразно спрямована на безпосередній контроль над ментальними процесами. Вона ґрунтується на здобутках нейронауки, зокрема нейрофізіології, нейропсихології та когнітивної нейронауки, які сьогодні активно залучаються як інструменти в стратегіях глобального протистояння [98, с.45].



медіа

Рис.2.1. Співвідношення та місце складників гібридної війни [98]

У цьому контексті російська пропагандистська машина активно використовує інструменти психологічного тиску, сучасні інформаційні технології та досягнення нейронаук для нав'язування фальшивих наративів. Такі дії спричиняють дестабілізацію внутрішнього соціального середовища, провокують зростання недовіри до державних інституцій, збройних сил та навіть до власної ідентичності громадян. Йдеться не лише про інформаційні атаки в традиційному сенсі, а про цілеспрямовану спробу змінити ментальні моделі, поведінкові реакції та загальний світогляд населення в довгостроковій перспективі.

Активне використання штучного інтелекту для генерації контенту дозволяє не лише прискорювати поширення фейків, а й адаптувати їх до індивідуальних психологічних профілів, посилюючи когнітивну втомленість населення [214]. Масові міграції (понад 5,7 млн біженців станом на серпень 2025 року), енергетичні блекаути та фрагментація інформаційного простору створюють сприятливі умови для поширення маніпулятивних повідомлень і формування паралельних реальностей, що руйнують спільне сприйняття загрози [255].

Вразливість до когнітивних атак має багатовимірну природу. По-перше, вона базується на нейропсихологічних механізмах: експлуатація когнітивних упереджень, активація центрів страху та провокування емоційних реакцій призводять до когнітивно-емоційного конфлікту, який значно знижує стійкість до маніпулятивних повідомлень [213]. По-друге, сучасні технологічні каталізатори підсилюють цю вразливість. Фрагментація інформаційного простору, спричинена переміщенням великих груп населення, розриває соціальні зв'язки та створює множину ізольованих середовищ, де дезінформація поширюється без ефективних механізмів корекції [271]. Енергетичні блекаути, викликані ударами по критичній інфраструктурі, спричиняють інформаційний

вакуум, у якому емоційно заряджені фейки поширюються швидше за перевірену інформацію. Алгоритмічна персоналізація контенту в цифрових екосистемах формує замкнені «ехокамери», які підсилюють поляризацію та знижують здатність суспільства до спільної реакції на загрози [254].

Застосування маніпулятивних наративів, психологічних операцій та технологічного підсилення створює синергетичний ефект, що ускладнює оборону. Агресор системно використовує стратегію рефлексивного контролю, спрямовану на порушення циклу OODA (спостереження – орієнтація – рішення – дія), маніпулюючи сприйняттям та спонукаючи до хибних або деструктивних рішень. Такий підхід дозволяє досягати стратегічних цілей – підривати довіру до державних інституцій, послаблювати ідентичність та деморалізувати населення – без масштабних військових дій [223]. У європейському вимірі подібні інструменти використовуються для дестабілізації транскордонної безпеки, створюючи когнітивні пастки, що провокують неадекватну оцінку ризиків і реакцій.

Відповіддю на ці загрози стає формування системи когнітивної безпеки, яка поєднує суспільні, технологічні та регуляторні механізми. Її ключове завдання полягає в перетворенні суспільства з пасивного об’єкта впливу на активного суб’єкта опору. Освітні програми з медіаграмотності та критичного мислення, а також розвиток незалежних фактчекінгових ініціатив (StopFake, Prometheus) створюють базовий захисний шар [212]. Технологічні інструменти: аналітика великих даних, автоматизовані системи виявлення координованих кампаній та боротьба з діпфейками – забезпечують своєчасне виявлення та блокування загроз [222]. Регуляторний вимір, гармонізація з нормами GDPR та AI Act, створює правове поле, яке обмежує можливості агресора для маніпуляції.

У воєнних умовах ця система доповнюється децентралізацією інформаційної інфраструктури (зокрема через використання Starlink та локальних серверів), забезпеченням офлайн-доступу до комунікації (радіо, SMS) та адаптацією рішень до регіональних умов. Така архітектура дає змогу не лише

знижувати рівень дезінформаційного впливу, а й підтримувати колективну стійкість у кризових сценаріях (Табл. 2.2).

Таблиця 2.2

Вектори загроз когнітивної війни та відповідні стратегії когнітивної безпеки

Інструмент когнітивної війни	Характеристика загрози	Відповідна стратегія когнітивної безпеки	Очікуваний ефект	Потенційні ризики реалізації
Маніпулятивні наративи	Створення альтернативної реальності, швидке поширення через цифрові платформи	Медіаграмотність, фактчекінг	Зниження рівня віри у фейки, зміцнення ідентичності	Низький рівень цифрових навичок у частини населення
Психологічні операції (PSYOP)	Емоційний вплив, когнітивно-емоційний конфлікт	Психологічна стійкість, освітні програми	Зростання опірності до маніпуляцій	Обмежені ресурси для реалізації програм підтримки
AI-посилені дипфейки та бот-мережі	Персоналізовані атаки, стирання межі між фактом і вигадкою	Аналітика Big Data, AI-детекція	Раннє виявлення атак, автоматизація реагування	Алгоритмічна упередженість, технічні вразливості
Кібератаки та інформаційний вакуум	Фрагментація сприйняття, посилення поляризації в кризових умовах	Децентралізація комунікаційних мереж, офлайн-доступ	Збереження зв’язку, підвищення стійкості у критичних сценаріях	Регіональна нерівність доступу, ризики ескалації гібридних атак

Таблиця створена автором на основі аналізу джерел представлених у списку літератури дисертаційного дослідження [224], [222], [220],[218].

Когнітивна війна являє собою цілеспрямований вплив на людську свідомість, систему переконань та ціннісні орієнтири. Основною метою агресора є руйнування української ідентичності, провокування внутрішньої нестабільності та розколу в суспільстві. Водночас міцне національне самоусвідомлення виступає надійним щитом у протидії таким атакам. Освіта, історична спадщина, мова, культура й інформаційна стійкість є ключовими стратегічними ресурсами в цій боротьбі [9, с. 12].

Українська ідентичність здатна перетворитися на ефективний інструмент опору когнітивному вторгненню завдяки таким факторам:

1. Освіта та медіаграмотність. Люди, які володіють навичками критичного мислення, менш схильні до впливу маніпуляцій та фейкових повідомлень. Саме тому надзвичайно важливо навчати учнів і студентів аналізувати інформацію, перевіряти достовірність джерел і виявляти дезінформацію.

2. Стійка історична пам’ять. Глибоке знання власної історії слугує бар’єром проти її спотворення та нав’язування фальшивих інтерпретацій. Історичні фейки – один із найбільш дієвих інструментів когнітивного впливу, здатний підривати національну свідомість.

3. Українська мова як засіб захисту. Дослідницькі дані свідчать, що ті, хто споживає інформацію українською мовою, менше потрапляють під вплив російської пропаганди. Підтримка й розвиток контенту українською мовою, включно з кінематографом, медіа, блогосферою та літературою, є важливим чинником інформаційної безпеки.

4. Створення позитивних наративів на основі усвідомлення національної ідентичності. Важливо не лише викривати фейки, а й формувати власні сильні смислові рамки. Україна має позиціонувати себе не лише як держава, що чинить опір, а як самобутня, сильна країна з вагомими культурними, науковими та військовими досягненнями.

Таким чином, когнітивна війна є не лише різновидом інформаційного протистояння, а самостійним доменом сучасних конфліктів, у якому вирішальним чинником стає контроль над сприйняттям та поведінкою.

Ефективність такої війни ґрунтується на поєднанні психологічних, соціальних і технологічних чинників, що забезпечують її довготривалий вплив. У відповідь на це когнітивна безпека постає як стратегічний інструмент національної та європейської безпеки, що поєднує превентивні освітні та технологічні заходи з адаптивним правовим регулюванням. Такий підхід забезпечує можливість не лише зменшувати наслідки атак, а й формувати проактивну архітектуру резилієнтності, у якій суспільство виступає активним суб'єктом опору, а не пасивною мішенню.

Когнітивна безпека перестає бути суто теоретичним поняттям і дедалі частіше виступає практичним інструментом забезпечення стійкості суспільства до зовнішніх і внутрішніх маніпулятивних впливів. В умовах сучасної війни, де активна боротьба ведеться не лише за території, а й за свідомість громадян, важливою стає здатність до збереження цілісності когнітивного простору як у фізичному (інформаційному), так і в ментальному вимірах.

Аналіз сучасних загроз засвідчив, що традиційні підходи до інформаційної безпеки є недостатніми для пояснення і нейтралізації новітніх форм впливу. У цьому контексті запропоновано розширене трактування загроз когнітивній безпеці як системи впливів на мислення, сприйняття, цінності, поведінкові установки, що можуть спричинити стратегічно значущі зміни у функціонуванні суспільства. Класифікація таких загроз охоплює не лише зовнішні (екзогенні) й внутрішні (ендогенні) виклики, але й зважає на ступінь реальності загроз, рівень гіпотетичної шкоди, характер походження (антропогенні, техногенні, стихійні), ймовірність реалізації, а також рівень структурної детермінованості.

У такому ключі важливо простежувати чітку залежність між інтенсифікацією когнітивних атак і розвитком новітніх технологій, зокрема штучного інтелекту, алгоритмів машинного навчання та цифрових платформ із персоналізованою видачею контенту. Такі загрози створюють принципово нові виклики для безпеки особистості та суспільства, оскільки виходять за межі контролю традиційних регуляторів і вимагають міждисциплінарної взаємодії – між урядом, ІТ-сферою, науковцями й громадянським суспільством.

Гібридна війна виступає багатовимірною стратегією, яка поєднує як військові, так і немілітарні (політичні, економічні, інформаційні, психологічні) методи впливу. Особливістю сучасного етапу гібридної агресії проти України є домінування когнітивного виміру – сфери мислення, емоцій, переконань та поведінкових моделей. За таких умов на перший план виходять не танки й ракети, а наративи, фейки, бот-мережі та психоемоційний тиск. Це визначає принципово нові орієнтири в розумінні безпеки не лише фізичної, а й ментальної.

Гібридна війна функціонує як у матеріальному, так і в дискурсивному вимірах. Фізична агресія супроводжується нав'язуванням альтернативної реальності, запереченням об'єктивних фактів і викривленням історії. Через це держава-агресор намагається посіяти сумніви в легітимності національної влади, спровокувати втрату довіри до інституцій, розколоти суспільство зсередини. Аналіз конкретних прикладів стратегічної пропаганди, психологічних операцій, кібератак демонструє ефективність скоординованих впливів на різні компоненти когнітивного простору.

На відміну від інформаційної чи психологічної війни, когнітивна війна охоплює повний спектр пізнавальної діяльності людини, спрямовуючи атаки безпосередньо на процеси сприйняття, інтерпретації та ухвалення рішень. Уперше на рівні НАТО когнітивна війна була визначена як цілеспрямована стратегія впливу на «сіру речовину», тобто на людську здатність аналізувати, робити висновки та зберігати критичне мислення.

Сутність когнітивної війни виявляється через широкий арсенал інструментів – від цифрових платформ і бот-мереж до впливу на освітні програми, культурні продукти й академічну науку. Системність таких атак дозволяє агресору поступово переформатовувати світогляд населення, підміняти цінності, знижувати рівень резистентності суспільства до зовнішніх загроз. Особливо вразливими є ділянки, де поєднуються соціальні слабкості (низький рівень освіти, довіра до держави, фрагментованість медіаполя) з технологічними можливостями для впровадження деструктивного контенту.

Наголосимо, що вразливість когнітивної безпеки посилюється під впливом таких чинників, як:

– низький рівень медіаграмотності,

– алгоритмічна ізоляція («інформаційні бульбашки»),

– когнітивна втома,

– розрив соціальних зв’язків,

– фрагментація комунікаційної інфраструктури в умовах війни.

Ефективна протидія когнітивній агресії можлива лише за умови формування стійкої системи когнітивної безпеки. Ця система має бути побудована на трьох ключових елементах:

– освітньому – впровадження програм критичного мислення, медіаграмотності, фактчекінгу,

– технологічному – створення інструментів раннього виявлення фейків, дипфейків, алгоритмічних атак,

– регуляторному – правове врегулювання інформаційного простору з огляду на етичні та гуманітарні засади.

У цьому контексті надзвичайно важливою є роль української національної ідентичності як «вакцини» проти когнітивної війни. Саме усвідомлення своєї історії, мови, культури, цінностей формує фундамент стійкості, який не можуть зруйнувати навіть найскладніші інформаційні впливи.

Український досвід протистояння когнітивній агресії є унікальним у світовому масштабі та заслуговує на глибоке осмислення як у теоретичному, так і прикладному вимірах, оскільки демонструє приклад стійкості нації в умовах комплексної гібридної війни.

РОЗДІЛ 3 ІНФОРМАЦІЙНІ СПЕЦІАЛЬНІ ОПЕРАЦІЇ ТА ТЕХНОЛОГІЇ КОГНІТИВНОГО ВПЛИВУ В УМОВАХ ВОЄННОГО СТАНУ

3.1. Когнітивний аспект використання технологій інформаційних операцій в політичній практиці

Інформаційна індустрія в умовах сучасного глобалізованого світу посідає провідне місце серед стратегічно важливих сфер діяльності, у які щорічно спрямовується дедалі більше фінансових, технологічних та інтелектуальних ресурсів. Нестача актуальної, достовірної та оперативної інформації може призводити до значних втрат у різних сферах суспільного функціонування – від політики та економіки до національної безпеки. У цьому контексті особливого значення набуває феномен інформаційних операцій, які охоплюють як легальні інструменти впливу, так і приховані (тіньові) механізми маніпуляції, розуміння яких є необхідним для мінімізації ризиків та запобігання негативним наслідкам для індивідів, організацій і держав.

Поняття «інформаційні операції» сформувалося на початку XXI століття через стрімку інформатизацію та посилення процесів глобалізації. Цей концепт відкриває нові аналітичні перспективи для дослідження сутності так званих інформаційних війн, які трактуються як цілеспрямовані дії, спроєктовані на досягнення інформаційної переваги шляхом деструкції інформаційних процесів противника та водночас захисту власних інформаційних ресурсів і комунікаційних систем. На практиці інформаційні операції реалізуються в найрізноманітніших формах – від рекламних кампаній і політичного маркетингу

до масштабних стратегічних впливів під час виборчих процесів чи гібридних атак економічного та інформаційного характеру.

Останні роки характеризуються суттєвим зростанням випадків використання інформаційно-комунікаційних технологій (далі – ІКТ) та глобального інформаційного середовища з метою поширення спеціально підготовленого контенту, що слугує інструментом впливу в політичних або економічних цілях, які нерідко мають неправомірний або деструктивний характер. У процесі глобалізації інформація остаточно перетворилася на стратегічний ресурс, володіння та контроль над яким стали критично важливими чинниками політичної влади та геополітичного домінування.

Центральною платформою для здійснення політичного впливу на свідомість сьогодні виступає інтернет-простір, зокрема соціальні мережі, які забезпечують оперативне розповсюдження інформації з можливістю охоплення великої та різнорідної аудиторії. Технології ШІ, зокрема, алгоритми обробки великих даних, дозволяють створювати високоточні персоналізовані повідомлення, що беруть до уваги індивідуальні характеристики, інтереси та поведінкові патерни користувачів. Така індивідуалізація інформаційного впливу підвищує ефективність комунікацій, але водночас створює підґрунтя для поширення дезінформації, маніпуляцій та фейкових повідомлень, які можуть суттєво впливати на політичні процеси та громадську думку.

На сучасному етапі розвитку політичної комунікації інформаційні операції стали інструментом системного впливу, невід’ємним складником виборчих кампаній і політичних дебатів. Такі операції можуть бути спрямовані на дискредитацію політичних опонентів, поглиблення соціальної поляризації, створення ілюзії широкої підтримки певних рішень, а також на впровадження вигідних суб’єктам впливу наративів [111, с. 23]. У виборчий період значного поширення набули технології таргетованої політичної реклами, які дозволяють адресно впливати на окремі електоральні групи, формуючи в них необхідні політичні преференції. Водночас інформаційні операції дедалі частіше застосовуються як інструмент антикризового управління, коли політичні актори

намагаються скоригувати або трансформувати громадську думку у відповідь на виклики соціально-політичного характеру [134]. У таких ситуаціях стратегічне використання соціальних мереж, оперативне реагування та контроль над медійним простором дозволяють формувати нові наративи та трансформувати суспільні настрої.

Інтернет-епоха змінила традиційні уявлення про комунікаційні процеси: багато концептів стали мобільними, гнучкими, взаємозалежними з іншими дисциплінарними підходами. Не став винятком і феномен інформаційної війни, у рамках якої останні два десятиліття віртуальна компонента конфлікту нерідко переважає реальну як за масштабом дій, так і за їхніми наслідками. У цій сфері накопичено значний емпіричний матеріал, що потребує поглибленого аналізу, систематизації та уніфікації термінологічного апарату.

Сучасні політичні інформаційні операції суттєво відрізняються від класичних інформаційних кампаній, які раніше ґрунтувалися на публічному піарі, медіаефектах і відкритій агітації. Натомість вони все більше наближаються до форм оперативної діяльності, у якій використовуються інструменти агентурної, оперативно-технічної та розвідувальної роботи. Як правило, за реалізацією таких операцій стоять спеціалізовані структури, пов’язані з державними розвідувальними службами, що засвідчує високий рівень організації та стратегічного задуму таких впливів.

Об’єкти, на які спрямовується вплив у межах сучасних інформаційних операцій, охоплюють широкий спектр елементів як державного, так і суспільного функціонування. До них належать:

- органи публічної влади та підрозділи збройних сил держави;
- системи управління цивільною інфраструктурою, зокрема телекомунікаційні, транспортні, енергетичні, фінансові та промислові сектори, а також засоби масової інформації;
- інформаційно-керівні компоненти військової інфраструктури: системи зв’язку, розвідки, бойового управління, логістики та управління озброєнням;

- канали та лінії зв’язку, що забезпечують передавання даних;
- інформаційні ресурси, які обробляються, циркулюють або зберігаються в системах управління;
- суспільство загалом – як цивільне населення, так і військовослужбовці, а також державні, економічні та соціальні інституції;
- масмедіа, особливо електронні;
- суб’єкти ухвалення рішень: керівний склад та персонал автоматизованих систем управління [186, с. 151-156].

Під час миротворчих місій перелік потенційних об’єктів впливу розширюється та охоплює воєнізовані та політичні організації, партизанські формування, релігійні спільноти, соціальні групи та окремих осіб, які відкрито або приховано чинять опір присутності збройних сил чи їхніх союзників, ускладнюючи виконання поставлених миротворчих завдань.

Інформаційні операції, по суті, передбачають застосування інформаційних ресурсів та технологій з метою впливу на військові або цивільні системи задля досягнення переваги в інформаційному просторі. Науковці пропонують низку подібних визначень цього явища. Наприклад, інформаційна операція розглядається як комплекс взаємопов’язаних у просторі, часі й меті дій, спрямованих на ініціювання і контроль процесів інформаційного впливу. Її метою є отримання й утримання інформаційної переваги шляхом впливу на інформаційні потоки та процеси в системах противника [20; 85, с. 26; 118, с. 98].

Сучасні інформаційні операції відзначаються високим ступенем технологічної організації, формалізованими методиками реалізації та попереднім моделюванням реакцій цільових аудиторій, що значно підвищує ефективність досягнення поставлених цілей.

Інформаційна операція являє собою структурований процес, що складається з низки взаємопов’язаних інформаційних атак, об’єднаних єдиним стратегічним задумом. Ці атаки координуються за цілями, завданнями, об’єктами, а також формами й методами реалізації інформаційного впливу [71, с. 72]. Ключовим

інструментом такої операції є інформаційне «вкидання» – блок заздалегідь підготовленої інформації, який запускається в публічне інформаційне поле в специфічних політико-безпекових умовах. Його метою є спровокувати об’єкт на миттєву реакцію, спричинену зовнішнім стимулом. Таким чином, інформаційна атака стає частиною більш масштабного процесу формування певної поведінкової моделі, вигідної ініціаторам операції, через вплив як на свідомий, так і на підсвідомий рівень сприйняття.

Використання інформаційних операцій у політичній сфері має глибокі суспільно-політичні наслідки. Зокрема, воно сприяє підриву довіри до традиційних медіа та політичних інституцій, адже масове поширення фейкових повідомлень, маніпуляцій і спотвореної інформації ускладнює розрізнення достовірного контенту. Крім того, подібна діяльність загострює політичну поляризацію, посилюючи розкол у суспільстві та ускладнюючи досягнення компромісу в публічному дискурсі.

Кожна інформаційна атака супроводжується фазою експозиції – періодом «інформаційної тиші», під час якого здійснюється спостереження за реакціями об’єкта впливу. Не менш важливим складником інформаційної операції є психологічний компонент. На підготовчому етапі створюється психологічний портрет цільової аудиторії або окремих осіб, визначаються мотиваційні фактори їхньої поведінки та прогнозуються реакції на інформаційний тиск. На основі цих даних здійснюється контрольований інформаційно-психологічний вплив із можливістю корекції сценарію в режимі реального часу.

Таким чином, поняття «інформаційна операція» та «психологічна операція», хоч і мають різну фокусну спрямованість, однак, фактично є двома аспектами єдиного процесу когнітивного впливу. У першому випадку йдеться передусім про технологічні, комунікаційні й стратегічні параметри, у другому – про цілеспрямований вплив на психоемоційний стан об’єкта та його поведінкові реакції. У своїй сукупності ці компоненти формують основу сучасної інформаційної війни – автономного напряму оперативного забезпечення,

покликаного реалізувати концепцію політичної переваги на інформаційному полі бою.

Інформаційна зброя становить засіб цілеспрямованого впливу на інформаційні ресурси супротивника, а також на його здатність функціонувати в інформаційному середовищі. У межах цього впливу відбувається не лише спотворення або руйнування ворожих інформаційних потоків, а й паралельний захист власної інформаційної інфраструктури. Такий підхід дозволяє обмежити спроможність противника до ефективного ведення бойових або політичних дій, знижуючи його волю до опору та стратегічні можливості [88].

Отже, інформаційна війна в сучасному розумінні постає як сукупність дій, що передбачають використання, модифікацію, знищення чи дезорганізацію інформації противника, а також захист і підтримку функціонування власної інформаційної системи. Зазначене визначення є основою для низки характеристик феномена інформаційної війни:

– інформаційна війна – це скоординоване та комплексне використання засобів інформаційного й збройного впливу задля досягнення стратегічних цілей;

– інформаційна війна розглядається як технологічний комунікативний процес, спрямований на завоювання інформаційної переваги шляхом впливу на інформацію та інформаційні системи противника за одночасного забезпечення кіберзахисту власних структур;

–у концептуальному сенсі інформаційна війна не є самодостатньою метою, а виступає інструментом реалізації політичних або військових стратегій. Вона може слугувати засобом для здійснення масштабної наступальної операції або, навпаки, інструментом інформаційної оборони [41].

Таким чином, інформаційна війна є невід’ємним складником сучасної гібридної конфліктності, що дозволяє досягати значних результатів без застосування фізичної сили шляхом впливу на інформацію як стратегічний ресурс.

Уперше термін «інформаційна війна» був уведений в науковий обіг американським аналітиком Т. Роною, який у 1976 році підготував для компанії Boeing звіт під назвою «Системи зброї та інформаційна війна». У цьому документі дослідник зазначив, що інформаційна інфраструктура становить критично важливий елемент національної економіки США, проте водночас вона є вразливою мішенню як у мирний, так і у воєнний період [7, с. 159]. Звіт Т. Рони став поштовхом до активного медійного обговорення цієї проблематики, що викликало жвавий інтерес у військових колах, особливо з огляду на потенційне стратегічне застосування інформаційних технологій у сфері безпеки. З 1980-х років концепт інформаційної війни набуває дедалі більшої актуальності у Воєнно-повітряних силах США.

Важливу роль у розвитку цієї ідеї відіграв Р. Банкер**,** експерт Пентагону, який у 1996 році на науковому симпозіумі представив нову військову доктрину XXI століття, відому як Force XXI. Її ключовим елементом став поділ театру воєнних дій на два основні виміри – традиційний фізичний простір та кіберпростір**,** причому останній визнавався навіть як більш стратегічно важливий. У межах цієї доктрини була запропонована концепція «кіберманевру» – нової форми оперативної дії, що доповнює класичні військові стратегії з нейтралізації противника [174, с. 135].

З огляду на трансформації у воєнній сфері, інформаційна сфера (інфосфера) офіційно внесена до переліку стратегічних середовищ бойових дій нарівні із сушею, морем, повітрям і космосом. Як зазначають військові аналітики, об’єктами впливу у війнах нового покоління стають не лише інфраструктурні елементи, а й психологічний стан противника, що відображено в терміні *«human network»*.

Серед основних форм сучасної технічної інформаційної війни можна виділити:

- радіоелектронну боротьбу,
- дії із застосуванням засобів електронної розвідки,
- точкові авіаційні удари,

- кібероперації,
- боротьбу з хакерськими атаками,
- а також психотропну війну.

Суттєвою характеристикою інформаційної війни є її інтегрований, скоординований характер: вона ніколи не здійснюється ізольовано, а є частиною широкомасштабної стратегії, у якій інформація використовується як зброя як на полі бою, так і в політичній, економічній чи соціальній площині. Яким би не було трактування цього терміну, його походження пов'язане з військовою доктриною, що підкреслює жорсткий, конфліктогенний і стратегічно значимий характер.

Фахівці у сфері військової стратегії, які займаються розробкою доктрини інформаційної війни, окреслюють її як багатовимірний феномен, що включає штабну**,** електронну**,** психотропну**,** інформаційно-психологічну та кібернетичну форми протистояння. Такий розподіл дозволяє виокремити низку характерних рис сучасних інформаційних операцій, які істотно відрізняють їх від традиційних форм збройного конфлікту:

- відносно низькі витрати на розробку та застосування засобів інформаційного впливу, що робить ці операції фінансово доступними;
- втрата значення державних кордонів як бар'єрів для поширення інформаційного впливу з огляду на глобальну природу цифрових комунікацій;
- посилення значення маніпулювання сприйняттям, зокрема через зміну контексту та інтерпретацій інформації;
- трансформація стратегічної розвідки**,** орієнтація якої зміщується в бік забезпечення інформаційної переваги над противником;
- складність у виявленні моменту початку інформаційної операції**,** оскільки вони можуть бути масковані під звичайну комунікаційну діяльність;
- труднощі в консолідації міжнародної відповіді на агресивні інформаційні дії через розмитість юридичних меж інформаційного простору.

Залежно від масштабів впливу та рівня управлінської інфраструктури, інформаційні операції умовно поділяють на операції державного та військового рівнів.

На державному рівні інформаційні операції мають за мету підрив авторитету та стабільності країн-суперників, дестабілізацію національних інституцій, ослаблення механізмів державного управління шляхом інформаційного впливу на політичну, економічну, дипломатичну та соціальну сфери. Такі дії можуть включати як пропагандистські кампанії, інформаційно-психологічні операції, так й інші форми деморалізаційного впливу.

Водночас інформаційні операції можуть використовуватись і для захисту національних інтересів, запобігання міжнародним конфліктам або локалізації їх, протидії терористичним чи провокаційним діям, а також гарантування безпеки національних інформаційних ресурсів.

На військовому рівні інформаційні операції виступають як інтегрований комплекс заходів, що реалізуються в межах збройних сил держави, її видів, родів військ та об'єднаних командувань у відповідних операційних зонах. Ці заходи є невід'ємним елементом військових кампаній і операцій стратегічного масштабу. Основною метою таких операцій є досягнення інформаційної переваги над супротивником, зокрема, у сфері систем управління військами, а також забезпечення захисту власних інформаційних інфраструктур. Для реалізації цієї мети залучаються всі наявні в розпорядженні військові та технічні ресурси, включно з засобами кібернетичної, радіоелектронної та психологічної боротьби. Важливо підкреслити, що застосування цих інструментів має здійснюватися з формальним дотриманням міжнародних правових, політичних, дипломатичних, моральних та військових норм [85, с. 24-27].

Залежно від рівня військового управління та масштабу впливу, інформаційні операції на військовому рівні поділяються на стратегічні, оперативні та тактичні:

- Стратегічні інформаційні операції ініціюються рішенням військово-політичного керівництва держави. Їхня мета полягає в здійсненні впливу на

ключові елементи державного устрою потенційного противника – політичні, військові, економічні та інформаційні структури – з одночасним забезпеченням захисту власних. Такі операції спрямовані на досягнення національних стратегічних цілей**.**

- Оперативні інформаційні операції проводяться для забезпечення ефективного ведення військових кампаній або окремих операцій. Вони передбачають вплив на системи зв'язку, логістики та бойового управління противника, паралельно із захистом аналогічних власних систем, зокрема союзних.

- Тактичні інформаційні операції мають локальний характер і спрямовані на досягнення конкретних тактичних цілей**.** Їхній фокус – вплив на інформаційні системи супротивника, безпосередньо задіяні в забезпеченні бойових дій (зв'язок, розвідка, управління військами), із паралельним захистом відповідних елементів власних військових підрозділів.

Особливої уваги заслуговує той факт, що вперше в сучасній військовій практиці інформаційні операції набули превентивного характеру. Вони розпочинаються ще в загрозливий період**,** тобто до початку активної фази бойових дій. Їхнє основне завдання – спрямувати процеси ухвалення рішень противником у вигідному для себе напрямі**,** впливаючи на його комунікацію, командування та загальну інформаційну обстановку.

У політичній практиці існує чимало прикладів як ефективного, так і неуспішного використання інформаційних операцій. Одним із найбільш резонансних та широко обговорюваних випадків є російська дезінформаційна кампанія під час президентських виборів у США 2016 року, яка отримала значний міжнародний розголос.

За результатами численних журналістських та урядових розслідувань встановлено, що російська федерація здійснювала цілеспрямовані спроби вплинути на хід виборчої кампанії з метою посилити шанси Д. Трампа на перемогу та послабити позиції його суперниці Г. Клінтон. Одним із основних інструментів впливу стала активність фейкових акаунтів у соціальних мережах,

які координувались так званим «Агентством інтернет-досліджень» (IRA), що діяло з території Санкт-Петербурга [193;199].

Ці акаунти поширювали контент, спрямований на поляризацію американського суспільства за критичними і чутливими темами, зокрема щодо міграційної політики, расових відносин, релігії та права на володіння зброєю. Таким чином, намагалися штучно посилити соціальну напругу, впливаючи на громадську думку та підриваючи внутрішню стабільність.

Крім того, фіксувалися кібератаки з боку російських спецслужб на сервери Демократичної партії США. Унаслідок зламу було отримано доступ до внутрішньої переписки виборчого штабу Г. Клінтон, яка згодом частково була оприлюднена задля її дискредитації. Додатково для інформаційного супроводу атак використовувалися проросійські медіа, спеціалізовані вебресурси, а також маніпулятивні наративи, що підривали довіру до кандидатки.

Попри складність оцінки прямого впливу цих заходів на результати виборів, інформаційна операція істотно посилила політичну поляризацію в американському суспільстві. Вона також стала каталізатором широкої суспільної дискусії щодо безпеки виборчих процесів, регулювання соціальних мереж і протидії дезінформації в цифрову епоху.

Ще одним показовим прикладом масштабного використання інформаційних операцій у політичному контексті став референдум щодо виходу Великої Британії з Європейського Союзу у 2016 році (так званий Brexit). Кампанія на підтримку виходу Великої Британії з ЄС супроводжувалася численними маніпуляціями, що ґрунтувалися на експлуатації соціальних страхів, передусім щодо імміграції, втрати суверенітету та економічної стабільності.

Одним із найвідоміших прикладів поширення дезінформації стало твердження, ніби Велика Британія щотижня переказує до бюджету ЄС 350 млн фунтів стерлінгів – ця неправдива цифра стала центральним меседжем кампанії Leave, попри спростування з боку незалежних джерел. Значну роль у поширенні маніпулятивного контенту відіграла компанія Cambridge Analytica, яка, використовуючи технології мікротаргетингу, поширювала рекламні матеріали в

соціальних мережах, зокрема Facebook, орієнтуючись на вразливі соціальні групи виборців. Контент був спеціально адаптований до потреб і страхів конкретних аудиторій – від питань імміграції до тематики національної безпеки. Крім того, фіксувалися підозри щодо російського впливу на хід кампанії, зокрема через дезінформаційні ресурси та непряме фінансування політичних груп, які виступали за вихід країни з ЄС.

У підсумку, 51,9% виборців підтримали Brexit, а сама кампанія стала прикладом того, як цілеспрямовані інформаційні впливи можуть сприяти радикалізації суспільства, посиленню політичної поляризації та формуванню стійких суспільних розломів [218].

Варто зазначити, що інформаційні технології у сфері політичного впливу постійно розвиваються. Удосконалюються методи таргетингу, аналізу користувацьких даних, генерації контенту, а також механізми поширення меседжів через лідерів громадської думки. Значну роль у цих процесах починають відігравати технології ШІ.

Зокрема, ШІ здатен автоматизовано створювати тексти, візуальний контент, виявляти соціальні зв’язки, аналізувати поведінку користувачів у мережі та визначати лідерів думок, навколо яких формуються цільові спільноти. Ці ж інструменти можуть ефективно застосовуватись як для моніторингу та запобігання деструктивним інформаційним атакам, так і в агресивних цілях – для посилення інформаційного впливу, створення фейкових новин чи провокацій.

Сьогодні одним із пріоритетних напрямів досліджень є розробка ШІ-систем для виявлення маніпулятивного контенту та ідентифікації загроз, що походять від інформаційних впливів екстремістського та терористичного характеру. В основі цих підходів лежать систематичний моніторинг мережевого середовища, аналіз поведінкових моделей та виявлення координаційних центрів інформаційного впливу.

3.2. Інформаційні спеціальні операції: особливості впливу на свідомість в сучасних умовах

Сьогодні важливим для кожної держави стає забезпечення інформаційної незалежності та когнітивної безпеки, зумовлене стрімким зростанням впливу інформаційних технологій і медіа, що спричинило трансформацію конфліктів: замість традиційного збройного протистояння дедалі частіше відбувається боротьба в інформаційному просторі, який поступово перетворюється на нову арену глобального суперництва. Відповідно, провідні держави світу дедалі активніше застосовують потенціал спеціальних інформаційних операцій (далі – СІО) як інструменту реалізації стратегічних інтересів.

Поняття СІО є вужчим проти раніше розглянутого поняття інформаційних операцій і використовується для позначення комплексних, цілеспрямованих дій, спрямованих на вплив на свідомість, емоційний стан та поведінку певних цільових аудиторій, як ворожих, так і нейтральних або союзницьких. Основною метою таких операцій є досягнення визначених стратегічних або тактичних результатів шляхом використання інформації як інструменту впливу. Натомість інформаційні операції – це ширше поняття, яке охоплює всі дії, пов’язані з інформацією: її збір, обробку, зберігання, передачу й захист. У межах цього концепту можуть реалізовуватись як нейтральні, так і маніпулятивні або деструктивні заходи, що не завжди мають на меті безпосередній психологічний вплив чи зміну поведінки. Таким чином, СІО є частиною ширшого явища – інформаційних операцій і орієнтуються переважно на досягнення контролю над інформаційним простором шляхом впливу на цільові аудиторії.

Історичні витоки СІО можна простежити ще з часів Першої світової війни, коли активно поширювалися агітаційні листівки з пропагандистським змістом. У період Другої світової війни інформаційна пропаганда набула системного характеру: вона базувалася на відвертих маніпуляціях і дезінформації, що, попри свою викривлену природу, демонструвала значну ефективність. Особливо масштабно можливості інформаційної пропаганди реалізовувалися в умовах тоталітарного режиму Радянського Союзу, де було створено потужну систему інформаційно-ідеологічного впливу, яка охоплювала всі рівні суспільного життя.

Саме завдяки цьому вдавалося забезпечувати штучну єдність, централізованість рішень та контрольованість процесів соціалістичного будівництва [123, с. 224].

Попри те, що різноманітні форми СІО застосовувалися протягом тривалого історичного періоду, саме у XX столітті вони набули статусу одного з ключових інструментів військово-політичного протистояння. Швидке поширення глобалізаційних процесів, інтенсивний розвиток інформаційно-комунікаційних технологій, зростання впливу медіа та цифрових каналів комунікації трансформували СІО в надзвичайно потужний засіб реалізації як зовнішньополітичних, так і внутрішньополітичних стратегій. За таких обставин сфера їхнього застосування вийшла далеко за межі суто військової площини, охопивши також політичний, економічний, соціальний та гуманітарний виміри функціонування суспільства [166, с. 135].

У межах досліджень, присвячених феномену інформаційної війни, кожна окрема операція трактується як цілеспрямований процес використання інформації як засобу впливу й охоплює її продукування, обробку, передавання та сприйняття. Конкретні характеристики та механізми реалізації інформаційних операцій варіюються залежно від контексту їхнього застосування – політичного, економічного, соціального тощо. Найбільш виразно ця специфіка проявляється у сфері політичної діяльності, де інформаційні технології активно використовуються для маніпулювання суспільною думкою та формування бажаних моделей поведінки [75, с. 135].

У цьому ключі спеціальні інформаційні операції визначаються як заздалегідь сплановані дії, спрямовані на певну аудиторію (ворожу, нейтральну або союзницьку), їх метою є вплив на свідомість, ціннісні орієнтації та поведінкові патерни аудиторії через застосування організованого інформаційного контенту та сучасних інформаційних технологій [176].

До ключових об’єктів впливу, що зазнають втручання під час реалізації СІО, належать:

– інститути публічного управління держави, включно з її збройними силами;

– системи управління цивільною інфраструктурою, зокрема телекомунікаційні мережі, засоби масової інформації, транспортна, енергетична, фінансова та промислова інфраструктури;

– елементи військової інфраструктури, які забезпечують зв'язок, розвідку, бойове командування, логістику та контроль над озброєнням;

– канали зв'язку та засоби передавання інформації;

– інформаційні ресурси, що циркулюють або зберігаються в системах управління;

– широкі соціальні верстви, включно з цивільним населенням і військовослужбовцями, а також відповідні державні, економічні та соціальні інституції;

– електронні медіа;

– управлінський та технічний персонал автоматизованих систем, що беруть участь у процесах ухвалення стратегічних рішень [186, с. 151-156].

Водночас проведення спеціальних СІО виокремлюються три головні цільові аудиторії:

1) психоемоційна сфера представників політичної еліти, що дозволяє впливати на ухвалення рішень на найвищому державному рівні;

2) масова свідомість населення протиборчих держав та інститути, що формують суспільну думку;

3) процеси ухвалення державно-управлінських рішень, зокрема у сфері національної безпеки.

СІО, що мають психологічну орієнтацію, передбачають цілеспрямоване створення та поширення спеціально підготовленого інформаційного контенту, який безпосередньо впливає на інформаційно-психологічне середовище, поведінкові моделі та емоційно-когнітивні стани політичних лідерів і громадян відповідної країни [20, с. 129].

У сучасному безпековому контексті інформаційно-психологічні операції посідають провідне місце в структурі інформаційно-психологічної війни [72, с.

296]. Залежно від характеру впливу та цільових орієнтирів такі операції поділяють на кілька основних типів:

– пропагандистські, які мають на меті формування та поширення ідеологічно забарвленої інформації, що слугує інструментом впливу в умовах політичної конкуренції або просування певних ідеологічних засад;

– дезінформаційні, спрямовані на цілеспрямоване введення суб'єкта впливу в оману. Такі операції активно застосовуються в контексті як політичного, так і економічного суперництва, а також під час військових конфліктів;

– маніпулятивні, основною метою яких є приховане управління поведінкою та рішеннями об'єкта впливу через інформаційне середовище;

– оборонні, покликані нейтралізувати зовнішній інформаційно-психологічний тиск, захистити власне населення або союзні структури, а також забезпечити адекватну інформаційно-психологічну відповідь [112, с. 210].

Ключовим завданням інформаційних операцій є маніпулювання свідомістю індивідів і масовими установками задля досягнення стратегічних або тактичних цілей. До найпоширеніших напрямів інформаційного впливу належать:

– формування та впровадження в суспільну свідомість ворожих або деструктивних ідей і переконань;

– дезінформація та свідоме порушення орієнтації в сприйнятті подій і фактів;

– підрив морально-етичних основ та послаблення наявних переконань;

– створення образу зовнішнього ворога з метою нагнітання страху серед населення;

– демонстрація сили й переваги для деморалізації противника;

– забезпечення власних економічних інтересів шляхом розширення ринку збуту через інформаційний вплив [179, с. 49–50].

У сучасній науковій літературі [72; 96; 176] значна увага приділяється дослідженню методів, що використовуються в межах СІО для дезорієнтації масової свідомості (Додаток Б). Найчастіше аналізу підлягають такі ключові інструменти:

1. *Дезінформація* – це метод навмисного спотворення інформації з метою введення суб'єкта впливу в оману, що має призвести до ухвалення запрограмованих рішень або вчинення очікуваних дій. У практиці СІО виокремлюють такі форми дезінформування:

тенденційне викладення фактів – подача інформації в упередженому світлі шляхом акцентування на вибраних правдивих даних, що формують спотворену картину дійсності;

дезінформація «від зворотного» – передача достовірної інформації в такому контексті, що її сприйняття стає хибним або відторгненим;

термінологічне «мінування» – викривлення змісту ключових понять і термінів, що ускладнює розуміння суті подій;

«сіре» дезінформування – поєднання правдивої інформації з дезінформаційними вставками;

«чорне» дезінформування – поширення переважно неправдивої або вигаданої інформації.

Застосування дезінформації може реалізовуватися через створення ілюзії витоку секретної інформації; організацію «успіхів» іноземних спецслужб; поширення через медіа, зокрема контрольовані інформаційні агентства, блогерів або лояльних журналістів.

1. *Пропаганда* є процесом поширення ідей, поглядів або концепцій із метою їхнього закріплення в громадській свідомості й активізації відповідної масової поведінки. Вона передбачає формування вигідного інформаційного середовища; викликання емоційної реакції; стимулювання певної політичної або соціальної поведінки.

Хоча поняття дезінформації й пропаганди іноді ототожнюються, вони мають відмінності. Пропаганда не завжди передбачає поширення фейкової інформації, а її застосування історично пов'язується з діяльністю держав у межах авторитарних або тоталітарних режимів. Сучасні форми публічної дипломатії, попри демократичну орієнтацію, можуть набувати рис інформаційного впливу з

ознаками пропаганди, що в умовах геополітичної напруги створює ризики їхнього ототожнення з дезінформаційними кампаніями [96, с. 1108–1109].

3. *Психологічний тиск* – метод впливу, заснований на залякуванні або створенні загрозливої атмосфери з метою примусу до певної поведінки. Застосовується як у відносинах між державами, так і щодо внутрішніх груп населення.

4. *Маніпулювання* полягає в прихованому інформаційному впливі на психіку особи чи групи з метою зміни їхніх переконань, установок або моделей поведінки. Здебільшого здійснюється без усвідомлення суб'єктом факту зовнішнього впливу.

5. *Інформаційний тероризм* означає цілеспрямований інформаційно-психологічний тиск, який супроводжується залякуванням, погрозами, поширенням контенту, який жахає, або навіть вбивствами, що мають за мету дестабілізацію громадської думки та нагнітання страху серед населення.

6. Поширення *чуток* – це неофіційне розповсюдження недостовірної або частково правдивої інформації з метою провокування дезорганізації суспільства чи окремих інституцій. Чутки класифікуються за експресивністю (викликані емоційними реакціями); інформаційним параметром (ступінь достовірності); ступенем впливу на індивідуальну або масову свідомість.

7. *Диверсифікація громадської думки п*ередбачає нав'язування штучних або перебільшених проблем, що призводить до розпорошення уваги управлінських структур та відволікання їх від розв'язання стратегічно важливих питань соціального, політичного чи економічного характеру [176].

У сучасному глобалізованому світі, де інформаційний простір дедалі більше стає ключовим елементом національної безпеки, СІО перетворюються на дієвий інструмент ведення гібридних конфліктів. На прикладі України, яка з 2014 року перебуває з російською федерацією в стані війни за Незалежність, можемо спостерігати широкий спектр методів і форм, що використовуються в рамках таких операцій. Згідно із сучасними дослідженнями у сфері інформаційного

елемента когнітивної безпеки [124, с. 103], найбільш характерними проявами СІО, спрямованих проти України, є:

- розвідувальна діяльність через інформаційні канали. До таких дій належить організація збору, обробки та передавання противнику чутливої інформації про стратегічно важливі об'єкти: військові частини, інфраструктуру енергетичного сектору, логістичні центри, розміщення озброєння та військової техніки, обсяги військової допомоги від міжнародних партнерів. Особливу небезпеку становлять «цивільні шпигуни» та так звані «коригувальники вогню», які використовують цифрові платформи, месенджери та соціальні мережі для передавання інформації ворогу;

- поширення деструктивного та антиукраїнського контенту. Пропагандистська діяльність охоплює не лише традиційні медіа, але й соціальні мережі, де поширюються візуальні й текстові матеріали, що підривають довіру до державних інституцій, знижують морально-психологічну стійкість населення та делегітимізують українську владу. Типовими прикладами є використання риторики на кшталт: «київський режим», «фашистська хунта», «громадянська війна» тощо. Це – спроба нав'язати хибну картину внутрішньої нестабільності й створити «альтернативну реальність» для внутрішнього і міжнародного споживача;

- поширення сепаратистських і антиконституційних наративів. Підрив державного суверенітету України також відбувається через заклики до зміни конституційного ладу, підтримку ідеї федералізації, розповсюдження тез про нібито «природне право» регіонів на самовизначення або приєднання до інших держав. Такі ідеї активно впроваджуються через підконтрольні Росії інформаційні ресурси, а також «автономізовані» акаунти в соціальних мережах;

- кібердари по державних та критичних інформаційних ресурсах. DDoS-атаки, злом офіційних сайтів органів влади, медіа, банківських структур та інших критично важливих інституцій стали буденною реальністю в умовах гібридної війни. Метою таких дій є створення хаосу, перешкоджання комунікації між

владою та суспільством, ослаблення довіри до інфраструктури цифрового урядування;

- маніпулятивне розгойдування суспільних настроїв. До такого типу операцій належать системні спроби розпалити внутрішні конфлікти в Україні: йдеться про експлуатацію тем релігійного розколу, мовного питання, ідеологічних відмінностей, історичних трактувань тощо. Через соціальні мережі та платформи миттєвого обміну повідомленнями організовується поширення панічних настроїв, посилюються протиріччя між різними суспільними групами, знижуються показники довіри до армії, уряду та союзників.

Незалежно від конкретного формату чи засобів реалізації, СІО, як правило, реалізуються за чіткою структурною схемою, що охоплює чотири основні етапи:

1. Планування операції (підготовчий етап). На цьому етапі проводиться детальний аналіз ситуації: визначаються стратегічні цілі, формулюються завдання, ідентифікуються цільові аудиторії та підбираються методи впливу. Окрім цього, розраховуються ресурси, канали комунікації, час проведення операції та очікувані результати. До участі залучаються фахівці із соціальної інженерії, політтехнологи, психологи, ІТ-спеціалісти та аналітики.

2. Створення або використання інформаційного приводу. Для активного запуску СІО обирається резонансна подія, яка вже має або потенційно може викликати сильний емоційний відгук. Це може бути: трагедія, політичний скандал, провокація, військова поразка або «героїчний вчинок». Подія подається з чітко сформульованим наративом, який апелює до страху, гніву або відчуття несправедливості. Інформаційний привід виконує роль спускового механізму для подальшого масштабного інформаційного впливу.

3. «Розкрутка» інформаційного приводу. Основна фаза операції полягає в активному поширенні підготовленого контенту. Задіяно всі можливі канали – від традиційних медіа до соціальних мереж і блогерських платформ. Часто використовується бот-мережа, лідери думок, а також підконтрольні медіа для ретрансляції наративу. Матеріали тиражуються багаторазово, змінюються

акценти, створюється візуальний супровід (меми, відео, графіка), що забезпечує широке охоплення аудиторії.

4. Завершення операції («вихід» з неї). Після досягнення запланованого ефекту – зміни громадської думки, делегітимізації органів влади, виклику паніки чи міжнародного резонансу – активність поступово знижується. У разі виявлення операції або суспільного спротиву її може бути згорнуто достроково. Завершальний етап також включає аналіз досягнутих результатів, коригування методів для подальших кампаній і підготовку нових етапів інформаційного впливу.

Одним із ключових чинників, що визначають ефективність таких операцій, є правильно підібраний інформаційний привід. Саме він виступає відправною точкою інформаційного впливу, слугуючи каталізатором процесів мотивації або демотивації цільової аудиторії відповідно до загального оперативного задуму, стратегічних цілей і тактичних завдань організаторів СІО.

Інформаційний привід є основою для подальшого етапу операції – фіксаційного, або фіксувального, під час якого цільова аудиторія, перебуваючи під впливом завчасно спланованої інформаційної інтервенції, або вдається до дії, або ж, навпаки, утримується від неї, залежно від завдань, поставлених ініціаторами СІО. Таким чином, саме на етапі фіксації перевіряється ефективність маніпуляційного чи психологічного тиску.

Варто підкреслити, що правильний вибір або створення інформаційного приводу – це не другорядний, а один із найважливіших складників будь-якої інформаційної операції. Некоректно підібраний привід може призвести до низького рівня емоційної залученості аудиторії, її апатії або навіть протидії. Відповідно, інституціалізація методології проведення СІО на основі стандартів країн НАТО та її нормативно-правове закріплення в секторі безпеки й оборони України дозволить суттєво посилити національні спроможності у сфері інформаційного протиборства, особливо в умовах тривалої війни за Незалежність України [166, с. 132].

Не менш важливим аспектом організації ефективної інформаційної операції є точне визначення цільових аудиторій – груп населення, які піддаються психологічному або інформаційному впливу. Ці аудиторії можуть бути як ворожими, так і нейтральними або дружніми, і саме від правильної ідентифікації їх залежить успішність впроваджених наративів.

Для цього використовується інформація про географічне розташування, демографічні характеристики, рівень соціальної напруги, а також показники взаємодії в соціальних мережах. Особливої ваги набуває аналіз активності так званих агентів впливу в цифровому просторі, тобто користувачів, які мають високий рівень публікаційної активності, значну кількість підписників і здатні формувати громадську думку в онлайн-середовищі. Методика оцінювання ефективності таких агентів базується на показниках кількості мережевих увімкнень та індексу впливу на цільову аудиторію [34, с. 56].

Згідно з аналітичними матеріалами, СІО, які проводяться спецслужбами російської федерації проти України, мають чітко виражену багатовекторність. Науковці виділяють щонайменше три основні напрями реалізації таких операцій. Розглянемо кожну з них детальніше.

Внутрішні спеціальні інформаційні операції (на території рф). Основною метою таких операцій є забезпечення інформаційного контролю над власним населенням. Це передбачає нав’язування ідеї про загрозу з боку НАТО чи України, підтримку військової мобілізації, демонстрацію уявних успіхів «спеціальної воєнної операції», формування образу зовнішнього ворога (Захід, Україна, колективний «фашизм»), придушення протестних рухів та дезавуація альтернативних джерел інформації. Значну роль у реалізації цих заходів відіграють державні медіа, а також приватні медіаплатформи, афілійовані з владою.

Зовнішні спеціальні інформаційні операції. Ці операції спрямовані на інфопростір інших держав і поділяються на дві підгрупи:

Операції в інформаційному просторі України, які мають на меті деморалізацію суспільства, поширення панічних настроїв, провокування зневіри

в ЗСУ, делегітимізацію політичного керівництва, розпалювання міжетнічної ворожнечі, мови ворожнечі та внутрішніх конфліктів.

Операції в просторі третіх країн, покликані вплинути на громадську думку в державах, які підтримують Україну. Йдеться про формування наративів про «неефективну» допомогу Україні, поширення зневіри в українських союзників, нав'язування образу «міжнародного конфлікту», що не стосується глядача напряму, аби зменшити підтримку з боку Заходу.

Операції в інформаційному середовищі тимчасового окупованих територій. Ці СІО спрямовані на контроль над населенням тимчасово окупованих територій шляхом поширення проросійських наративів, ідеологічної обробки, нав'язування сепаратистських або екстремістських поглядів. Метою є створення серед місцевого населення образу України як ворога, легітимізація дій окупаційної адміністрації та залучення новобранців до лав збройних формувань рф. Особливо активно впроваджуються тези про «звільнення від українського нацизму», «історичну справедливість» та «захист російськомовного населення» [124, с. 100–102].

Таким чином, ефективне проведення спеціальних інформаційних операцій вимагає поєднання кількох критично важливих факторів: наявності чітко спланованого інформаційного приводу, точного визначення цільових аудиторій, глибокого моніторингу соціальних мереж, використання сучасних технологій мікротаргетингу, а також продуманого завершення операції з урахуванням ефективності впливу. З огляду на актуальну безпекову ситуацію Україні необхідно не лише адаптувати західні підходи до СІО, але й створювати власні механізми протидії національного рівня як у законодавчому, так і у практичному вимірі.

Спеціальні інформаційні операції проти України мають комплексний, багаторівневий характер і реалізуються через відкриті і приховані канали впливу. Їхня ефективність значною мірою зумовлена глибокою інтеграцією в суспільний дискурс, активним використанням технологій мікротаргетингу, маніпулятивної риторики, емоційної мобілізації та цифрової інфраструктури. Тому критично

важливим завданням державної політики у сфері національної безпеки має стати розробка системи оперативного реагування на загрози інформаційного характеру, посилення медіаграмотності населення, розширення функцій кіберрозвідки та інформаційної протидії.

На основі проведеного дослідження встановлено, що інформаційні спеціальні операції нині є потужним інструментом досягнення політичних цілей шляхом планомірного використання засобів, форм та методів поширення інформації для впливу на свідомість і поведінку людей. У сучасних умовах реалізація інформаційних спеціальних операцій відзначається низкою особливостей, які проявляються в методах, видах, формах, завданнях тощо.

Отже, інформаційний вплив у тому чи іншому вигляді супроводжував людську цивілізацію на багатьох ключових етапах її розвитку і людство адаптувалося до нових умов. Сьогодні ми вже є очевидцями того, як технології штучного інтелекту починають застосовуватися для управління масовою поведінкою людей з використанням єдиних загальносвітових систем зв'язку – насамперед мережі Інтернет. На державному рівні триває не тільки реалізація наступальних інформаційних операцій, а й активний пошук науково обґрунтованих рішень для проведення захисних й оборонних заходів; проблемам інформаційно-психологічного протиборства приділяється підвищена увага в науковому середовищі, передусім у центрах, афілійованих із відповідними відомствами.

3.3. Порівняльний аналіз технологій пропаганди та інформаційних операцій в умовах воєнного стану: досвід України

У контексті повномасштабної збройної агресії, розв'язаної російською федерацією проти України, особливої уваги набуває вивчення не лише воєнних аспектів протистояння, але й гібридних форм ведення війни, ключовим елементом яких є інформаційно-психологічний вплив та забезпечення когнітивної безпеки. Сучасна війна за Незалежність України виходить за межі

традиційного розуміння збройного конфлікту і все більше набуває рис комплексного протиборства у сфері інформації, свідомості та сприйняття. Інформаційні операції, що здійснюються рф, є частиною стратегії гібридної війни та спрямовані як на внутрішню, так і на міжнародну аудиторію.

російська федерація суттєво вдосконалила свої інформаційно-пропагандистські технології, зокрема у використанні інструментів масової комунікації, соціальних мереж, спеціалізованих інтернет-платформ та мережевих агентів впливу. Через масовану кампанію поширення дезінформації, маніпулятивних повідомлень, фейкових новин та викривленої інформації агресор формує альтернативну картину реальності, покликану узаконити власні дії, делегітимізувати українську владу та знизити рівень міжнародної підтримки України.

Інформаційні кампанії рф мають на меті не лише маніпулювання громадською думкою всередині країни, а й суттєвий вплив на міжнародне інформаційне поле: створення уявлення про Україну як нестабільну державу, дискредитацію її позицій на міжнародній арені, розкол у поглядах світової спільноти, послаблення консолідованої підтримки з боку стратегічних партнерів.

У зв’язку з цим, дослідження технологій інформаційних операцій, засобів пропаганди та механізмів їхньої реалізації в умовах воєнного часу набуває особливої ваги. Воно дозволяє не лише виявити інструменти впливу на свідомість та поведінку масової аудиторії, але й сформувати ефективні підходи до протидії інформаційним загрозам. Знання механізмів поширення дезінформації, особливостей конструювання фейкових повідомлень, каналів їхнього розповсюдження сприяє формуванню адекватної політики інформаційної безпеки та захисту державного інформаційного простору.

Крім того, наукове осмислення феномену пропаганди в умовах війни дозволяє краще зрозуміти, яким чином відбувається мобілізація населення, легітимізація агресії, маніпулювання історичними наративами та ціннісними орієнтирами. Так само це дає змогу створювати системи раннього виявлення

інформаційних атак, підвищувати інформаційну обізнаність громадян, зменшувати вразливість суспільства до інформаційних впливів.

Однією з найбільш резонансних подій в інформаційному полі під час повномасштабної війни російської федерації проти України став підрив Каховської гідроелектростанції, що стався 6 червня 2023 року. Цей акт техногенного тероризму, вчинений російськими окупаційними військами, призвів до масштабних наслідків: екологічних, гуманітарних, економічних та соціальних. Зокрема, значно постраждали Херсонська, Миколаївська, Запорізька, Одеська області, а також територія тимчасово окупованого Криму. Підрив Каховської ГЕС укотре актуалізував питання протидії російській пропаганді та інформаційним операціям, які безпосередньо впливають не лише на внутрішню, а й на міжнародну політичну комунікацію. У перші години після трагедії міжнародні медіа вийшли з низкою неоднозначних і суперечливих матеріалів, у яких або не було вказано конкретного винуватця, або ж звучали обережні формулювання на кшталт «сторони звинувачують одна одну» [91, с. 193-194]. Це засвідчило, наскільки потужно російська пропагандистська машина здатна впливати на світові інформаційні наративи навіть у випадках, коли факти очевидні.

Після підриву гідроелектростанції російська федерація застосувала комплексну систему пропагандистських прийомів, спрямованих на досягнення політичних і комунікаційних цілей. Зокрема, майже одночасно було оприлюднено кілька версій причин вибуху, які суперечили одна одній; згодом ці версії було спростовано, а відповідальність перекладено на Україну. Протягом короткого часу інформаційний простір наповнився фейковими повідомленнями, серед яких – сфальсифіковані фото й відео нібито «українського ракетного обстрілу». У результаті таких маніпуляцій було створено викривлену картину подій, яка мала на меті розмити відповідальність і поставити під сумнів очевидні факти [91, с. 193-194.]. Цей приклад яскраво демонструє, як інформаційно-психологічна війна є невід’ємною складовою сучасного воєнного протистояння. Російська пропаганда системно впливає на міжнародні медіа, які у свою чергу

впливають на позиції урядів різних країн. Таким чином формується певна «третя реальність» – інформаційна площина, де замість фактів домінують інтерпретації, вигідні державі-агресору.

У сучасних умовах пропаганда становить надзвичайно серйозну загрозу для інформаційної безпеки, оскільки вона володіє значним потенціалом маніпулювати масовою свідомістю, ціннісними орієнтирами та політичними переконаннями громадян. Під впливом пропаганди можлива трансформація суспільної свідомості – від апатії до радикалізації, від довіри владі до її повного заперечення, від співчуття до агресії. Це створює передумови для поширення ненависті, поляризації суспільства та виправдання насильства.

Пропагандистськими інструментами є дезінформація, перекручення фактів, поширення фейків, психологічний тиск, що стають засобами підриву міжнародної стабільності й дестабілізації внутрішнього соціально-політичного середовища держави, проти якої ведеться гібридна війна. Саме тому надзвичайно важливо досліджувати механізми формування пропаганди, її вплив на колективну свідомість і виробляти ефективні стратегії контрпропаганди та захисту національного інформаційного простору.

З огляду на дослідницьку проблематику нашої наукової роботи, виникає потреба детального аналізу поняття «пропаганда»в контексті сучасних наукових підходів. Це дозволить визначити сутність, інструменти та цілі пропагандистського впливу в умовах війни, а також окреслити ефективні механізми його нейтралізації.

У зв’язку з цим, нижче подаємо аналітичну таблицю (Табл. 3.1), у якій систематизовано підходи до визначення поняття «пропаганда», сформовані українськими і зарубіжними дослідниками. Такий порівняльний аналіз дозволить краще зрозуміти сутнісні характеристики цього явища, а також специфіку його реалізації в різних контекстах [91, с. 193-194].

Таблиця 3.1

Трактування категорії «пропаганда» в працях сучасних науковців

№	Автор	Визначення
1.	Некрасов А.	Пропаганда – це спрямована система впливу, що передбачає використання комунікативних методів та засобів для формування певних переконань, ставлень та дій аудиторії [122, с. 116].
2.	Заболотний А.	Пропаганда – це специфічний вид комунікації, який має на меті переконати інших та вплинути на них шляхом представлення інформації з метою досягнення певної мети чи підтримки певної ідеї [67, с. 216].

Продовження Табл.3.1

3.	Кухоцька Т.	Пропаганда – це масовий, організований і систематичний процес, спрямований на маніпуляцію суспільною свідомістю та вплив на неї [91, с. 193-194].
4.	Городнича К.	Пропаганда – це інженерія згоди, спрямована на створення сприятливого налаштування аудиторії та вплив на її поведінку через ретельне керування інформацією [43, с. 82-84].
5.	Шевців М., Гончарук К.	Пропаганда – це створення ілюзії, сприяння формуванню інтерпретацій і подій з метою зміни думок та дій громадськості [182, с. 119-122].
6.	Метінглі Д. К., Яо Е.	Пропаганда – це здійснення систематичного та прихованого впливу на маси за допомогою розроблених та вивчених технологій комунікації [247, с. 1569-1594].
7.	Малхан М., Девані П. П.	Пропаганда – це масштабна організована спроба вплинути на громадську думку та переконання зазвичай через розповсюдження односторонньої та вибіркової інформації [244, с. 1-15].

Оформлено автором за даними, на які посилаються вище

Таким чином, на основі аналізу наукових підходів можемо зробити висновок, що пропаганда є складним та багатовимірним поняттям. Її розглядаємо як систематичний, масовий процес цілеспрямованого впливу на громадську думку, переконання і поведінку окремих осіб або соціальних груп з метою

досягнення конкретних стратегічних, політичних, ідеологічних чи соціальних цілей.

Пропагандистський вплив реалізується через різноманітні канали комунікації: засоби масової інформації, соціальні мережі, телебачення, радіо, графічні матеріали, публічні виступи тощо. Її характер часто маніпулятивний, вона може містити елементи дезінформації, спотворення фактів та емоційного тиску, що сприяє зміні ставлення, поведінки та суспільних настроїв.

Зміст пропаганди тісно пов'язаний із конкретним політичним чи геополітичним контекстом, у якому вона використовується як інструмент інформаційного тиску, психологічного впливу або підтримки легітимності певної влади чи режиму. Тому її аналіз і викриття є критично важливими для забезпечення стабільності демократичних суспільств та інформаційної безпеки. У цьому контексті інформаційна війна російської федерації проти України є прикладом масштабного використання пропаганди в сучасному воєнно-політичному конфлікті. рф постійно застосовує інформаційні технології маніпуляції, створюючи викривлену картину реальності: поширює фейки, звинувачення, підроблені новини, а також формує негативний образ України на міжнародній арені. Основна мета таких дій – дискредитувати українську владу, деморалізувати населення, вплинути на міжнародну громадську думку та знизити рівень підтримки України з боку партнерів, що створює серйозні виклики для національної та міжнародної безпеки, тому потребує глибокого аналізу, моніторингу та розробки ефективних заходів протидії як з боку державних інституцій, так і громадянського суспільства.

Аналогічно здійснимо порівняння трактувань категорії «інформаційна операція» в працях сучасних учених. Для цього скористаємося нижченаведеною таблицею (Табл. 3.2), у якій наочно відобразили інтерпретації українських і іноземних науковців.

Таблиця 3.2

Трактування категорії «інформаційна операція»
в працях сучасних науковців

№	Автор	Визначення
1.	Верголяс О.	Інформаційна операція – це систематична стратегічна діяльність для досягнення стратегічних цілей шляхом контролю над інформаційною обстановкою [22, с. 7-16].
2.	Ділай А., Кротченко В.	Інформаційна операція – використання інформації та комунікації для впливу на інших із метою досягнення стратегічних цілей [61, с. 13-20].
3.	Сніцаренко П.	Інформаційна операція – систематична діяльність зі створення, розповсюдження та керування

Продовження Табл.3.2

		інформацією для впливу на сприйняття та поведінку цільових аудиторій [169, с. 37-42].
4.	Ерретт К., Лінвілл Д. Л., Сміт Г., Воррен П. Л., Белламі Л., Моавад М., Муді М.	Інформаційна операція – комплекс дій зі збору, аналізу, обробки, розповсюдження та контролю інформації для досягнення стратегічних цілей, що охоплює вплив на громадську думку [221, с. 1595-1613].
5.	Лінвілл Д. Л., Воррен П. Л.	Інформаційна операція – інтегрована система комунікації та впливу для маніпуляції інформацією та враженнями для досягнення політичних чи військових цілей [242].

Оформлено автором за даними, на які посилаються вище

Таким чином, інформаційна операція може бути визначена як складне, багатовимірне явище, що передбачає скоординовану діяльність із збору, обробки, аналізу, створення та поширення інформації з метою впливу на свідомість, сприйняття та поведінку визначених цільових аудиторій. Така діяльність охоплює широкий спектр комунікаційних засобів, зокрема традиційні медіа (телебачення, радіо, друковану пресу), цифрові платформи (інтернет, соціальні мережі), а також спеціалізовані інформаційні технології. Вплив, що

здійснюється в межах інформаційних операцій, може бути як прямим, так і опосередкованим, а його наслідки – короткостроковими або стратегічними.

Цілі інформаційних операцій надзвичайно варіативні: вони можуть полягати у впливі на громадську думку, маніпулюванні інформаційним простором, створенні або руйнуванні певних образів (лідерів, країн, подій), зміні політичного порядку денного або в сприянні конкретним діям чи їх гальмуванню.

Поняття інформаційної операції активно застосовується в політичному, військовому, економічному, соціальному та культурному контекстах, де важливу роль відіграє не лише передача інформації, а й цілеспрямований психологічний вплив. Це передбачає використання спеціальних методик впливу, маніпуляційних стратегій та інформаційних технологій, здатних змінювати переконання, спонукати до дій або, навпаки, дезорієнтувати цільову аудиторію.

Критично важливою характеристикою інформаційних операцій є їхній вплив на національну та міжнародну безпеку, а також їхній потенціал змінювати хід політичних, економічних та безпекових процесів. У зв’язку з цим моніторинг, аналіз і протидія інформаційним операціям є першочерговими завданнями для інституцій державної безпеки та інформаційного захисту.

Варто також зауважити, що, попри наявність понятєвих відмінностей між термінами «пропаганда» та «інформаційна операція», у практиці гібридної війни (зокрема, в умовах збройної агресії російської федерації проти України) ці інструменти застосовуються не ізольовано, а комплексно та взаємодоповнювально, утворюючи єдиний впливовий контур. У такому поєднанні вони реалізуються як взаємопов’язані елементи, що підсилюють ефективність один одного в межах спільної логіки впливу на цільові аудиторії. Обидва явища спрямовані впливати на інформаційний простір, використовуючи техніки маніпуляції, дезінформації та психологічного тиску, які, хоча й можуть мати різні форми прояву, виконують подібну функцію в досягненні очікуваних комунікативних результатів.

З огляду на це, у рамках дослідницької проблематики наукової роботи доцільним є розкриття ключових спільних рис технологій пропаганди та інформаційних операцій, що дає змогу чіткіше окреслити їхню структурну спорідненість і практичну взаємозалежність. Саме така постановка питання дозволяє узагальнити характерні елементи обох феноменів і представити їх у зіставному вигляді, без втрати змістової специфіки кожного з них. Для ілюстрації цієї взаємозалежності та структурної спільності подано блок-схему (Рис. 3.1), яка наочно демонструє системні елементи й взаємозв'язки між цими поняттями, підкреслюючи їхню функціональну близькість у контексті гібридного протистояння.

Рисунок 3.1. Ключові спільні риси технологій пропаганди та інформаційних операцій

Розглядаючи взаємозв'язок між технологіями пропаганди та інформаційних операцій, можна виокремити низку ключових спільних рис, що демонструють їхню взаємну природу та перехресне застосування в сучасних конфліктах, зокрема в умовах гібридної війни. До таких рис належать:

- Використання медійних платформ. Обидві технології активно залучають традиційні та цифрові медіа: телебачення, радіо, вебсайти, соціальні мережі – для поширення цільових повідомлень. У контексті війни за Незалежність України особливого розповсюдження набули проросійські Telegram-канали, які виконують функцію інструментів впливу на суспільну думку. Також варто згадати колишні проросійські телеканали, пов'язані з представниками олігархічного середовища (зокрема проросійськими політичними силами), які до заборони слугували каналами ретрансляції ідеологічних наративів країни-агресора.

- Активне використання кіберпростору**.** Як пропаганда, так і інформаційні операції широко застосовують цифрові інструменти: від створення вебресурсів й інтернет-форумів до залучення бот-мереж, фейкових акаунтів й автоматизованих систем для генерації та поширення повідомлень.

- Залучення візуальних засобів впливу. Для підсилення емоційного впливу обидві технології активно використовують відео, фотографії, інфографіку, меми тощо. Ці елементи, часто вирвані з контексту або сфабриковані, відіграють важливу роль у формуванні хибних уявлень про події.

- Аналітика даних. Технології обох напрямів застосовують інструменти аналітики (у тому числі Big Data та штучний інтелект) для моніторингу ефективності інформаційних повідомлень, рівня їхнього поширення, реакції аудиторії, а також для прогнозування потенційного впливу на різні соціальні групи.

- Таргетування аудиторій. Як пропагандистські кампанії, так і інформаційні операції розробляються з урахуванням особливостей цільової аудиторії. Це дозволяє адаптувати повідомлення до конкретного культурного, соціального чи демографічного контексту, підвищуючи їхню ефективність.

- Співпраця з внутрішніми акторами. У низці прикладів реалізація таких технологій передбачає координацію з внутрішніми групами, спільнотами,

інфлюенсерами або навіть політичними діячами, які стають трансляторами наративів, вигідних зовнішнім замовникам.

- Використання шифрування та анонімності. Захист ідентичності організаторів і джерел є важливим елементом обох технологій. Широко застосовуються технології анонімізації, шифрування повідомлень, використання VPN і проксі-серверів, що унеможливлює оперативне виявлення джерел дезінформації або пропаганди.

Здійснимо розкриття та аналіз ключових відмінностей технологій пропаганди та інформаційних операцій за допомогою нижченаведеної блок-схеми (Рис. 3.2), на якій наочно відображена зазначена системність структурних елементів.

Рисунок 3.2. Ключові відмінності технологій пропаганди та інформаційних операцій

Попри наявність значної кількості спільних рис, пропаганда та інформаційні операції є різними за своєю природою, цілями, масштабом, методами реалізації та контекстом використання. Нижче наведемо основні

аспекти, що виокремлюють ці два явища як самостійні, хоча й взаємопов'язані інструменти впливу.

1. Цілі та спрямованість

– Пропаганда насамперед орієнтована на переконання аудиторії в правильності певних ідеологічних, політичних або соціальних поглядів, формування стійких переконань і підтримки конкретної позиції.

– Інформаційні операції мають ширший спектр цілей, який може охоплювати не лише переконання, але й дезінформацію, збір розвідданих, дестабілізацію ситуації, психологічний тиск, нейтралізацію противника в інформаційному просторі тощо.

2. Масштаб та амплітуда впливу

– Пропаганда має зазвичай масовий характер й орієнтується на широку аудиторію, часто на рівні всієї держави чи міжнародної спільноти.

– Інформаційні операції можуть бути локалізованими та спрямованими на конкретні групи або навіть окремих осіб (наприклад, військових командирів, політиків, журналістів) залежно від цілей операції.

3. Рівень відкритості та легітимності

- Пропагандистська діяльність може здійснюватися відкрито і навіть офіційно підтримуватися державними структурами або політичними партіями.

- Інформаційні операції зазвичай мають прихований характер, часто реалізуються у форматі секретних спецоперацій, що можуть порушувати міжнародне або національне законодавство.

4. Контекст застосування

– Пропаганда широко використовується в політичній, культурній, соціальній, релігійній сферах та в мирний час.

– Інформаційні операції найчастіше застосовуються в умовах конфліктів, війни, гібридної агресії, у галузях кібербезпеки, розвідки та воєнної стратегії.

5. Засоби реалізації

– Пропаганда використовує традиційні канали комунікації: телебачення, пресу, соціальні мережі, публічні виступи, культурні продукти тощо.

– Інформаційні операції охоплюють технічно складні методи, зокрема кібератаки, бот-мережі, цілеспрямовану дезінформацію, збір і викрадення даних, вплив через агентів впливу, психологічні операції (PSYOPS).

6. Актори впливу

– Пропаганда часто є продуктом державної політики або ідейно зорієнтованих структур, наприклад політичних партій чи ідеологічних організацій.

– Інформаційні операції можуть здійснюватися державними, напівдержавними, приватними, а в деяких випадках навіть кримінальними угрупованнями або терористичними організаціями.

7. Оцінка ефективності

– Ефективність пропаганди часто важко виміряти в кількісному вимірі, адже вона працює з емоціями, ідеологією та глибинними переконаннями, що змінюються повільно.

– Натомість інформаційні операції мають чіткі оперативні цілі (наприклад, злам інформаційного ресурсу, змінення поведінки конкретного актора, дестабілізація ситуації) та можуть оцінюватися за результатами дій аудиторії чи ефектом у реальному часі.

У результаті проведеного дослідження можемо зробити такі узагальнення:

1. Технології пропаганди та інформаційних операцій демонструють низку спільних характеристик, що вказують на їхню взаємозалежність та потенціал взаємного підсилення в умовах сучасної інформаційної війни. Обидва інструменти активно використовують медійні платформи (телебачення, соціальні мережі, інтернет-ресурси), кіберпростір (вебсайти, форуми, боти), а також візуальні засоби комунікації (фото, відео, інфографіка) для формування та трансляції цільових меседжів. Крім того, спільною рисою є використання аналітики даних, інструментів таргетингу, а також залучення внутрішніх акторів (громадських діячів, блогерів, агентів впливу) для поширення ідеологічних або стратегічних наративів. Не менш важливим аспектом є застосування технологій

шифрування та збереження анонімності для забезпечення конфіденційності джерел та каналів інформаційного впливу.

2. Попри спільну комунікаційну природу, пропаганда та інформаційні операції мають принципові відмінності, які полягають у різній спрямованості, методах реалізації, масштабах впливу та рівнях відкритості. Пропаганда, як правило, реалізується відкрито і передбачає систематичний вплив на масову свідомість із метою підтримки певних політичних чи ідеологічних позицій. Інформаційні операції ж охоплюють ширший спектр завдань – від маніпулятивного впливу та дезінформації до кібератак і розвідки – і можуть здійснюватися приховано, часто в умовах конфліктів або воєнного протистояння. На відміну від пропаганди, яка зазвичай здійснюється під егідою державних інституцій або політичних організацій, інформаційні операції можуть реалізовуватися також недержавними структурами, приватними акторами, а іноді й кримінальними угрупованнями.

Таким чином, усвідомлення відмінностей і спільних рис між пропагандою та інформаційними операціями є ключовим для формування ефективної системи інформаційної безпеки**.** У контексті гібридної війни, яку розв’язано проти України, ці інструменти виступають засобами стратегічного впливу, що потребує чіткого наукового осмислення, постійного моніторингу та адаптивної відповіді з боку державних структур, експертної спільноти та громадянського суспільства.

Порівняльний аналіз технологій когнітивного впливу в умовах воєнного стану дозволяє розглядати сучасний інформаційний простір як автономне середовище стратегічного протиборства, у межах якого вирішальне значення набуває не лише контроль над інформаційними потоками, а й вплив на свідомість, емоційні стани, ціннісні орієнтації та поведінкові моделі індивідів і соціальних груп. У цьому контексті когнітивна безпека постає як ключовий вимір національної безпеки, що безпосередньо пов’язаний зі здатністю держави та суспільства зберігати стійкість до деструктивних інформаційно-психологічних впливів.

Розглянуті інтерпретації інформаційних операцій у політичній практиці свідчать про їхню трансформацію з допоміжного інструменту політичної комунікації в самостійний елемент стратегічного управління політичними процесами. Сучасні інформаційні операції виходять за межі традиційного публічного піару чи агітації та дедалі більше наближаються до форм спеціальної діяльності, що використовують інструментарій соціальної інженерії, аналізу великих даних, штучного інтелекту та поведінкової психології. Така еволюція зумовлює підвищення рівня загроз когнітивній безпеці, оскільки об’єктом впливу стає не лише інформаційна інфраструктура, а й процеси мислення, інтерпретації реальності та ухвалення рішень.

Особливістю сучасних інформаційних операцій є їхня здатність формувати альтернативні інформаційні реальності, у межах яких викривлюються причинно-наслідкові зв’язки, підмінюються смисли та легітимізуються деструктивні наративи. За таких умов когнітивна безпека втрачає суто індивідуальний характер і набуває системного значення, оскільки масове поширення маніпулятивного контенту здатне змінювати колективні уявлення про політичну дійсність, підривати довіру до інститутів влади та дестабілізувати політичну систему загалом.

Встановлено, що спеціальні інформаційні операції є найбільш концентрованою формою когнітивного впливу, орієнтованою на цілеспрямоване втручання в психоемоційний і ціннісний простір цільових аудиторій. На відміну від ширших інформаційних операцій, СІО мають чітко окреслені цілі, ретельно визначені об’єкти впливу та структуровану поетапну логіку реалізації. Їхня ефективність значною мірою зумовлена здатністю ініціаторів операцій поєднувати інформаційні, психологічні та технологічні компоненти в єдину систему впливу.

Важливим результатом аналізу є усвідомлення того, що СІО функціонують у межах логіки когнітивного домінування, де основним ресурсом стає не фізична сила, а контроль над сприйняттям, інтерпретаціями та мотиваціями. У цьому ключі когнітивна безпека може бути визначена як стан захищеності

індивідуальної та колективної свідомості від нав’язування деструктивних смислів, що порушують здатність до автономного мислення та раціонального ухвалення рішень.

Досвід України в умовах гібридної війни засвідчує, що спеціальні інформаційні операції проти держави мають комплексний, багаторівневий характер і спрямовані одночасно на кілька цільових площин: масову свідомість населення, політичні еліти, міжнародну громадську думку та процеси ухвалення стратегічних рішень. Це дозволяє розглядати когнітивну безпеку не лише як індивідуальну психологічну характеристику, а як системну властивість політичної та соціальної організації суспільства.

Порівняльний аналіз технологій пропаганди та інформаційних операцій дає підстави для висновку про те, що обидва явища мають спільну комунікаційну природу, проте відрізняються за рівнем організованості, масштабом впливу та ступенем прихованості. Пропаганда, як правило, орієнтована на довгострокове формування ідеологічних установок і може здійснюватися відкрито, тоді як інформаційні операції мають більш гнучкий, ситуативний характер і часто реалізуються в латентній формі.

Водночас у практиці сучасної гібридної війни пропаганда та інформаційні операції функціонують у тісній взаємодії, взаємно підсилюючи одна одну. Саме ця синергія створює найбільші загрози когнітивній безпеці, оскільки поєднання масового емоційного впливу з точковими маніпулятивними технологіями здатне суттєво знижувати рівень критичного мислення та підвищувати сприйнятливість до дезінформації.

Особливо показовими в цьому контексті є приклади інформаційних кампаній, пов’язаних із резонансними подіями воєнного характеру, де спостерігається одночасне використання фейкових повідомлень, суперечливих наративів, маніпулятивних візуальних образів та психологічного тиску. Такі кампанії спрямовані не лише на дезорієнтацію аудиторії, а й на формування стану когнітивної перевтоми, апатії або недовіри до будь-яких джерел інформації, що є однією з найнебезпечніших форм когнітивної уразливості.

З огляду на це вважаємо, що когнітивна безпека в умовах воєнного стану повинна розглядатися як інтегральний компонент національної безпеки, що охоплює інституційний, соціальний та індивідуальний рівні. На інституційному рівні йдеться про здатність держави формувати цілісну систему інформаційної протидії, забезпечувати стратегічні комунікації та підтримувати легітимність політичних рішень. На соціальному рівні – про стійкість суспільства до маніпулятивних впливів, збереження соціальної згуртованості та довіри між ключовими акторами. На індивідуальному рівні – про розвиток критичного мислення, медіаграмотності та психологічної резильєнтності.

Таким чином, результати дослідження дозволяють констатувати, що інформаційні спеціальні операції та пропагандистські технології в умовах воєнного стану є не лише інструментами інформаційного впливу, а й чинниками трансформації когнітивного простору суспільства. Їхній вплив виходить за межі короткострокових інформаційних ефектів і здатен формувати довготривалі зміни в системі політичних уявлень, ідентичностей та моделей поведінки.

У цьому зв’язку забезпечення когнітивної безпеки постає як стратегічне завдання, що потребує комплексного підходу, поєднання правових, інституційних, освітніх і комунікаційних механізмів. Подальше ігнорування когнітивного виміру безпеки створює ризики не лише для інформаційного суверенітету держави, а й для функціональності політичної системи загалом, оскільки підриває її здатність до ефективного управління, легітимації влади та мобілізації суспільства в умовах екзистенційних викликів.

РОЗДІЛ 4. МОДЕЛЬ ФОРМУВАННЯ КОГНІТИВНОЇ БЕЗПЕКИ СУЧАСНОЇ УКРАЇНИ

4.1. Роль когнітивної безпеки у формуванні та збереженні легітимності політичної влади: виклики для України

Через цифровізацію парадигма національної безпеки зазнала суттєвої трансформації, вийшовши за межі традиційних військово-політичних та економічних вимірів. Когнітивна сфера суспільства як простір формування суджень, переконань та колективної ідентичності стала критичним фронтом боротьби за державний суверенітет і стабільність. Ядром цієї боротьби є когнітивна безпека**,** яку визначають як стан захищеності суспільної свідомості та процесів ухвалення рішень від цілеспрямованих маніпулятивних впливів.

Для України, яка з 2014 року є об'єктом збройної агресії та зовнішньої гібридної війни з боку російської федерації, а з 24 лютого 2022 року протистоїть повномасштабному вторгненню, забезпечення когнітивної безпеки набуло характеру практичного імперативу національного виживання. Особливу актуальність ця проблема набуває в контексті легітимності політичної влади**,** яка є фундаментальною основою функціонування держави в умовах екзистенційного протистояння. Легітимність, будучи соціально-психологічним феноменом визнання громадянами правомірності владних інститутів, виявляється вкрай вразливою до інформаційно-психологічних атак, що становить ключовий елемент гібридної стратегії агресора. Систематичний підрив довіри до уряду, парламенту та силових структур спрямований на внутрішню дестабілізацію, ерозію суспільної єдності та саботування спроможності держави до опору.

У ключі нашого дослідження є потреба в системному аналізі механізмів, за допомогою яких когнітивна безпека сприяє збереженню та зміцненню легітимності влади в умовах тривалої російсько-української війни. Поширення складних дезінформаційних кампаній, експлуатація соціально-економічних

наслідків повномасштабного вторгнення та використання технологій для таргетованого поширення ворожих наративів створюють виклики, що вимагають комплексної та науково обґрунтованої відповіді. Таким чином, наукове осмислення взаємозв'язку між когнітивною безпекою та легітимністю влади, а також розробка на його основі практичних рекомендацій є не лише теоретичною, але й нагальною прикладною задачею української політичної науки.

Наше дослідження базується на системному аналізі для визначення взаємозв'язків між когнітивною безпекою та легітимністю політичної влади в контексті гібридних загроз. Порівняльний аналіз застосовано до вивчення досвіду США та Естонії в протидії інформаційним загрозам, зокрема через стратегії міжвідомчої координації та розвитку відкритих державних даних. Контент-аналіз дезінформаційних кампаній 2022–2024 років в Україні проведено на основі даних Центру протидії дезінформації при РНБО та аналізу стратегічних наративів у соціальних медіа. Емпірична частина охоплює аналіз звітів громадських організацій і урядових установ щодо рівня довіри до державних інститутів, зокрема опитувань Центру Разумкова та Sociological Group «Rating» за 2023–2025 роки, а також оцінку антикорупційних механізмів.

Дослідження в галузі міжнародних відносин показують, що легітимність інституцій може ґрунтуватися не лише на внутрішній відповідності нормам, але й на когнітивній емуляції – процесі, коли організації наслідують інституційні форми успішних референтних організацій (наприклад, ЄС), щоб підвищити свою сприйняту легітимність. Цей механізм безпосередньо стосується когнітивної безпеки, оскільки він показує, як інформаційні потоки, зовнішні приклади та наративи можуть бути використані для маніпулювання інституційною легітимністю та відповідно суспільною довірою.

Для глибшого розуміння цих процесів необхідно враховувати когнітивні основи формування суджень про легітимність. Дослідження Т. Ленца та Л. Віоли [239] демонструє, що традиційна «модель конгруентності», яка пояснює легітимність винятково через відповідність інституційних рис соціальним нормам, є недостатньою. Насправді, судження про легітимність формуються

через складні когнітивні процеси, які опосередковуються ментальними схемами, евристиками та порівняннями з доступними еталонами. Це означає, що сприйняття легітимності є інерційним («липким»), порівняльним і схильним до систематичних спотворень. Наприклад, знайомі та встановлені інституції можуть сприйматися як більш легітимні навіть за наявності об'єктивної невідповідності нормам, тоді як різка зміна відбувається лише під впливом сильного, приголомшливого стимулу (наприклад, кризи), який викликає негативні емоції та змушує переосмислити наявні схеми [240].

Така модель пояснює, чому атаки в когнітивній війні часто спрямовані саме на підрив еталонних організацій, щоб викликати ефект «заразності» легітимаційної кризи (contagion), або навпаки, – на поширення певних наративів легітимації, що апелюють до знайомих схем, аби підтримати непопулярні режими. Таким чином, захист когнітивного простору вимагає не лише боротьби з дезінформацією, але й розуміння та протидії маніпуляціям самими когнітивними механізмами оцінки легітимності.

Ключовим інструментом протидії когнітивним загрозам та формування когнітивної стійкості (cognitive resilience) суспільства є медіаграмотність. Вона виступає як «колективна когнітивна імунна система», що поєднує зусилля державних, неурядових та міжнародних акторів для підвищення критичного мислення, впізнаваності маніпулятивних технік та здатності до спростування шкідливих наративів [240]. Досвід України та країн Балтії демонструє, що ефективна медіаграмотність потребує цілісного стратегічного підходу, інтегрованого в національну безпеку, із врахуванням моніторингу інформаційного простору, цільових кампаній для різних аудиторій (зокрема вразливих груп) та тісної взаємодії із сектором безпеки й оборони. У цьому контексті медіаграмотність виходить за рамки простого розпізнавання фейкових новин й охоплює розвиток емоційного інтелекту та практики здорового діалогу, що сприяють конструктивній участі громадян у суспільному житті, зокрема в дискусіях про ідентичність, пам'ять, історію та культурне розмаїття. Це особливо важливо для України з огляду на чутливість суспільного порядку

денного, пов’язаного з війною, виборами, мобілізацією та інтеграцією різноманітних соціальних груп.

Таким чином, когнітивна безпека виступає не лише як технологічний щит, але й як соціально-політичний інструмент, що сприяє збереженню довіри до влади в умовах гібридних загроз та інформаційних війн, зокрема протидії специфічній загрозі когнітивної війни, спрямованої на самі основи суспільного світогляду [206]. Її реалізація неможлива без розвитку медіаграмотності як основи когнітивної стійкості суспільства [240], а також без глибокого розуміння когнітивних механізмів (таких як емуляція [11] та формування суджень на основі схем і евристик [215], через які і може бути підірвана легітимність інституцій влади.

Ключові функції когнітивної безпеки в контексті легітимності влади (Додаток В):

1. Запобігання дезінформації. Когнітивні системи використовують передові методи обробки природної мови, машинного навчання та аналізу великих даних для виявлення, аналізу та нейтралізації дезінформаційних кампаній у реальному часі. Вони здатні ідентифікувати спотворення в сприйнятті діяльності влади, аналізуючи патерни маніпулятивних наративів та автоматизуючи їхнє спростування. Ця функція є ключовою для протидії когнітивній війні, яка використовує масштабне поширення брехні як зброю. Ефективним інструментом тут є створення системи моніторингу та раннього запобігання, що дозволяє оперативно реагувати на загрози.

2. Зміцнення медіаграмотності. Через інтерактивні платформи, освітні кампанії та персоналізовані інструменти когнітивна безпека сприяє розвитку критичного мислення в громадян. Системи можуть адаптувати контент відповідно до культурних, мовних та освітніх особливостей користувачів, навчаючи їх розпізнавати маніпуляції, перевіряти джерела й аналізувати інформацію. Це створює когнітивний щит суспільства проти спроб маніпулювання, які є основним інструментом когнітивної війни. Як показує досвід України, критично важливою є робота з різноманітними аудиторіями,

зокрема вразливими групами, через децентралізовані мережі акторів медіаграмотності, що формують *колективну когнітивну імунну систему*. У цьому контексті медіаграмотність передбачає не лише розпізнавання фейків, але й розвиток емоційного інтелекту, що сприяє конструктивному діалогу та зміцненню суспільної єдності [11].

3. Забезпечення стратегічної комунікації. Когнітивна безпека забезпечує побудову прозорих двосторонніх каналів взаємодії між державою та суспільством. Використовуючи інструменти стратегічної комунікації, такі як автоматизовані системи моніторингу суспільної думки, генерації контенту та управління кризами, вона допомагає формувати довіру, оперативно реагувати на запити громадян та забезпечувати цілісність інформаційного простору. Ця функція безпосередньо протистоїть меті когнітивної війни – ерозії довіри до інституцій влади через розкол суспільства. Ключову роль у цьому відіграє журналістська спільнота, яка потребує переосмислення своєї ролі та підвищення власної стійкості для ефективного виконання цієї функції [215].

4. Захист інституційної легітимності від когнітивних атак. Аналізуючи механізми когнітивної емуляції та когнітивні основи формування суджень про легітимність, когнітивна безпека може виявляти спроби маніпулювання інституційними образами та наративами, спрямовані на підрив довіри до національних установ шляхом їхнього непрямого порівняння із зовнішніми (часто ідеалізованими або, навпаки, дискредитованими) моделями. Це передбачає не лише моніторинг інформаційних потоків, але й активну роботу з когнітивними еталонами та схемами, що формують уявлення про «успішні» чи «неуспішні» інститути. Розвиток критичного розуміння того, як конструюється легітимність у глобальному інформаційному просторі, стає ключовим для протидії спробам штучного викликання легітимаційних криз через механізм «заразності» (*contagion*) [240] або через атаки на довіру до ключових інституцій-еталонів.

На основі даних дослідження «Індекс медіаграмотності українців за 2024 рік», проведеного ГО «Детектор медіа» [70], аналізу політики боротьби з

дезінформацією в Україні [158], а також дослідження дезінформації як загрози національній безпеці України в умовах неоголошеної російсько-української війни [44, с. 53], можемо виділити основні виклики, які впливають на когнітивну безпеку та легітимність політичної влади в Україні:

1. Масштабне поширення дезінформації. Дезінформаційні атаки є ключовим інструментом гібридної війни, спрямованої на підрив довіри до уряду, військових та міжнародних союзників України. Зокрема, російська агресія з 2022 р. активізувала використання дезінформації для маніпуляції суспільною думкою, посилення соціальної напруги та створення політичної нестабільності [158, с. 55]. Дезінформація в цифрову епоху набула нового рівня, використовуючи Інтернет як основний канал поширення ворожих наративів з огляду на ІПСО, спрямовані на пропаганду насильства, виправдання військових злочинів та підрив демократичних інститутів [44]. Основними темами таких атак є воєнні події, економічна ситуація та мобілізація, що експлікують емоційну втому населення.

2. Низький рівень медіаграмотності населення. Згідно з дослідженням «Індекс медіаграмотності українців за 2024 рік», лише 7% українців мають високий рівень медіаграмотності, тоді як 28% демонструють низький або нижчий за середній рівень. Хоча з початком повномасштабної війни частка аудиторії з вищим за середній рівнем медіаграмотності зросла з 55% (2020 р.) до 81% (2022 р.), у 2024 р. спостерігається зниження частки осіб із високим рівнем медіаграмотності (з 31% у 2022 р. до 7% у 2024 р.). Це пов’язано з коригуванням методології обчислення індексу, а також з емоційною втомою від важкої інформації та зменшенням кількості джерел, які використовуються для перевірки новин. Лише 40% українців регулярно перевіряють достовірність інформації, що робить суспільство вразливим до маніпулятивних впливів [70].

3. Відсутність координації та єдиної стратегії протидії інформаційним загрозам. Діяльність державних органів, таких як Центр протидії дезінформації при РНБО, є фрагментованою, що знижує ефективність боротьби з дезінформацією [158, с. 48–55.]. Відсутність централізованого міжвідомчого

органу, який би координував зусилля у сфері когнітивної безпеки, ускладнює швидке реагування на інформаційні атаки та створення єдиної стратегії комунікації. О. Пташенко наголошує на необхідності створення комплексної стратегії національної безпеки для протидії дезінформації, яка б поєднувала законодавчі, технічні та освітні заходи. Крім того, дослідження Б. Гривнака, І. Лопушинського та І. Сапіжак підкреслює, що для ефективної протидії дезінформації необхідно вдосконалити законодавство України, висвітлити юридичне визначення дезінформації та механізми притягнення до відповідальності за її поширення, а також виконання європейських рекомендацій щодо підвищення медіаграмотності [44, с. 52–55].

4. Емоційна втома та зниження активності в перевірці інформації. Дослідження 2024 р. показує зниження середньої кількості джерел, які використовують українці для отримання суспільно-політичних новин, а також зменшення кількості тих, хто активно перевіряє достовірність контенту [70]. Це свідчить про адаптацію до поточного медіаландшафту, але також про ризик зниження пильності через тривалу дію стресових факторів війни. Дезінформація, зокрема через новинний відеоконтент та інформаційно-психологічні операції, експлуатує цю втому, посилюючи вплив на суспільну свідомість [44, с. 52–55].

5. Недостатній розвиток цифрових компетентностей. Незважаючи на зростання використання інтернету як джерела новин (89% українців використовують інтернет для отримання інформації про суспільно-політичне життя [70]), лише 32% респондентів застосовують практики цифрової безпеки, такі як двофакторна автентифікація чи використання VPN. Обізнаність щодо штучного інтелекту також залишається низькою: лише 25% опитаних повідомили, що використовують системи ШІ, а 60% не можуть визначити контент, створений за допомогою ШІ [70]. Це створює вразливість до нових форм маніпуляцій, зокрема deepfake-технологій, що є серйозною загрозою в умовах інформаційної війни [158, с. 48–55].

Сучасні інструменти поширення дезінформації, такі як автоматизовані системи та соціальні мережі, вимагають розвитку нових засобів захисту, а також вдосконалення технологій моніторингу інформаційного простору (Табл.4.1).

Таблиця 4.1

Основні показники медіаграмотності українців у 2022-2024 рр.

Показник	Значення (2024)	Порівняння з 2022	Коментар
Загальний індекс медіаграмотності	5.2 (за шкалою 0–10)	5.8	Зниження через коригування методології та емоційну втому
Високий рівень медіаграмотності	7%	31%	Значне зниження через адаптацію до медіаландшафту
Вищий за середній рівень	65%	50%	Зростання порівняно з довоєнним періодом
Регулярна перевірка інформації	40%	48%	Зниження активності через емоційну втому
Використання практик цифрової безпеки	32%	38%	Низький рівень обізнаності з двофакторною автентифікацією та VPN
Обізнаність із ШІ	25%	Н/Д	Низька здатність ідентифікувати контент, створений ШІ (60% не можуть визначити)

Укладено автором на основі [70].

Ці виклики підкреслюють необхідність комплексного підходу до зміцнення когнітивної безпеки, який би включав не лише технічні, але й соціально-освітні заходи, спрямовані на підвищення медіаграмотності та цифрової компетентності населення. Особлива увага має приділятися співпраці

з міжнародними партнерами та технологічними компаніями для створення ефективних механізмів моніторингу й блокування дезінформаційних мереж.

Ми здійснили порівняльний аналіз стратегій когнітивної безпеки США та Естонії, який дозволяє оцінити їхні підходи до протидії інформаційним загрозам і зміцнення легітимності влади через підвищення довіри, прозорості та стійкості інформаційного простору. США зосереджуються на реактивних заходах протидії дезінформації через інституційну координацію та технологічні інструменти [220; 225; 218], тоді як Естонія використовує цифрове врядування для забезпечення прозорості та залучення громадян, що сприяє когнітивній стійкості [256; 263; 257]. Обидва підходи мають сильні та вразливі сторони, цінний досвід яких може запозичити Україна.

США застосовують реактивний підхід до когнітивної безпеки, зосереджений на виявленні та нейтралізації дезінформаційних кампаній. Агентство кібербезпеки та безпеки інфраструктури (CISA) у складі Департаменту внутрішньої безпеки (DHS) координує зусилля з протидії іноземним і внутрішнім інформаційним загрозам, використовуючи аналіз соціальних мереж і стандартизовану термінологію (IC Lexicon) для ідентифікації маніпулятивних тактик, таких як фальшиві персони, deepfakes і астротурфінг. CISA проводить освітні кампанії для підвищення медіаграмотності, зокрема щодо розпізнавання ботів і синтетичних медіа [220]. Проте фрагментація міжвідомчої координації та відсутність єдиної стратегії, як зазначено у звіті DHS (2022), знижують ефективність протидії інформаційним загрозам [257]. Звіт GAO (2024) підкреслює потребу в чіткому визначенні провідної агенції для уникнення дублювання зусиль [225].

Естонія, відома як «цифрова держава», демонструє проактивний підхід до когнітивної безпеки через цифрове врядування, прозорість і залучення громадян. У 2023 р. 83% громадян висловили задоволеність адміністративними послугами (вище за середній показник ОЕСР 66%), а довіра до національного уряду становила 38% (близько до середнього ОЕСР 39%) [256]. Високий індекс цифрового врядування (DGI) у 2022 р. (0,74 проти 0,61 ОЕСР) відображає

сильний дата-орієнтований підхід, який сприяє прозорості та зменшує вразливість до маніпулятивних наративів [256]. Крім того, OGD відіграють ключову роль у кризовому управлінні, зокрема під час пандемії COVID-19, через ко-креацію даних із громадянами, що підвищує довіру та суспільну єдність [256]. Однак, на місцевому рівні лише 15% муніципалітетів (12 із 79) публікують OGD через організаційні, технологічні та правові бар'єри, що обмежує прозорість у локальному вимірі [264].

Стратегії США та Естонії є комплементарними: США зосереджуються на реактивній боротьбі з дезінформацією, тоді як Естонія будує стійкість через прозорість, цифрове врядування та ко-креацію. США мають перевагу в технологічній зрілості, але страждають від координаційних прогалин. Естонія демонструє сильну інституційну інтеграцію на національному рівні та високий рівень довіри до адмінпослуг, але стикається з викликами на місцевому рівні через бар'єри OGD [264]. Ко-креація даних, як показано в кризовому управлінні, є унікальним елементом естонського підходу, що підсилює залучення громадян і зменшує дезінформаційні ризики. Обидва підходи сприяють легітимності влади, але їхня ефективність залежить від подолання специфічних бар'єрів (Табл. 4.2).

Таблиця 4.2

Порівняльний аналіз стратегій когнітивної безпеки США та Естонії

Критерій	США	Естонія
Базовий підхід	Реактивна протидія дезінформації через технології та координацію	Проактивна прозорість через цифрове врядування, OGD і ко-креацію
Інституційна координація	Помірна (3/5): фрагментація через відсутність єдиної стратегії	Висока (4/5): централізоване цифрове врядування, але слабка локальна інтеграція

Продовження Табл.4.2.

Технологічна зрілість	Висока (4/5): AI, аналіз соцмереж, стандартизована термінологія	Висока (4/5): DGI 0.74, дата-орієнтований підхід
Медіаграмотність	Активні кампанії (4/5): освіта про deepfakes, боти, конспірологічні теорії	Обмежена (3/5): фокус на прозорість і ко-креацію, але брак цільових програм
Довіра до інститутів	Помірна (3/5): брак даних про загальну довіру, фокус на безпеку	Висока до адмінпослуг (4/5): 83% задоволення, 38% до уряду
Бар'єри	Фрагментація координації, невизначеність провідної агенції	Організаційні, технологічні, правові бар'єри на місцевому рівні (15% муніципалітетів з OGD)
Вплив на легітимність	Помірний (3/5): зміцнення через протидію дезінформації, але обмежена координація	Високий (4/5): прозорість, ко-креація та цифрове врядування зміцнюють довіру

Укладено автором на основі [264], [261], [263].

Примітка: Оцінка за шкалою від 1 (низький) до 5 (високий).

Проаналізувавши досвід США та Естонії, можемо виокремити такі рекомендації для України:

1. *Інституційна координація:* створення централізованого органу для протидії дезінформації, подібного до CISA, з чіткою стратегією.

2. *Технологічний розвиток:* впровадження AI-інструментів для моніторингу дезінформації та створення цифрових платформ за естонським зразком для прозорості.

3. *Медіаграмотність:* розробка освітніх кампаній для розпізнавання дезінформаційних тактик, таких як deepfakes і астротурфінг.

4. *Прозорість і ко-креація:* впровадження OGD і механізмів ко-креації для залучення громадян, як під час кризового управління в Естонії.

5. *Локальний рівень:* подолання бар'єрів OGD на місцевому рівні через навчання та ресурси для муніципалітетів.

6. *Співпраця з приватним сектором:* посилення партнерства з технологічними компаніями для моніторингу та нейтралізації дезінформаційних мереж.

США та Естонія демонструють комплементарні підходи до когнітивної безпеки: реактивний (протидія дезінформації) та проактивний (цифрове врядування, OGD, ко-креація). Для України ключовим є інтеграція цих стратегій через створення міжвідомчого органу, розвиток цифрової інфраструктури, підвищення медіаграмотності.

Запропонована модель інтеграції когнітивної безпеки спрямована на зміцнення легітимності політичної влади в Україні через захист когнітивного простору від дезінформації та підвищення довіри громадян до державних інститутів у контексті гібридної війни та внутрішніх викликів, зокрема корупції, яка залишається головною внутрішньою проблемою після зовнішньої загрози – росії [216]. Модель поєднує організаційні, технологічні та соціальні механізми, адаптовані до українських реалій, таких як низька медіаграмотність і фрагментація зусиль, та спирається на міжнародний досвід США та Естонії. Вона протидіє маніпулятивним наративам, що підривають сприйняття легітимності влади, сприяючи формуванню суспільної довіри та антикорупційної культури.

Варто зазначити, що Україна вибудувала багаторівневу систему стратегій когнітивної протидії на державному, суспільному та індивідуальному рівнях. Так, державний рівень представлений діяльністю РНБО, ЦПД, Центру стратегічних комунікацій, які здійснюють моніторинг та спростування дезінформації, а також ведуть власні стратегічні комунікації. Суспільний рівень представлений діяльністю незалежних медіа та фактчекінгових організацій (StopFake, VoxCheck, «Детектор медіа»), які відіграють ключову роль у верифікації інформації. Індивідуальний рівень – це підвищення медіаграмотності та критичного мислення громадян через освітні програми [73,

с. 50]. Ефективність цієї системи є високою, але вона потребує постійної адаптації до нових методів агресора.

Організаційний механізм передбачає створення Міжвідомчого центру протидії дезінформації при Кабінеті Міністрів України, що забезпечить координацію зусиль державних інституцій, таких як Служба безпеки України, Міністерство цифрової трансформації та Центр протидії дезінформації при РНБО. Центр уніфікує стратегії протидії дезінформації, зокрема про корупцію, яка підриває довіру до влади. Модель Департаменту внутрішньої безпеки США (DHS) демонструє ефективність централізованого підходу, тоді як прогрес України в антикорупційних реформах, визнаний міжнародними партнерами, зміцнює легітимність через інституційну прозорість.

Технологічний механізм можливий через впровадження цифрових платформ, інтегрованих із сервісами, за аналогом платформи «Дія», забезпечить прозору комунікацію, знижуючи вплив дезінформаційних наративів про корупцію, що послаблюють легітимність. Естонський досвід цифрового врядування, який підтримує прозорість і довіру, є орієнтиром. Інструменти штучного інтелекту для моніторингу інформаційного простору в реальному часі дозволять виявляти маніпуляції, спрямовані на підрив сприйняття влади. Прогрес у цифровізації антикорупційних механізмів, таких як ProZorro, підкреслює потенціал технологій для зміцнення довіри та легітимності.

Соціальний механізм пропонує партнерство з громадянським суспільством, зокрема організаціями StopFake, VoxCheck і Detector Media, і сприятиме розвитку медіаграмотності, допомагаючи громадянам розпізнавати дезінформацію про корупцію, яка підриває легітимність. Освітні програми для шкіл, держслужбовців і місцевих громад формуватимуть когнітивну стійкість. Естонський досвід ко-креації відкритих державних даних (OGD) показує, як залучення громадян підвищує довіру. Подолання бар'єрів OGD на місцевому рівні потребує додаткових ресурсів, але сприяє антикорупційній культурі, що є основою легітимності.

Інтеграція механізмів обґрунтовує синергію організаційної координації, цифрових технологій і суспільної участі та створює екосистему когнітивної безпеки, яка протидіє дезінформації і корупційним наративам, зміцнюючи легітимність політичної влади. Централізоване управління забезпечує стратегічну єдність, ШІ та платформи – захист від маніпуляцій, а медіаграмотність – суспільну стійкість. Модель адаптована до українських викликів, зокрема низької медіаграмотності та високих корупційних ризиків, і підтримує європейську інтеграцію, що є фактором легітимності.

Ефективність заходів когнітивної безпеки у зміцненні легітимності політичної влади можна простежити через динаміку громадської довіри до ключових інституцій у 2023–2025 роках. Зокрема, дані Центру Разумкова та групи «Рейтинг» засвідчують, що стабільно найвищу довіру отримують Збройні сили України (93–95%), тоді як політичні інститути демонструють поступове падіння показників. Для порівняння, у 2023 р. довіра до Президента становила 83,3%, але вже у 2025 р. знизилася до 57,5%, а рівень підтримки Верховної Ради впав із 34,9% до 17,8% відповідно (Додаток Г). Подібні тенденції фіксуються і щодо Кабінету Міністрів та антикорупційних органів. Узагальнені показники наведено в Табл. 4.3.

Таблиця 4.3

Динаміка довіри до ключових інституцій та акторів у контексті когнітивної безпеки у 2023–2025 рр.

Інститут	2023	2024	2025	Деталізація динаміки
ЗСУ	93.0%	95%	93.5%	Стабільно висока довіра, результат прозорої комунікації та патріотичного *«connective narrative»*.
Президент	83.3%	69%	57.5%	Поступове падіння довіри через корупційні наративи та управлінські проблеми.
Кабінет Міністрів	39.4%	35%	22.5%	Зниження легітимності, що підкреслює потребу в

Продовження Табл.4.3

				технологічних механізмах прозорості.
Верховна Рада	34.9%	21%	17.8%	Поглиблення кризи довіри через скандали та слабку комунікацію.
Антикорупційні органи	~27.8%	Н/Д	~20.2%	Сприйняття неспроможності долати системну корупцію.
Громадські організації	61.1%	Н/Д	60.5%	Стабільна підтримка, що відображає запит на горизонтальні механізми довіри.
Волонтерські організації	81.7%	Н/Д	80.0%	Лідери суспільної довіри; ключова роль у когнітивній мобілізації.

Укладено автором на основі [131-132; 252].

Як показує таблиця 4.3, рівень довіри до силових і громадських структур залишається стабільно високим, що свідчить про їхню ключову роль у підтриманні когнітивної безпеки. Водночас падіння довіри до політичних інститутів демонструє, що самі по собі комунікаційні кампанії не є достатніми: без технологічних інструментів прозорості, системної боротьби з корупцією та розбудови довіри до державних інституцій легітимність влади продовжуватиме знижуватися. Таким чином, емпіричні дані підтверджують необхідність інтеграції організаційних, технологічних і соціальних механізмів у модель когнітивної безпеки України.

Когнітивна безпека є критично важливим інструментом формування та збереження легітимності політичної влади в Україні в умовах гібридної війни, інформаційних загроз і соціально-економічної нестабільності. Емпіричні дані за 2023–2025 рр. підтверджують високу довіру до Збройних сил України та волонтерських організацій, що зумовлено ефективністю децентралізованого стратегічного наративу соціальних медіа, який включає 57% неофіційних повідомлень про героїзм і самодопомогу. Натомість зниження довіри до

Президента, Кабінету Міністрів, Верховної Ради та антикорупційних органів відображає стійке сприйняття корупції як системної проблеми та брак ефективної координації у протидії дезінформації. Проросійський наратив, що спирається на централізовану пропаганду, не резонує з українцями через слабку автентичність.

Запропонована модель інтеграції когнітивної безпеки в державну політику передбачає створення міжвідомчих центрів протидії дезінформації за зразком США, розвиток цифрових платформ, таких як ProZorro та «Дія», для підвищення прозорості, та партнерство з громадянським суспільством, як-от: StopFake і VoxCheck, для зміцнення медіаграмотності. Досвід Естонії в ко-креації відкритих державних даних підкреслює важливість залучення громадян для відновлення довіри. Основними викликами для України залишаються обмежені ресурси для медіаосвіти, низький рівень міжвідомчої координації та стійке сприйняття корупції. Впровадження запропонованої моделі може підвищити довіру до державних інститутів, зміцнюючи легітимність влади через прозору комунікацію, суспільну участь і протидію маніпулятивним наративам.

4.2. Вплив національної ідентичності на формування когнітивної безпеки українського суспільства: політико-інформаційні аспекти

Війна засвідчила, що стійкість спротиву агресору значною мірою залежить від ідентичності населення як інформаційно-політичного складника в структурі когнітивної безпеки українського суспільства. Український народ загартовується, проходячи спільне випробування, і це призводить до значних позитивних трансформацій та змін у суспільстві. Однак вплив маніпулятивних технологій та викривлення інформації з боку рф продовжується. З початком війни за Незалежність України та окупацією Криму питання національної ідентичності та формування когнітивної безпеки ідентичності актуалізувалися з особливою гостротою.

Існування та сталий розвиток Української держави не можливі без загального усвідомлення громадянами своєї національної ідентичності, що бере початок від ототожнення себе з українським народом. Відчуття такої належності через мову, традиції, цінності безпосередньо позначається на житті кожної людини. На думку І. Монолатія, ідентичність традиційно розглядається як процес самоідентифікації індивіда з певними територіальними спільнотами чи соціальними групами. Територіальна (регіональна) ідентичність має складну багаторівневу структуру, серед основних різновидів якої виокремлюють політичну (що в західній політологічній традиції часто позначається як національна) та етнічну. Взаємовідносини між цими двома формами є доволі складними: у певних випадках першочергово формується етнічна ідентичність, а згодом виникає потреба в її інституційному, зокрема державному, закріпленні [115, с. 157; 114; 116].

Сукупність усіх індивідів, які пройшли таке самовизначення, є необхідним фундаментом для формування потужного громадянського суспільства, сильної нації та міцної держави. Саме українська ідентичність є визначальним підґрунтям становлення демократичних основ життя суспільства та української національної держави [10, с. 144], а також протидії в інформаційній та когнітивній війні ворога.

Принагідно зауважимо, що інформаційна війна – це «операція, яка проводиться з метою отримання інформаційної переваги над супротивником. Вона полягає в контролі власного інформаційного простору, захисті доступу до власної інформації при отриманні та використанні інформації опонента, знищенні його інформаційних систем, порушенні інформаційного потоку» [253]. Натомість когнітивна війна передбачає інформаційну війну, наступальні кібероперації та психологічні операції. Це до певної міри міждисциплінарний підхід, що поєднує соціальні науки та нові технології з метою вплинути на процеси розуміння та ухвалення рішень, зламати евристику людського мозку в головній спробі, а саме – «виграти війну ще до її початку». У всіх війнах використовується пропаганда, але когнітивна війна відрізняється від традиційної

тим, що до цього впливу масову аудиторію залучають непомітно, у результаті люди починають активно сприймати нав'язаний інформаційний контент. Це певна революція, бо поєднується використання психічних упереджень, рефлексивного мислення, вплив на ухвалення рішень через перешкоджання діям на індивідуальному та колективному рівнях [97, с. 123].

Когнітивний простір людини заснований і багато в чому організований на його ідентичності. Люди реагують не просто на факти, а на моделі в головах, і якщо вони ставляться під сумнів, то це найбільш важливо для людини. Коли ідентичність виявляється під загрозою, люди жорсткіше захищають свої погляди і не приймають не схожих на них. Коли ж ідентичність підтримується, люди спокійніше ставляться до нових ідей [11, с. 172]. Інформаційна агресія російської федерації проти України передбачає проведення когнітивної війни, яка розвалює українську суспільну свідомість. Через залучення когнітивних методів впливу фрагментується колективне світосприйняття, а тому стає можливим просування стратегічно-орієнтованих пропагандистських наративів держави-агресора. Вони базуються на глобальних аспектах функціонування російської державності і створенні моделей, за яких такі аспекти стануть прийнятними для українського суспільства. У межах війни за Незалежність України можна виокремити багато суспільних верств та шляхів впливу на них. Сегментація відбувається за віком, соціальним статусом, рівнем освіти, географічними показниками, приналежністю до соціальних чи політичних груп, гендером тощо. Наприклад, для дітей когнітивний ефект виражається в нав'язуванні стереотипів поведінки. Як наслідок, розмивається українська ідентичність і дитина не може критично осмислити всю отриману інформацію, і тому вона або помилково ідентифікує себе з російським світоглядом, або потребує часу для переорієнтації в українську модель світосприйняття [172, с. 48]. Розмита національна ідентичність, створена політиками або деякими політичними силами, ідея регіональної відмінності українців заважає об'єднатися нації [90, с. 153].

Зазначимо, що 1 січня 2023 року набув чинності Закон України «Про основні завдання державної політики у сфері підтвердження української

національної та громадянської ідентичності», який уперше в історії незалежної України визначив мету, завдання, принципи, напрями, особливості формування та реалізації державної політики у сфері утвердження української національної та громадянської ідентичності як складника забезпечення національної безпеки України, а також гарантії участі громадян України, закордонних громадян, громадських об'єднань та інших інститутів громадянського суспільства в її реалізації. Українську національну ідентичність у вказаному законі законодавець визначає як стійке усвідомлення особою належності до української нації як самобутньої спільноти, об'єднаної назвою, символами, географічним та етносоціальним походженням, історичною пам'яттю, комплексом духовно-культурних цінностей, зокрема українською мовою і народними традиціями [147].

Утвердження української національної ідентичності громадян є одним з основних елементів формування здатності держави протистояти внутрішнім і зовнішнім безпековим загрозам, а отже, набуває особливого значення для сфери національної безпеки й оборони. Досвід боротьби за державність і територіальну цілісність, який сьогодні проживає Україна, є унікальним, а тому адаптація міжнародних практик для розв'язання наявних проблем є неможливою. При цьому питання формування української національної ідентичності не може піддаватися впливу з боку міжнародних партнерів, а отже, є об'єктом державної підтримки та регулювання [156].

Суттєвий вплив на соціально-економічну ситуацію в державі, а відповідно і на формування національної свідомості в цілому та її регіонах протягом останніх років чинять такі виклики і загрози, як збройна агресія держави-окупанта проти України, тимчасова окупація частини території України, демографічна криза, епідемічна ситуація, проблеми у сферах освіти, науки, культури, відсутність єдиної системи національно-патріотичного виховання в регіонах. Зазначені виклики і загрози здійснюють деструктивний вплив на процес досягнення єдності в українському суспільстві, розвиток свідомого демократичного суспільства та провокують суперечності соціокультурного, регіонального

характеру. Як наслідок – наявність у суспільній свідомості розбіжностей про історичне минуле нації, що створює підґрунтя для просування несумісних із незалежністю держави місцевих ідентичностей та мовних конфліктів [156].

Концептуалізація феномену ідентичності чітко окреслює коло загроз і викликів для національної безпеки в умовах російської агресії, спрямованої на окупацію території України з подальшим посиленням ризиків, пов'язаних із нівелюванням ознак національної, громадянської, культурної, релігійної ідентичності українців [82].

Основою, зокрема і для української національної ідентичності, є спільна історія, спільна культура й мова, відчуття необхідності колективного спільного майбутнього як спільної економічної, соціальної, культурної тощо діяльності, що є ключовими чинниками, які містять консолідаційний потенціал для суспільства. Продуктом взаємодії цих ключових чинників та водночас гарантом їхнього існування є українська держава, адже без такого усвідомлення та культивування український національний рух, а значить, і українська держава як результат його зусиль і боротьби, були б неможливими. Водночас держава має спрямовувати перманентні зусилля на підтримку функціонування тих інститутів, діяльність яких прямо чи опосередковано спроєктована на культивування та примноження спільних для суспільства цінностей [52, с. 35]. Зауважимо, що відповідно до чинного законодавства основними суспільно-державними (національними) цінностями України є:

1) соборність – єдність, неподільність усіх територій України, духовна єдність українців, які проживають на території України, а також єдність усіх громадян України незалежно від національності та віросповідання, спрямована на утвердження справжнього суверенітету й незалежності України, побудову демократичної національної держави;

2) самобутність – національна ідентичність, неповторність, оригінальність, які виявляються окремою особою чи групою осіб у ментально обумовленому художньо-мистецькому світосприйнятті, національно прийнятних способах

спілкування, діяльності, поведінки. Самобутність українського народу визначається його історією, культурою, традиціями та українською мовою;

3) воля – здатність, намір, кероване намагання, прагнення досягти мети. Проявом волі українського народу є героїка боротьби за незалежність України, прагнення до самостійності, невпинний пошук шляхів досягнення свободи;

4) гідність – відстоювання своїх духовно-моральних і державницьких позицій, усвідомлення власної ваги та громадянського обов'язку у міжнародному співтоваристві [147].

Стійкість української держави залежить від цих чинників, позаяк саме вони створюють та утримують консолідаційний потенціал суспільства. Цей потенціал, зі свого боку, значною мірою залежить від наявності в людей колективного відчуття необхідності бути разом, готовності до спільної взаємодії щодо спільного майбутнього. При цьому така взаємодія є можливістю застосування усього арсеналу способів громадянської активності в умовах сучасної демократії та сучасних глобальних комунікацій [52, с. 35].

Національна ідентичність інтегрує суспільство для протидії зовнішньому ворогу, включає складні елементи культури, які формувалися впродовж багатьох поколінь. Національна ідентичність в умовах війни дозволяє зберігати групову цілісність і здійснювати вплив на громадськість із погляду їхньої етнонаціональної відмінності від ворога. Посилення відчуття національної належності дасть можливість у близькій і далекій перспективі мобілізувати українців для протидії збройній агресії, післявоєнної відбудови та залучення людей, які перебувають у вимушеній міграції, до колективної діяльності українців як етнонаціональної групи [163, с. 91]. Спільне використання національної ідентичності має тенденцію сприяти соціальній згуртованості, формувати довіру та солідарність.

Слід відзначити, що, на думку багатьох українських дослідників, національна ідентичність не є вродженою, а є результатом соціалізації особистості, а тому не дивно, що вона може змінюватися під впливом соціокультурних, політичних, етнічних та інших чинників. Зокрема, йдеться про

ідентифікацію, яка пов’язана з певною територією, мовними особливостями, соціальним статусом тощо [264, с. 26-42]. На наш погляд, національна ідентичність у всіх випадках завжди складається з двох частин. Одна частина – це успадкована ідентичність, незалежно від того, який конкретний фактор успадкування це може бути, наприклад, мова, етнічна приналежність, віра тощо. Інша частина національної ідентичності завжди є сучасною, розвивається та перебуває в стані зміни, тому що спосіб життя та характеристики людей неминуче залежать від конкретних місць, де вони проживають, від дії міжнародних, регіональних, національних та місцевих умов, які впливають на їхні засоби до існування та їхню культуру. Таким чином, значна частина національної ідентичності змінюється непомітно та поступово з часом: вона не є фіксованою чи статичною.

Поділ на «своїх» і «чужих» відбувається на різних рівнях, залежно від особистних меж і критеріїв. У територіальних межах «чужим» буде той, хто знаходиться далі, у соціальних – хто займає найвищий / найнижчий статус, у культурних – хто має відмінності в традиціях, фольклорі тощо. Тобто «чужий» визначається наявністю або відсутністю спільних рис. У цьому складному процесі задіяні як органи чуття людини, так і її психіка, а також чинники, які стали домінантними в процесі формування її ідентичності, пріоритетні цінності тощо. Науковці наголошують на тому, що для українців мова не є об’єднувальним фактором у процесі формування нації, навпаки, вона роз’єднує, адже титульною мовою в різних регіонах є різні мови – українська та російська. Ідентифікація в цьому випадку відбувається на рівні мови – носій іншої мови є чужим. При цьому українці не враховують ні спільного громадянства, ні спільної території, ні принципово спільної релігії, ні багатьох інших чинників, що визначають національну ідентичність [264, с. 27]. Однак слід відзначити, що із початком повномасштабного вторгнення рф на територію України ситуація неабияк змінилася.

Слід також відзначити, що обов’язковою умовою збереження національної ідентичності є національна самосвідомість. Національна свідомість формується

навколо усвідомлення причетності людини до роду і соціальної групи, наявних як факт існування певної культурної системи. Історія засвідчує: національність у свідомості – це виявлення часового модусу буття людини жити не тільки тепер, у цю мить, а й завтра – у перспективі. Вона формується на основі знання мови, історії, культури, розуміння власної ментальності та ментальності інших народів Посягання на національну самосвідомість здійснюється уже напрацьованими століттями ефективними засобами впливу, такими як «гібридні війни», задіяння «м'якої сили», застосуванням концепції «організованого хаосу» та інші. Інколи подібні засоби впливу маскуються під загально-позитивні процеси наднаціонального рівня, такі як «культурне чи економічне співробітництво», «занепокоєність дотриманням прав і свобод якоїсь частини населення», «ініціативи щодо розвитку науки і освіти» країни впливу тощо. Одним із напрямків такого тиску можна назвати впровадження у свідомість населення цінностей і принципів ерзац-культури індивідуальності та поділ суспільства на окремі елементи, позбавлені національної самобутності. Мультикультуралізм, на нашу думку, є чи не найефективнішим засобом руйнування національного духу. Він призначений для підриву ідеї національної держави, що може призвести до руйнування самого громадянського суспільства. Результатом розпаду громадянського суспільства може стати війна «всіх проти всіх». Це небезпечно не тільки для окремого народу, а й для всього людства. Люди, позбавлені відповідного їхній національній природі світорозуміння, змушені будуть існувати в постійних протиріччях між формою поведінки, яка їм нав'язується, і потребами національного самовираження, а отже, для знищення визначеної держави не потрібен буде насильницький переворот, достатньо «перевороту» У свідомості людей, після якого вони не бажатимуть підкорятися державній владі [92, с. 87].

Національна ідентичність є не менш важливим чинником безпечного існування нації, ніж національна територія та національне багатство. Як слушно з цього приводу зауважується у науковій літературі, саме завдяки національній самосвідомості й інстинкту національного самозбереження будь-яка

життєздатна нація прагне продовження своєї самобутньої еволюції. Кожна нація дбайливо оберігає свою територію та політичну незалежність, але якщо з якихось причин вона їх втратила, то мова, культура, писемність і релігія стають основними об'єднувальними чинниками [92, с. 83]. Від змісту і характеру національної ідентичності (-ей) значною мірою залежить як характер розвитку відносин у суспільстві між різними групами населення, так і майбутнє держави загалом. Від того, чи населення певної держави ідентифікує себе, свої інтереси з державними, чи держава розуміється як перешкода для реалізації політичних, економічних, культурних, етнічних, релігійних, мовних тощо інтересів, безпосередньо залежить територіальна цілісність країни, стан взаємин між різними групами населення, міра консолідованості та сприйняття суспільством власного майбутнього в межах певної держави, повага й довіра до державних інституцій, законів, символів тощо. Можна стверджувати, що більшість внутрішньополітичних проблем, з точки зору безпеки, відбувається переважно через кризу національних ідентичностей [52, с. 20-21].

У результаті проведеного дослідження встановили, що національна ідентичність має вагомий вплив на формування інформаційної та когнітивної безпеки українського суспільства. Вона інтегрує суспільство для протистояння зовнішньому ворогу та включає елементи культури, що розвивалися протягом багатьох поколінь. Національна ідентичність допомагає підтримувати єдність групи та впливати на громадськість, підкреслюючи їхню етнонаціональну відмінність від супротивника.

Існування та розвиток Української держави не можливі без усвідомлення громадянами своєї громадянської ідентичності, що починається з ототожнення себе з українським народом. Відчуття приналежності, яке формується через мову, традиції та цінності, безпосередньо впливає на кожного з нас. Сукупність усіх, хто пройшов таке самовизначення, становить необхідний фундамент для формування сильного громадянського суспільства, міцної нації та стабільної держави. Українська ідентичність є ключовим підґрунтям для розвитку демократичних основ життя суспільства та національної державності. Спільне

використання національної ідентичності має тенденцію сприяти соціальній згуртованості, формуючи довіру та солідарність.

4.3. Формування когнітивної стійкості (резильєнтності) в суспільстві як компоненту когнітивної безпеки в сучасній Україні

Через стрімку цифровізацію парадигма національної безпеки зазнає докорінної трансформації і виходить за межі класичних вимірів військової, політичної та економічної стабільності. Усе більшого значення набуває когнітивна сфера суспільства – простір, у якому формуються спільні смисли, цінності, судження та колективна ідентичність. Саме ця сфера стала центральним фронтом гібридних конфліктів нового покоління, де інформаційно-психологічний тиск реалізується з не меншою стратегічною вагою, ніж класичні військові засоби.

У сучасних кризових умовах істотно зростає сукупність ризиків і загроз, пов’язаних із забезпеченням задоволення базових соціальних потреб та реалізацією соціально значущих інтересів громадян, а також із підтриманням стабільності соціального життя населення. Збройні конфлікти на території України виступають потужним дестабілізувальним чинником, який не лише актуалізує наявні соціальні проблеми, але й поглиблює структурні диспропорції в соціальній сфері.

Зокрема, фіксується стійка тенденція до зростання рівнів бідності та безробіття, посилення майнової диференціації населення і розширення масштабів соціальної нерівності. Водночас процеси масової внутрішньої міграції зумовлюють загострення проблем доступності та якості освітніх, медичних і соціальних послуг, що негативно позначається на рівні соціальної інтеграції та соціальної згуртованості суспільства. Паралельно спостерігається зниження якості життя населення, підвищення рівня соціальної напруженості та зростання конфліктного потенціалу, що створює додаткові виклики для стабільності соціальної системи.

В умовах поглиблення кризових явищ істотно зростає потреба у комплексній соціальній, гуманітарній і психологічній підтримці населення, спрямованій на мінімізацію негативних наслідків соціально-економічних та воєнних потрясінь. Ефективність подолання зазначених проблем безпосередньо залежить від результативності, системності та своєчасності реалізації державної інформаційної та гуманітарної політики, а також від рівня координації зусиль органів державної влади з інститутами громадянського суспільства та міжнародними організаціями, спроможними сприяти стабілізації соціальної ситуації в Україні.

Оскільки сукупність окреслених суспільних ризиків має потенціал трансформації в загрози національній безпеці, спостерігається тенденція до кумулятивного зростання ризиків у сфері національної безпеки загалом.

Доцільно констатувати наявність системної проблеми у сфері забезпечення безпеки українського суспільства, зумовленої відсутністю цілісної та комплексної стратегії протидії ментальній і когнітивній агресії, а також нестачею ефективних механізмів контрдій у межах психологічної війни, спрямованої проти України. Недостатня узгодженість державних і суспільних зусиль у цій сфері знижує рівень стійкості соціуму до деструктивних інформаційно-психологічних впливів та посилює вразливість когнітивного простору.

Подолання зазначеної проблеми можливе за умови застосування принципу, відповідно до якого «гібрид сил нападу на країну має протистояти гібрид сил захисту» [40]. Ключовим елементом таких протистоянь є когнітивна війна – комплексна діяльність, спрямована на зміну сприйняття реальності, маніпулювання емоційними станами та підрив здатності суспільства до колективного опору. Відповіддю на цю загрозу виступає не лише когнітивна безпека, а й формування суспільної стійкості (резильєнтності) – здатності спільноти чинити опір інформаційному тиску в умовах тривалого гібридного протистояння. У практичному вимірі це означає, що в умовах воєнного конфлікту критично важливою є інтеграція зусиль усіх елементів сектору безпеки й оборони, державних інституцій та громадянського суспільства. Такий

синергійний підхід дозволяє сформувати цілісну систему протидії когнітивним загрозам, забезпечити ефективний захист суспільної свідомості та підвищити рівень національної стійкості в умовах гібридної війни.

Повномасштабна фаза війни за Незалежність України, що триває з лютого 2022 р., перетворила Україну на полігон відпрацювання найновіших технологій когнітивного впливу. Інтенсивність інформаційно-психологічних операцій, спрямованих на підрив суспільної єдності та деморалізацію населення, значно посилилась.

Наявність постійних загроз безпеці людини зумовлює формування специфічного психологічного стану українського суспільства та відповідних емоційно-психологічних настроїв (Додаток Ґ) . За результатами соціологічних досліджень, проведених у вересні 2022 року [159], домінантними емоційними станами серед населення стали напруженість (42%), надія (41%) та втома (41%), що відображає одночасне поєднання мобілізаційних і виснажувальних чинників суспільного буття в умовах війни.

До другої групи за поширеністю належать такі емоційні стани, як страх (26%), гнів (24%) і гордість (22%), які свідчать про високий рівень емоційної поляризації та реакції на воєнні події. Третю позицію посідають роздратування (21%), обережність (20%), безсилля (19%) і розгубленість (17%), що відображає зростання психологічної вразливості окремих соціальних груп та ускладнення процесів адаптації до тривалого кризового середовища.

Водночас від 11% до 14% респондентів демонструють більш глибокі негативні емоційні стани, зокрема відчай і водночас готовність до дії (14%), відчуття розчарування (13%) та гостре переживання самотності (11%).

Найбільш оптимістично українці оцінювали перспективи подолання проблем і труднощів наприкінці 2022 – на початку 2023 р. (наприклад, у лютому-березні 2023 р. 49% вважали, що Україна здатна подолати наявні проблеми і труднощі протягом найближчих кількох років, 36% – що вона здатна це зробити в більш віддаленій перспективі, і лише 3% – що взагалі не здатна їх подолати). Після цього рівень оптимізму зменшувався – у червні 2024 р. ці показники

становили відповідно 29%, 46% і 11%, хоч оптимізм усе одно був вищим, ніж у довоєнному 2021 р. [62, с.19].

Сукупність наведених показників засвідчує складний і багатовимірний характер психологічного стану українського суспільства, що формується під впливом безпекових загроз та тривалого воєнного протистояння, і має безпосереднє значення для аналізу когнітивної безпеки та суспільної стійкості.

Інформаційно-психологічна стійкість спільноти тісно пов'язана з концептами національної та міжнародної безпеки, однак у сучасних умовах вона дедалі більше набуває когнітивного виміру, що зумовлює необхідність захисту не лише матеріальних ресурсів і територіальної цілісності, а й свідомості, сприйняття та процесів ухвалення рішень як на індивідуальному, так і на колективному рівнях. У цьому контексті когнітивна безпека постає як ключовий елемент стійкості оточення, оскільки саме через інформаційно-психологічні впливи формується уявлення суспільства про загрози, цінності та пріоритети безпеки.

На відміну від політичних візій або стратегічних наративів окремих політичних лідерів, безпекова стійкість у когнітивному вимірі є об'єктивним станом, сформованим сукупністю соціальних взаємодій, інформаційних потоків і комунікативних практик, що значною мірою не залежать від волі окремих акторів. Одним із ключових чинників, що визначають характер когнітивного безпекового середовища, є конкуренція між державами у сфері формування та просування стратегій національної й регіональної безпеки, яка дедалі частіше реалізується через боротьбу за контроль над інформаційним і смисловим простором.

Когнітивний вимір безпекового оточення має виразно динамічний характер, оскільки постійні зміни в технологіях комунікації, інформаційному середовищі та соціальних настроях призводять до трансформації загроз і ризиків. Такі процеси можуть одночасно створювати нові можливості для зміцнення когнітивної стійкості суспільства або, навпаки, посилювати його вразливість до маніпуляцій, дезінформації та психологічного тиску. Саме тому аналіз

когнітивно стійкого оточення, прогнозування його розвитку та розробка механізмів цілеспрямованого впливу на нього є необхідними складниками сучасної політики національної безпеки [37, с. 54].

Когнітивна стійкість людини формується під впливом сукупності зовнішніх і внутрішніх чинників та забезпечується функціонуванням безпечного середовища, яке конструюється як соціумом і державою, так і безпосередньо самою особистістю. Внутрішні чинники безпечного оточення, що залежать від індивіда, охоплюють усвідомлення цінності людського життя, орієнтацію на самозбереження, самозахист і саморозвиток, а також відповідальність за власне життя, здоров'я, добробут й особистий внесок у підтримання загального рівня безпеки. У цьому контексті особливого значення набуває когнітивний вимір безпеки, оскільки саме через свідомість, систему цінностей і здатність до осмислення загроз формується індивідуальна модель безпечної поведінки.

Сучасні соціально-політичні реалії актуалізують проблему забезпечення безпеки людини в умовах підвищеної нестабільності та обмеження традиційних форм життєдіяльності. За таких обставин особливої ваги набуває формування ефективної системи соціальної безпеки, здатної адаптуватися до нових викликів та забезпечити належний рівень захисту прав і життєвих інтересів громадян. Для українського суспільства в сучасних умовах ключовими інструментами гарантування соціальної безпеки особи є комплекс взаємопов'язаних правових, інституційних і поведінкових чинників [94].

До них належать насамперед закони та нормативно-правові акти, спрямовані на закріплення та захист прав і свобод людини та громадянина. Важливу роль відіграє розвиток соціального партнерства й конструктивного діалогу між державними органами, роботодавцями та найманими працівниками, що сприяє зниженню соціальної напруженості та запобіганню конфліктам. Не менш значущим чинником є формування відповідальної та безпечної поведінки громадян, яка виступає передумовою стабільності соціального середовища.

Суттєвим елементом системи соціальної безпеки є функціонування демократичних інститутів громадянського суспільства, здатних забезпечувати

суспільний контроль, представництво інтересів різних соціальних груп та посилення соціальної згуртованості. Зміцнення соціальної єдності, підтримання стабільності та суспільного порядку розглядаються як базові умови зниження ризиків соціальної дестабілізації. Водночас важливого значення набуває чітке визначення критеріїв соціальної підтримки для різних категорій населення, що дозволяє забезпечити адресність й ефективність соціальної допомоги.

Нарешті, вагомим чинником гарантування соціальної безпеки є наявність розгалуженої мережі служб і сервісів, які надають соціальні послуги, а також спрямована підтримка осіб та груп, що перебувають у складних життєвих обставинах та потребують особливого соціального захисту.

Ефективне забезпечення безпеки особи в умовах криз і воєнних конфліктів потребує застосування інноваційних та конструктивних підходів, спрямованих на збереження життя, підвищення здатності витримувати стресові впливи, адаптуватися до нестабільного середовища, а також відновлювати повноцінну життєдіяльність у складних соціально-політичних умовах. Важливим результатом таких підходів є не лише виживання, а й формування потенціалу для подальшого розвитку та активної участі особи в суспільному житті.

Саме ці обставини актуалізують науковий інтерес до проблематики резильєнтності як ключового чинника соціальної та когнітивної безпеки людини. Формування безпеки особи на засадах резильєнтності передбачає усвідомлення її значущості для позитивних трансформацій, оскільки завдяки стресостійкості індивід здатний не лише подолати кризові та воєнні виклики, але й досягати успіху, відновлювати якість життя, мінімізувати негативні наслідки війни та демонструвати спроможність до подальшого розвитку [126, с. 60].

Поняття «резильєнтність» активно інтегрується в соціальні, економічні та психологічні дослідження, водночас його початкове тлумачення походить із фізики, де цей термін означає здатність матеріалу відновлювати початкову форму після деформації, спричиненої зовнішнім тиском. Перенесення цього концепту в гуманітарну сферу дозволяє осмислити резильєнтність як

універсальну властивість особистості й суспільства зберігати цілісність і функціональність в умовах тривалих кризових впливів.

Деякі автори вводять поняття когнітивного опору як вищої форми когнітивної стійкості, тобто здатності населення, військових структур та політичного керівництва зберігати функціональність, критичне мислення й інформаційну стійкість перед маніпуляціями, дезінформаціє. та пропагандистськими атаками [128, с. 354]. Когнітивна стійкість трактується як здатність індивіда, соціальної групи або інституції зберігати спроможність до раціонального аналізу інформації, ухвалення обґрунтованих рішень та ефективного опору зовнішньому маніпулятивному впливу. У сучасному науковому дискурсі цей феномен розглядається як міждисциплінарний елемент, що поєднує аспекти інформаційної, психологічної та стратегічної безпеки.

Когнітивна стійкість охоплює широкий спектр навичок і характеристик, серед яких ключовими є розвинене критичне мислення, інформаційна й цифрова грамотність, здатність до емпатичного розуміння, навички рефлексії, а також довіра до легітимних інституцій, відповідальних за ухвалення управлінських рішень. Саме ці чинники формують індивідуальну та колективну резистентність до дезінформації, когнітивних викривлень і психологічного тиску, що має критичне значення в умовах гібридної війни та когнітивного протистояння (Додаток Д).

У цих умовах формування стійкості до інформаційного тиску стає не другорядним завданням, а стратегічним імперативом безпекової політики, від якого безпосередньо залежить здатність держави зберігати суверенітет та функціональність. Особливої гостроти проблема набуває в контексті масової міграції, інформаційної фрагментації та періодичних вимкнень енергопостачання, що обмежують доступ до достовірних джерел інформації та підвищують вразливість суспільства до маніпулятивних впливів. Використання цифрових платформ, таких як Telegram та TikTok, як каналів поширення ворожих наративів, лише посилює масштаб і швидкість інформаційних операцій і висуває вимогу до швидкої адаптації механізмів захисту.

Важливість розгляду такої проблематики в нашому дослідженні зумовлена гострою потребою в науково обґрунтованому підході до розбудови ефективної системи протидії інформаційному тиску в умовах тривалої гібридної війни. Систематизація міжнародного досвіду, аналіз механізмів інформаційного впливу та розробка стратегії когнітивного суверенітету адаптованої до українського контексту когнітивних атак є критично важливими для збереження національної ідентичності та консолідованості суспільства.

Наше дослідження ґрунтується на комплексній методології, що поєднує якісні та кількісні підходи. Основним методом виступив кейс-аналіз, спрямований на вивчення конкретних проявів когнітивної війни в українському контексті, зокрема кампанії дезінформації навколо «біолабораторій»; використання платформ Telegram, TikTok та X (Twitter) для поширення маніпулятивних наративів; кібератаки на критичну інфраструктуру (енергетичну, фінансову). У дослідженні застосовано соціальний мережевий аналіз (SNA) для виявлення координованої неавтентичної поведінки та бот-мереж, а також контент-аналіз медійних повідомлень і публікацій у соціальних мережах. Емпіричну базу становили дані моніторингових платформ (наприклад, StopFake, EDMO), відкриті статистичні звіти (GLOBSEC, PLOS ONE) та аналітичні звіти міжнародних організацій (NATO ACT, CSIS). Порівняльний аналіз дозволив оцінити ефективність різних інструментів когнітивної безпеки (медіаграмотність, аналітика великих даних, кіберзахист) на різних етапах гібридної агресії (2014-2021, 2022-2023, 2024 і дотепер). Для узагальнення теоретичних засад використано систематизацію наукових публікацій із тематики когнітивної війни та безпеки, а також аналіз нормативно-правових актів України та ЄС у контексті гармонізації законодавства (GDPR, AI Act).

В умовах війни в Україні когнітивна загроза набуває особливої гостроти через фрагментацію інформаційного простору та фізичні обмеження доступу до достовірних даних. Масова міграція населення (понад 6,9 млн біженців та 3,6 млн внутрішньо переміщених осіб) призвела до розриву соціальних зв’язків і виникнення множинних інформаційних середовищ, що посилює групову

поляризацію та ерозію довіри на мезорівні [196]. Додатковим чинником є атаки на енергетичну інфраструктуру, які провокують масштабні блекаути, створюючи інформаційний вакуум. У такому разі прості, емоційно заряджені меседжі, поширювані через цифрові платформи, набувають домінантного впливу, а когнітивна негнучкість, потреба в приналежності та стрес виступають ключовими тригерами маніпуляції.

росія системно застосовує рефлексивний контроль – технологію маніпулювання сприйняттям із метою спонукання цільової сторони до саморуйнівних рішень. З 2014 року маскування атрибуції, кампанії дезінформації через RT і Sputnik, а також атаки на критичну інфраструктуру використовувалися для розмивання циклу OODA (Observe–Orient–Decide–Act), що підривало інформаційну довіру [190].

У 2024-2025 роках ці тактики посилилися через використання штучного інтелекту: отруєння великих мовних моделей, фейкові акаунти та бот-мережі стали інструментом масштабування пропаганди [265; 259]. В окупованих регіонах Херсонщини та Запоріжжя москва вибудувала систему контролю над медіа для створення альтернативної інформаційної реальності [244].

Когнітивна війна не є винятково українським феноменом. Втручання у вибори в США 2016 р., масштабні кампанії дезінформації в Європейському Союзі та використання платформ на кшталт TikTok демонструють універсальність когнітивних операцій [213]. Вони стають частиною глобальної конкуренції в сірій зоні, де дезінформація, deepfakes, штучний інтелект та NBIC-технології посилюють вплив на когнітивну сферу. Як зазначає NATO ACT, ці інструменти дозволяють досягати стратегічних цілей без повномасштабних воєнних дій, атакуючи моральні чинники та здатність суспільств до опору [216; 211].

Стратегічні конкуренти, зокрема росія та Китай, активно інтегрують когнітивні інструменти в комплекс гібридних операцій. Російська практика рефлексивного контролю та китайська система інформаційного протистояння

демонструють, що поле бою зміщується до людської свідомості, а об'єктом атак стає будь-який користувач цифрових технологій.

Когнітивна війна в сучасних гібридних конфліктах ґрунтується на поєднанні низькотехнологічних маніпулятивних методів, таких як поширення дезінформації та психологічні операції з високотехнологічними інструментами, зокрема кібератаками та алгоритмічним посиленням контенту. Такий синтетичний арсенал дозволяє агресорам, зокрема росії, досягати максимального когнітивного ефекту – дезорієнтації населення, поляризації суспільства та підриву довіри до інституцій.

Одним із найяскравіших прикладів стала кампанія навколо так званих «біолабораторій» в Україні. З 2022 року російські медіа та офіційні дипломатичні канали поширювали твердження про існування американських бактеріологічних лабораторій, які нібито розробляють етнічну біологічну зброю, проводять експерименти над військовими та використовують птахів, які мігрують, як «біоносіїв» [261]. Ці наративи інтегрувалися в ширший пропагандистський контекст про «нацизм в Україні», «загрозу від НАТО» та «захист слов'янських народів» і використовувалися для виправдання повномасштабного вторгнення.

Кампанія поширювалася через Telegram, TikTok, X (Twitter) та офіційні дипломатичні акаунти, зокрема російських посольств. Соціальний мережевий аналіз Twitter показав координовану неавтентичну поведінку (КНП) з використанням бот-мереж, що орієнтувалися як на англомовну, так і на російськомовну аудиторію [193]. Telegram-канали, пов'язані з кремлем, збільшили обсяг постів на 119% після початку вторгнення, а середній показник переглядів зріс більш ніж утричі, що вказує на масштабне алгоритмічне посилення наративів [275]. На TikTok кампанії типу #RussianLivesMatter досягали понад 50 млрд переглядів через використання ауді-мемів та відеочеленджів, які стимулювали емоційне залучення аудиторії [206].

Поширення таких наративів не лише створює альтернативну інформаційну реальність, а й викликає емоційні реакції страху, обурення та недовіри, які підривають раціональне мислення та стійкість до маніпуляцій. Як зазначає М.

Армстронг, у добу «нерегулярних інформаційних загроз» дані перетворюються на зброю, яка працює через емоційні тригери, а не лише через зміст повідомлень [194].

Російські психологічні операції зосереджені на цілеспрямованому впливі на емоції, цінності та поведінку. Використовуючи сірі та чорні інформаційні операції (непрямо або фальшиво приписані джерела), PSYOP спрямовані на деморалізацію українського суспільства, виклик відчуття невпевненості й фаталізму, а також розкол між регіонами та соціальними групами [269]. Типовим прикладом є наративи про «етнічну зброю» чи «геноцид», які викликають страх та формують образ зовнішньої загрози.

Когнітивна війна неможлива без високотехнологічного компоненту, який забезпечує масштабування та довготривалість впливу. З 2015 р. росія активно застосовує кібератаки проти критичної інфраструктури України: енергетичних компаній, фінансового сектору, зокрема, атакуючи банківські сервіси. Такі атаки, як BlackEnergy-3 (2015 р.), Industroyer (2016 р.) та Industroyer-2 (2022 р.), а також нові кампанії 2024 р. призводили до масштабних блекаутів і порушення цифрових сервісів, створюючи інформаційний вакуум, який посилює ефект дезінформаційного впливу[191].

Додатково зауважимо, що алгоритмічне посилення через соціальні мережі забезпечує вибухове зростання охоплення: Telegram демонструє найвищі показники взаємодії завдяки низькій модерації та мультимодальному контенту, тоді як TikTok – найвищий рівень емоційного залучення молоді [272]. Дипломатичні канали, попри нижчий обсяг охоплення, забезпечують ефект легітимізації [267]. Дослідження HKS Misinformation Review показало, що відеорозвінчання (*debunking videos*) в TikTok лише частково нівелюють ефект дезінформації, що підкреслює стратегічну ефективність швидких атак першої хвилі [275] (Табл. 4.4).

Таблиця 4.4

Порівняльна ефективність платформ у поширенні інструментів когнітивного впливу у війні за Незалежність України

Платформа	Основний інструмент	Кількісні показники поширення	Рівень координації (КНП)	Якісна оцінка впливу	Специфіка адаптації
Twitter (X)	Неавтентичне посилення (боти)	1,3 млн твітів, 420 тис. користувачів	Високий	Вірусне поширення в нішевих групах	Англомовна/ російська аудиторія
Telegram	Мультимодальні наративи	+119% постів, +323% переглядів	Середній	Високе залучення, мінімальна модерація	Адаптація під BRICS/Африку
TikTok	Аудіомеми, челенджі	36,9 млрд (#Ukraine), 50 млрд (#RussianLives Matter)	Високий	Емоційне залучення молоді	Алгоритмічна персоналізація
Дипломатичні канали	Офіційні наративи	190 тис. коментарів	Низький	Легітимізація наративів	Форум ООН, регіональні адаптації

Укладено автором на основі [275]

Аналіз кейсів показує, що когнітивна війна є багаторівневою системою, у якій маніпулятивні наративи посилюються технологічно, створюючи ефект першого удару. Telegram забезпечує найвищий рівень охоплення завдяки мультимодальності та низькому контролю контенту, TikTok – найвищий емоційний ефект через алгоритмічну персоналізацію, а дипломатичні канали додають легітимізаційний вимір. Синергія цих платформ формує цілісний арсенал когнітивного впливу, що дозволяє агресору досягати стратегічних цілей без прямого військового зіткнення.

Еволюція когнітивної безпеки в Україні відбувалася в тісному зв’язку з етапами гібридної агресії Росії та трансформацією інформаційного середовища.

Від прелюдії гібридної війни (2014–2021 рр.) до повномасштабного вторгнення (2022 – наш час) «м'які» (суспільно-людські) та «жорсткі» (технологічні) інструменти поступово інтегрувалися з нормативно-правовим каркасом, формуючи цілісну систему протидії когнітивним атакам. Цей процес демонструє перехід від реактивних тактик до моделі превентивної стійкості, здатної адаптуватися до еволюціоністських загроз, зокрема штучно інтелектуалізованої дезінформації.

Після анексії Криму та початку війни на Донбасі у 2014 р. Україна опинилася перед новим типом загрози – когнітивними атаками, заснованими на експлуатації історичних, культурних й етнічних наративів, зокрема тез про «історичне братство» та «нацифікацію». У цей період ключовим захисним інструментом стали медіаграмотність і фактчекінг, які заклали фундамент суспільної стійкості.

OSINT-моніторинг фіксував зростання дезінформаційного потоку на понад 300%, що зумовило потребу в масовому просвітницькому навчанні. Ініціативи типу платформи Prometheus стали прототипом системних програм розвитку критичного мислення, охопивши тисячі учасників та знизивши вразливість населення до дезінформації на 15-20% [228]. Водночас платформа StopFake, заснована у 2014 р., еволюціонувала від реактивного спростування до проактивної верифікації з використанням OSINT-інструментів (понад 10 тис. верифікованих фейків до 2022 р.) [221]. Емпіричний аналіз засвідчив суттєвий кореляційний зв'язок між зростанням рівня медіаграмотності та зменшенням поширення фейкових матеріалів (r=0,72), що підкреслило визначальну роль «м'якого» стовпа в ранній фазі когнітивної протидії [250].

З початком повномасштабного вторгнення росії 24 лютого 2022 р. когнітивна війна перейшла у фазу інтенсивної ескалації: з'явилися мультимодальні наративи, AI-згенеровані дипфейки та масштабні бот-мережі. Відповіддю стало активне впровадження технологічних інструментів: систем аналітики великих даних, кібербезпекових рішень та альтернатив інфраструктури зв'язку.

Big Data-аналітика, розгорнута в 2022 р., дозволила виявляти близько 85% скоординованих дезінформаційних кампаній у режимі реального часу, обробляючи мільйони постів [230]. Технологічна стійкість також була підсилена через впровадження Starlink, що забезпечило безперебійний зв'язок 80% критичної інфраструктури під час блекаутів та дало змогу заблокувати понад 70% фішингових атак [241]. Системи розпізнавання діпфейків, такі як SecureVision, досягли 92% точності в гібридних контекстах [237].

Цей період продемонстрував ефективність синергії між технологічними інструментами та суспільними механізмами, особливо на тлі масової міграції понад 6 млн осіб. Водночас були виявлені прогалини в масштабуванні систем швидкого реагування та потреба в міжнародній координації фактчекінгу – понад 2300 матеріалів було перевірено мережею EDMO [224].

З 2024 р. фокус поступово змістився на регуляторно-правову інтеграцію, яка стала системним «третім стовпом» когнітивної безпеки. Україна почала гармонізувати законодавство з європейським правовим полем, інтегруючи General Data Protection Regulation та Artificial Intelligence Act, зокрема через механізми «регуляторних пісочниць» для безпечного тестування нових технологій [188], що забезпечило нормативну базу для синергії між людськими, технологічними та інституційними ресурсами.

Масові програми медіаграмотності охопили понад 33 000 учасників [225], тоді як технологічні рішення інтегрувалися з правовим наглядом, зменшуючи вплив дезінформації на 20-30%. Фактчекінг еволюціонував у міждисциплінарний інструмент: контент-аналіз поєднувався з опитуваннями понад 19 000 респондентів, що дозволило ефективно протидіяти «відбиванню» (*gatebouncing*) пропаганди [250]. Цей період ознаменував перехід до проактивної моделі, де правовий фреймворк виконує роль інтеграційного стрижня між різними стовпами (Табл.4.5).

Таблиця 4.5

Хронологічна типологія трендів еволюції когнітивної стійкості в українському контексті гібридної війни

Період	Домінантний тренд	Ключові ініціативи та метрики	Виклики та адаптації	Внесок у загальну стійкість
2014–2021 (Початкова фаза)	«М'який» (суспільний)	StopFake (10 000+ фейків); Prometheus (тисячі учасників)	Етнічні наративи, обмежена інфраструктура	Базова резилієнтність (–15-20% вразливості)
2022–2023 (Ескалація)	«Жорсткий» (технологічний)	Big Data (85% детекції ботів); Starlink (80% охоплення); 2 300+ EDMO-спростувань	Deepfakes, блекаути, труднощі з аудіовізуалом	Оперативна нейтралізація (скорочення часу реагування до годин)
2024 – наш час (Стабілізація)	Регуляторний (інтеграційний)	Roadmap AI (60% гармонізації з AI Act); міждисциплінарні опитування (19 000+ респондентів)	Мовні бар'єри, масштабованість	Синергетична модель (підвищення ефективності на 20-30%)

Укладено автором на основі [250]

Аналіз цієї хронологічної типології демонструє нелінійну динаміку розвитку когнітивної стійкості. Соціальний фундамент початкової фази забезпечив базову резилієнтність, але без технологічних інструментів вона залишалася переважно реактивною. Етап ескалації показав, що технології здатні швидко компенсувати прогалини, проте потребують нормативного підґрунтя для стійкості. Стабілізаційна фаза забезпечила інтеграцію трьох трендів у єдину систему, де взаємодія між ними (r =0,78) підвищує ефективність протидії на 25-35% – рівень, зіставний із моделями НАТО щодо гібридних загроз.

Когнітивна стійкість в Україні трансформувалася з тактичного інструменту на стратегічний імператив національної стійкості, що поєднує медіаграмотність, технологічну протидію та нормативну координацію. Подальший розвиток цього фреймворку потребує розширення міждисциплінарних досліджень (психологія, нейрокомунікація), підтримки

ментального здоров'я в умовах інформаційного тиску та глобальної кооперації для протидії безкордонним когнітивним атакам.

Ефективність запропонованої моделі когнітивної безпеки детермінована її адаптованістю до специфіки воєнного стану, зокрема фрагментації інформаційного простору та системних енергетичних обмежень. Як свідчить аналіз гібридних операцій з 2022 року, саме комбінація етапних реформ і публічно-приватного партнерства дозволяє не лише мінімізувати ризики дезінформації, але й трансформувати кризові виклики в можливості для системного підвищення стійкості.

Запропонована дорожня карта на 2025–2031 рр. передбачає послідовну реалізацію заходів – від оперативних інтервенцій до довгострокових структурних змін. На першому етапі (2025–2026 рр.) пріоритет відводиться впровадженню заходів із негайним ефектом, таких як масштабування освітніх платформ на кшталт Prometheus для понад 50 тис. учасників із включенням модулів з OSINT-аналітики. Мета-аналіз ефективності подібних ініціатив свідчить про потенційне зниження сприйняття фейкової інформації на 15-25% [212]. Наступні етапи (2027–2031 рр.) передбачають інтеграцію аналітики великих даних для моніторингу загроз та повну гармонізацію національного законодавства з Європейським актом про штучний інтелект (*EU AI Act*). Стратегічне планування враховує різні сценарії розвитку конфлікту, що дозволяє здійснювати превентивну адаптацію політик [268]. Подібна послідовність реалізації відображає перехід від реактивного запобігання загроз до формування стратегічної переваги, а очікувана економічна ефективність може виражатися в скороченні витрат на кризове реагування до 30%.

Подолання інформаційних розривів вимагає комплексних рішень, зокрема:

- Забезпечення офлайн-доступності інформації. Розгортання механізмів поширення ключових повідомлень через радіомовлення, друковані носії та локальні мережі дозволяє протидіяти інформаційному вакууму під час масових вимкнень електроенергії, що охоплювали понад 50% території України у 2022–2024 рр. Саме в такі періоди спостерігалось активне поширення

дезінформації, наприклад, про «атмосферні феномени» як причини вимкнень [218]. Використання державних радіомереж та систем SMS-оповіщення забезпечує охоплення до 70% населення, надаючи доступ до верифікованих даних без необхідності під'єднання до Інтернету.

- Децентралізація інфраструктури**.** Акцент на розгортанні локальних серверів та розподілених обчислювальних потужностей (edge computing) забезпечує функціональність критичних сервісів, зокрема платформ фактчекінгу, під час тривалих блекаутів. Інтеграція рішень на кшталт Starlink дозволяє відновлювати до 80% зв'язку протягом години блекату, що є ключовим для протидії інформаційній фрагментації, посиленій масовою міграцією населення (понад 6 млн осіб) [218]. Аналіз вказує, що децентралізація інфраструктури знижує загальну вразливість інформаційного простору на 40%, перетворюючи блекаути з каталізаторів кризи на інструмент тестування та підвищення стійкості системи.

Синергія між ключовими акторами є вирішальним фактором ефективності. Бізнес-сектор (наприклад, monobank) демонструє високу оперативність у протидії кіберзагрозам, успішно відбиваючи масовані DDoS-атаки (понад 10 інцидентів з 2022 року, зокрема, з атакою в серпні 2024 р. з піковим навантаженням 1 Tbps) шляхом впровадження багатофакторної аутентифікації та систем локального резервного копіювання, забезпечуючи захист понад 10 мільйонів клієнтів. Громадянські ініціативи здійснюють критичну роботу з фактчекінгу: спростовано понад 2300 дезінформаційних матеріалів з початку повномасштабного вторгнення. Держава виконує координувальну та нормативну функцію через CERT-UA та вдосконалення законодавчої бази (наприклад, проєкт Закону "Про захист персональних даних" № 8153, у якому пропонуються ширші умови автоматизованої обробки персональних даних відповіднодо GDPR). За оцінками експертів GLOBSEC, така синергія дозволяє підвищити загальну ефективність протидії загрозам на 25%, особливо за умови фінансування до 30% ініціатив приватним сектором [273].

Емпіричні дані підтверджують, що комплексне впровадження запропонованої моделі може знизити вплив дезінформації на 15-25%, як демонструє мета-аналіз PLOS ONE щодо ефективності корекції хибних наративів про російсько-українську війну [212], що супроводжується підвищенням суспільної стійкості до маніпуляцій, а економічний ефект може передбачати скорочення соціальної поляризації на 20%. В українському контексті це еквівалентно збереженню суспільної єдності та консолідованості під час найгостріших криз, таких як масштабні блекаути 2024-2026 років.

Проведене дослідження дало змогу сформулювати низку теоретичних узагальнень і практичних результатів, що мають ключове значення для розробки ефективної політики когнітивної стійкості в Україні.

1. Когнітивна війна становить окремий домен гібридних конфліктів, у межах якого об’єктом впливу виступають не лише інформаційні ресурси, а насамперед когнітивні процеси суспільства, що вимагає формування цілеспрямованої стійкості до інформаційного тиску**.** Емпіричний аналіз підтвердив еволюцію арсеналу таких операцій в Україні – від переважно пропагандистських наративів (2014-2021 рр.) до комплексних когнітивно-кібернетичних кампаній (2022-2025 рр.), що поєднують AI-генерований контент, цілеспрямовані кібератаки на критичну інфраструктуру для створення інформаційного вакууму та алгоритмічне підсилення в цифровому середовищі для швидкого поширення маніпулятивних наративів.

2. Трикомпонентна модель формування суспільної стійкості (суспільний, технологічний та регуляторний виміри) продемонструвала свою результативність в умовах воєнного стану. Встановлено, що її впровадження сприяє зниженню впливу дезінформаційних кампаній на 20-30% та підвищує рівень суспільної стійкості до інформаційно-психологічного тиску. Ключову роль у формуванні цієї стійкості відіграла синергія між фактчекінговими ініціативами (зокрема, StopFake, що спростував понад 10 000 фейків), системами аналітики великих даних (виявлення 85% координованих кампаній у режимі реального часу) та правовою адаптацією (гармонізація з положеннями AI Act),

що забезпечила перехід від реактивного реагування до проактивної моделі стійкості.

3. Запропоновані механізми протидії (децентралізація інфраструктури, забезпечення офлайн-доступу до інформації, публічно-приватне партнерство) довели свою ефективність для підвищення резильєнтності в умовах фрагментованого інфопростору та енергетичних обмежень**.** Використання мережі Starlink та локальних серверів забезпечило функціонування близько 80% критичної інфраструктури, а радіомовлення та SMS-оповіщення охопили до 70% населення навіть в умовах масштабних блекаутів, що дозволило протидіяти інформаційному вакууму, який є ключовим елементом стратегії когнітивного впливу.

Таким чином, розвиток суспільної стійкості до інформаційного тиску має стати пріоритетним напрямом забезпечення національної безпеки в умовах тривалого гібридного протистояння.

У межах нашого дослідження когнітивну безпеку розглядаємо як системоутворювальний вимір національної безпеки України в умовах гібридної війни, що безпосередньо впливає на функціональність політичної системи та здатність держави до довготривалого опору. Аналіз сучасних безпекових викликів засвідчує, що когнітивна війна виступає окремим доменом гібридних конфліктів, у межах якого ключовим об’єктом впливу є свідомість суспільства, механізми формування смислів, ідентичностей та політичних установок.

Еволюція когнітивних загроз в Україні характеризується поступовим ускладненням інструментарію впливу – від інформаційно-пропагандистських практик до комплексних когнітивно-кібернетичних операцій, що поєднують дезінформацію, інформаційно-психологічні операції, кібератаки та алгоритмічне підсилення маніпулятивних наративів. Такі впливи спрямовані на ерозію довіри до політичних інститутів, фрагментацію суспільної свідомості та підрив соціальної згуртованості, що створює додаткові ризики для стабільності політичної системи.

У цьому контексті когнітивна безпека постає як багатовимірний процес, ефективність якого визначається інтеграцією трикомпонентного підходу, що охоплює легітимність політичної влади, стійкість суспільства до інформаційно-психологічних впливів та формування національної ідентичності. Легітимність виступає ключовим чинником підтримання довіри громадян до державних інститутів й ухвалення політичних рішень; стійкість забезпечує здатність суспільства адаптуватися до тривалих кризових впливів без втрати функціональності; національна ідентичність виконує інтегративну роль, зменшуючи вразливість до маніпулятивних наративів та зовнішнього символічного тиску.

Таким чином, когнітивна безпека набуває характеру стратегічного імперативу, що поєднує інституційні, соціальні та смислові виміри та визначає довгострокову спроможність політичної системи України зберігати суверенітет, єдність й ефективність в умовах воєнного протистояння та постійної трансформації безпекового середовища.

ВИСНОВКИ

Дослідження феномену когнітивної безпеки є одним із пріоритетних напрямів сучасної політичної науки, оскільки він охоплює широкий спектр проблем, пов’язаних із захистом суспільної свідомості, стійкістю політичних процесів та забезпеченням національної безпеки в умовах гібридної війни. Когнітивна безпека передбачає здатність держави й суспільства протистояти маніпулятивному інформаційно-психологічному впливу, зберігати критичне мислення, довіру до інституцій та цілісність національної ідентичності.

Когнітивна безпека як наукова категорія має багаторівневу внутрішню структуру, що поєднує інформаційні, психологічні, комунікативні та інституційні компоненти. Її структурними елементами є когнітивна стійкість особистості, смислова цілісність суспільства, інституційна надійність процесів ухвалення рішень і захищеність національного інформаційного середовища від маніпулятивних впливів. У цьому контексті когнітивна безпека не зводиться лише до протидії дезінформації, а охоплює управління смислами, наративами та інтерпретаційними рамками, які визначають політичну поведінку й суспільні реакції. Саме структурованість когнітивної безпеки дозволяє розглядати її як системоутворювальний елемент національної безпеки, що забезпечує узгодженість між індивідуальним сприйняттям, колективною свідомістю та стратегічними цілями держави.

В епоху цифрових технологій, що охоплюють усі аспекти людського життя, когнітивна безпека набуває першочергового значення. Цей феномен стосується оберігання особистості від інформаційних маніпуляцій, поширення неправдивих відомостей та цифрових атак, що цілеспрямовано впливають на розумові та пізнавальні функції людини.

Зміст поняття «загроза когнітивній безпеці» визначається як сукупність інформаційно-психологічних і технологічних впливів, спрямованих на спотворення сприйняття реальності, підрив довіри до інституцій і розмивання ідентичності. Загрози класифіковано за джерелом походження (зовнішні та

внутрішні), рівнем реалізації (індивідуальні, групові, суспільно-державні), інструментами впливу (дезінформація, пропаганда, ІПСО, маніпулятивні наративи, алгоритмічна персоналізація, ШІ-технології), а також за масштабом і наслідками. Окремої уваги заслуговує психологічний вимір когнітивної безпеки, зокрема роль емоційних станів, когнітивного перевантаження та зниження здатності до раціональної оцінки інформації в підвищенні вразливості до пропагандистсько-маніпулятивних впливів.

Концептуальний аналіз понять «гібридна війна» та «когнітивна війна» виявив їх як взаємопов'язані форми деструктивного впливу на суспільство в сучасному політичному процесі. Гібридна війна розглядається як комплексна стратегія протистояння, що поєднує військові, політичні, інформаційні, економічні та психологічні інструменти з метою послаблення держави зсередини без формального оголошення війни.

Когнітивна війна є як складник та водночас еволюційний етап гібридного протистояння, у межах якого ключовим об'єктом впливу стає людська свідомість, процеси пізнання, інтерпретації інформації та ухвалення рішень. На відміну від класичних форм інформаційної війни, когнітивна війна спрямована не лише на поширення повідомлень, а й на зміну ментальних моделей, ціннісних орієнтацій і поведінкових установок.

Гібридна та когнітивна війни функціонують у тісному взаємозв'язку, де когнітивний вимір виконує роль ключового фронту сучасного протистояння. Саме через маніпуляцію наративами, емоціями та сприйняттям реальності здійснюється деструктивний вплив на суспільну єдність, легітимність політичних інститутів і стійкість держави, що обґрунтовує необхідність розгляду когнітивної безпеки як стратегічного елемента національної безпеки.

Основні інструменти когнітивного впливу, що застосовуються в процесі гібридної агресії проти України реалізуються через комплекс інформаційно-психологічних, комунікативних і технологічних засобів, спрямованих на зміну сприйняття реальності, підрив критичного мислення та формування деструктивних моделей поведінки. До ключових інструментів когнітивного

впливу відносимо пропагандистські та дезінформаційні наративи, інформаційно-психологічні операції, маніпулятивні медіатехнології, використання соціальних мереж й алгоритмів персоналізації контенту, а також сучасні цифрові інструменти, зокрема технології штучного інтелекту та дипфейків. Їхнє застосування спрямоване на емоційну дестабілізацію суспільства, поляризацію громадської думки, зниження довіри до державних інституцій і делегітимацію політичної влади.

Важливе значення у цьому контексті мають психологічні механізми когнітивного впливу, такі як апеляція до страху, тривоги, образу жертви, ефекту перевантаження інформацією та формування «інформаційних бульбашок». Саме поєднання технологічних і психологічних інструментів робить когнітивний вплив особливо ефективним у межах гібридної війни, перетворюючи свідомість людини на ключовий об’єкт сучасного протистояння.

В умовах інтенсивного розвитку цифрових технологій інформація набуває статусу одного з ключових ресурсів і водночас інструментів сучасного політичного протистояння. Технології інформаційного та когнітивного впливу, що охоплюють використання традиційних медіа, соціальних мереж і цифрових платформ, відіграють дедалі вагомішу роль у формуванні суспільних уявлень, політичних орієнтацій і моделей поведінки. Інформаційні та когнітивні операції характеризуються широким спектром проявів — від поширення пропагандистських і дезінформаційних наративів до цілеспрямованого психологічного впливу на індивідуальну й колективну свідомість. Такі практики застосовуються як державними, так і недержавними акторами з метою трансформації політичного порядку денного, маніпулювання електоральними настроями та впливу на процеси ухвалення політичних рішень. Зазначені тенденції актуалізують необхідність наукового осмислення когнітивної безпеки як важливого виміру сучасної національної та політичної безпеки.

Компаративний аналіз технологій пропаганди та інформаційних операцій, що застосовуються в умовах воєнного стану з огляду на їхні цілі, інструментарій та вплив на когнітивну стійкість суспільств, показує, що пропаганда переважно

має системний і довготривалий характер: вона спрямована на формування стабільних ідеологічних установок, легітимацію потрібних наративів, нормалізацію агресії та створення “пояснювальних рамок”, через які аудиторія інтерпретує події. Натомість інформаційні операції (зокрема ІПСО) є більш ситуативними, гнучкими та тактично зорієнтованими: вони націлені на конкретні ефекти: дезорієнтацію, деморалізацію, поляризацію, зниження довіри до інституцій, вплив на політичні рішення або поведінку окремих груп.

У ході порівняння відзначимо відмінності за основними параметрами: за масштабом (пропаганда – масова й довготривала; операції – сегментовані та коротко-/середньострокові), за каналами поширення (пропаганда активно використовує традиційні медіа та повторювані меседжі; інформаційні операції – цифрові платформи, таргетинг, мережеві кампанії), за методами впливу (пропаганда апелює до цінностей, ідентичності та міфологем; ІО – до емоційних тригерів, когнітивного перевантаження, фейків, маніпуляцій контекстом, дипфейків й алгоритмічного підсилення контенту). Водночас доведено їхню спільну рису – системне використання психологічних механізмів (страх, тривога, ненависть, недовіра), які в умовах воєнного стану підвищують вразливість аудиторій та прискорюють поширення деструктивних наративів.

В умовах воєнного стану пропаганда та інформаційні операції функціонують у синергії: пропаганда формує “смисловий каркас”, тоді як інформаційні операції забезпечують швидкі тактичні ефекти. Це створює додаткові ризики для когнітивної безпеки, що обґрунтовує необхідність комплексної протидії, яка поєднує стратегічні комунікації держави, моніторинг інформаційного середовища та розвиток когнітивної резильєнтності суспільства.

Взаємозв’язок легітимації політичної влади та когнітивної безпеки має системний характер, оскільки легітимність у сучасних умовах формується не лише через юридичні процедури, а передусім через когнітивно-комунікаційні механізми – довіру, переконаність у правомірності й компетентності інституцій, прийнятність рішень у ціннісному вимірі та готовність суспільства визнавати їх обов’язковими. У гібридному протистоянні противник спрямовує значну

частину інформаційно-психологічного впливу саме на легітимаційні контури, оскільки підрив довіри до держави, дискредитація управлінських рішень, формування образу «недієздатних інституцій» або нав'язування фаталістичних інтерпретацій безпосередньо знижують здатність суспільства до колективної мобілізації й підтримання стійкості. У цьому контексті політичний складник когнітивної безпеки виступає базою, що забезпечує стабільність легітимації: вона підтримує здатність громадян розрізняти достовірні повідомлення та маніпуляції, зберігати раціональність у ситуації емоційного тиску, а також відтворювати спільні смисли, які утримують суспільну згуртованість і довіру до інституцій. Водночас легітимація є ресурсом когнітивної безпеки, адже чим більш узгодженою, послідовною і прозорою є публічна комунікація влади, тим нижча когнітивна вразливість аудиторій до дезінформації, тим слабше працюють механізми поляризації та тим ефективнішими стають контрнаративи. Отже, когнітивна безпека і легітимація перебувають у взаємопідсилювальній залежності: ерозія легітимності поглиблює когнітивні ризики, тоді як захищеність когнітивного простору зменшує ефекти делегітимаційних кампаній і підтримує керованість політичної системи в умовах війни. Саме тому інтеграція когнітивної безпеки в державні стратегічні комунікації – через системний моніторинг загроз, узгоджені наративи, кризову комунікацію та партнерство з громадянським суспільством – стає необхідною умовою збереження довіри, політичної стійкості та здатності держави ухвалювати й реалізовувати рішення в умовах тривалого гібридного тиску.

З початком війни за Незалежність України та окупацією Криму питання національної ідентичності та формування інформаційної і когнітивної безпеки актуалізувалися з особливою гостротою. Існування та розвиток Української держави неможливі без усвідомлення громадянами своєї національної ідентичності, що починається з ототожнення себе з українським народом. Відчуття приналежності, яке формується через мову, традиції та цінності, безпосередньо впливає на кожного. Сукупність усіх, хто пройшов таке самовизначення, становить необхідний фундамент для формування сильного

громадянського суспільства, міцної нації та стабільної держави. Українська ідентичність, яку слід розуміти як стійке усвідомлення особою належності до української нації як самобутньої спільноти, об'єднаної назвою, символами, географічним та етносоціальним походженням, історичною пам'яттю, комплексом духовно-культурних цінностей, зокрема українською мовою і народними традиціями, є ключовим підґрунтям для розвитку демократичних основ життя суспільства, національної державності, інформаційної та когнітивної безпеки українського суспільства.

Національна ідентичність має вагомий вплив на формування інформаційної і когнітивної безпеки українського суспільства та є не менш важливим чинником безпечного існування нації, ніж національна територія і національне багатство. Вона інтегрує суспільство для протистояння зовнішньому ворогу та охоплює складники культури, що розвивалися протягом багатьох поколінь, а також допомагає підтримувати єдність групи та впливати на громадськість, підкреслюючи їхню етнонаціональну відмінність від супротивника. Концептуалізація феномену ідентичності чітко окреслює коло загроз і викликів для національної безпеки в умовах російської агресії, спрямованої на окупацію території України з подальшим посиленням ризиків, пов'язаних із нівелюванням ознак національної, громадянської, культурної, релігійної ідентичності українців. Водночас розмита національна ідентичність, створена політиками або деякими політичними силами, ідея регіональної відмінності українців заважає об'єднатися нації.

Компаративний аналіз міжнародного досвіду США та Естонії у сфері протидії дезінформації та забезпечення когнітивної безпеки вказує, що підходи обох держав базуються на розумінні інформаційного та когнітивного простору як ключового виміру національної безпеки, однак реалізуються через різні інституційні моделі.

Досвід США характеризується розвиненою міжвідомчою координацією, залученням приватного сектору та громадянського суспільства, а також акцентом на аналітиці, публічній комунікації та оперативному реагуванні на

дезінформаційні кампанії. Естонська модель натомість ґрунтується на поєднанні цифрової держави, системної медіаграмотності та активної участі громадянських ініціатив, що сприяє формуванню високого рівня суспільної стійкості до маніпулятивних впливів.

Узагальнення цього досвіду дозволяє виокремити апробовані механізми забезпечення когнітивної безпеки, зокрема міжінституційну взаємодію, прозорі комунікаційні протоколи реагування на дезінформацію, освітні програми з розвитку критичного мислення та інтеграцію когнітивної складової з кібербезпековими практиками. Зазначені підходи можуть бути адаптовані до українських умов з урахуванням специфіки гібридної війни та потреби посилення національної когнітивної стійкості.

Значимість когнітивного захисту виявляється в тому, що його відсутність може спровокувати ухвалення помилкових рішень, деформацію особистого світобачення та руйнування довіри до інформаційних джерел. До інструментів захисту належать аналітичне мислення, інформаційна компетентність та розуміння психологічних методів впливу. Розвиток когнітивної безпеки сприяє формуванню поінформованих, незалежних та раціональних користувачів інформації в епоху цифровізації.

Когнітивний суверенітет у межах цієї дисертації доцільно розуміти як стратегічну спроможність держави й суспільства зберігати автономність формування колективних смислів, оцінок і ціннісних орієнтацій, тобто утримувати контроль над ментальним (смисловим) простором за умов зовнішнього тиску та конкурентної боротьби за інтерпретацію реальності. На відміну від інформаційного суверенітету, який переважно акцентує на інфраструктурі, правовому режимі доступу до даних і регулюванні комунікаційних каналів, когнітивний суверенітет фокусується на «кінцевій точці» впливу – тому, як інформаційні потоки перетворюються на переконання, емоційні реакції та поведінкові установки, що визначають політичні рішення громадян і рівень суспільної стійкості. У гібридній війні саме цей вимір стає критично важливим, оскільки деструктивні впливи спрямовуються не лише на

викривлення фактів, а й на підміну причинно-наслідкових зв’язків, нав’язування рамок сприйняття, ерозію національної ідентичності та делегітимацію державних інституцій. У практичній площині когнітивний суверенітет означає здатність держави забезпечувати стійкість когнітивного середовища через взаємопов’язані контури: нормативно-інституційний (узгодженість політик, компетенцій і відповідальності суб’єктів), комунікаційний (послідовність стратегічних наративів і кризової комунікації), освітньо-культурний (критичне мислення, медіаграмотність, підтримка національного культурного контенту) та технологічний (моніторинг і виявлення когнітивних атак, протидія алгоритмічному підсиленню деструктивного контенту). У такому розумінні когнітивний суверенітет постає не абстрактною категорією, а умовою збереження політичної суб’єктності: без можливості виробляти й захищати власні смисли, підтримувати довіру до легітимних джерел та зберігати інтегрованість комунікаційного простору держава втрачає здатність до консолідації суспільства, мобілізації ресурсів і забезпечення наступності політики у ситуації тривалих екзистенційних загроз.

Зв’язок між когнітивною та державною безпекою має фундаментальне значення. Когнітивна захищеність нації визначається спроможністю населення аналітично підходити до інформації, протистояти дезінформаційним кампаніям та цифровим загрозам. Це безпосередньо впливає на політичну стабільність та консолідацію суспільства. Викривлені або недостовірні повідомлення можуть стати засобом гібридної агресії і підірвати національну оборону та міжнародні зв’язки. Послідовна увага до когнітивної безпеки посилює оборонний потенціал країни та стійкість соціуму до різноманітних викликів.

Когнітивна безпека створює умови для виховання свідомих громадян, здатних виявляти інформаційні маніпуляції, що гарантує надійність інформаційної екосистеми та загальну резистентність держави проти внутрішніх та зовнішніх дестабілізувальних чинників.

В умовах війни за Незалежність України захист національного інформаційного простору від негативних інформаційно-психологічних впливів,

операцій та інформаційних війн стає надзвичайно важливим. Забезпечення інформаційної безпеки та збереження інформаційного суверенітету є ключовими факторами для підтримки національної ідентичності України та її існування як суверенної і незалежної держави.

Когнітивна модель безпеки України розглядається як комплексна система захисту процесів сприйняття, інтерпретації інформації, формування переконань й ухвалення рішень в умовах гібридної війни. Вона ґрунтується на розумінні когнітивного простору як ключового домену сучасного протистояння, у межах якого об'єктом впливу стає не лише інформація, а й свідомість, емоції та поведінкові установки суспільства.

Запропонована модель охоплює кілька взаємопов'язаних рівнів: індивідуальний (критичне мислення, інформаційна гігієна, психологічна стійкість), груповий (соціальна згуртованість, зниження поляризації, протидія «інформаційним бульбашкам»), інституційний (захист процесів ухвалення рішень, легітимність і довіра до влади) та національний (збереження ідентичності, стійкість політичного порядку, когнітивний суверенітет).

Функціонально модель базується на чотирьох ключових контурах: моніторингу й ранньому виявленні когнітивних загроз; аналітичній оцінці ризиків і вразливостей; оперативному реагуванні через стратегічні комунікації, контрнаративи та кризову інформаційну політику; профілактиці та формуванні когнітивної резильєнтності шляхом медіаосвіти, розвитку критичного мислення й підтримки якісного національного контенту.

Когнітивна модель безпеки має мультиакторний характер і передбачає взаємодію державних інституцій, сектору безпеки й оборони, системи освіти, медіа, громадянського суспільства, цифрових платформ і міжнародних партнерів. Її ефективність визначається рівнем суспільної довіри, здатністю швидко нейтралізувати дезінформаційні кампанії та зберігати внутрішню цілісність суспільства. Таким чином, когнітивна безпека постає як стратегічний складник національної безпеки України, без якого не можливі стійкість держави та успішне протистояння гібридним загрозам.

СПИСОК ВИКОРИСТАНИХ ДЖЕРЕЛ

1. Абакумов В.М. Інформаційна безпека підприємництва як об’єкт адміністративно-правової охорони. *Форум права*. 2012. № 4. С. 10–16.

2. Актуальні проблеми інформаційної безпеки / О.О. Тихомиров, А.В. Ватраль, Д.С. Мельник та ін. Одеса : Видавництво «Юридика», 2025. 264 с.

3. Алямкін Р. Правове забезпечення національної інформаційної безпеки. *Наукові записки Інституту законодавства Верховної Ради України*. 2013. № 4. С. 91–96.

4. Антонюк В.В. Основні науково-методологічні підходи до дослідження державної політики інформаційної безпеки. *Інвестиції: практика та досвід*. 2013. № 20. С. 143–147.

5. Арістова І.В. Державна інформаційна політика: організаційно-правові аспекти. МВС України, Ун-т внут. справ. Харків : Вид-во Ун-ту внутр. справ, 2000. 366 с.

6. Архипова Є.О. Соціально-філософське осмислення поняття «інформаційна безпека». *Вісник Нац. технічного ун-ту України «Київський політехнічний інститут». Філософія. Психологія. Педагогіка*. 2011. № 3. С. 7-11.

7. Баглікова М. Інформаційна війна і Україна. *Науковий вісник Ужгородського університету. Серія: Політологія, Соціологія, Філософія*. 2010. Вип. 14. С. 158–161.

8. Баранов А. Інформаційний суверенітет чи інформаційна безпека? *Нац. безпека і оборона.* 2001. № 1(13). С. 70–76.

9. Бевз Т. Когнітивна війна та національна ідентичність: протидія дезінформації як елемент стратегії ідентичності. *Утвердження української ідентичності в умовах воєнного стану: стратегічні орієнтири та інноваційні практики.* Збірник наукових праць за ред. К.О. Журби, Л.В. Канішевської. Івано-Франківськ: НАЇР, 2025. С. 11–16.

10. Бевз Т. Українська ідентичність і національна безпека у викликах сьогодення. *Українознавство.* 2020. № 4 (77). С. 143–158.

11. Безкоровайна М. Війна за розум: медіаграмотність у боротьбі за національну безпеку. *Детектор медіа.* 5 серпня 2022. URL: https://detector.media/infospace/article/243171/2025-08-05-viyna-za-svidomist-mediagramotnist-u-borotbi-za-natsionalnu-bezpeku/ (дата звернення: 15.12.2024).

12. Бекешкіна І. Є. Установки на громадську активність як компонент політичної культури індивіда. Соціологічні виміри громадянського суспільства в Україні / за наук. ред. О. Резніка. Київ: Інститут соціології НАН України, 2019. С. 134–164.

13. Бєлкін Л., Юринець Ю., Бєлкін М., Криволап Є. Співвідношення понять «інформаційна безпека», «безпека інформації», «кібербезпека» в контексті безпекових стратегій України 2020-2021 років. *Наукові праці Київського авіаційного інституту. Серія: Юридичний вісник «Повітряне і космічне право».* 2022. № 3 (64). С. 78–86.

14. Богайчук В. Ж. Соціальна ідентичність в умовах гібридної війни. *Вісник Луганського національного університету імені Тараса Шевченка : педагогічні науки*. 2018. № 8 (322). Ч. 2. С.167–175.

15. Богданович В., Муженко В., Цибізов А. Когнітивна модель організації протидії негативним тенденціям безпекового середовища, спрямованим на порушення сталого розвитку вибраної країни-мішені. *Військово-технічний збірник*. 2024. № 30. С. 3–7.

16. Богданович В., Олексіюк В., Павліковський А., Передрій О., Муженко В. Метод когнітивного моделювання негативного впливу гібридних загроз на національну безпеку держави. *Збірник наукових праць Центру воєнно-стратегічних досліджень Національного університету оборони України*. 2023. № 1(77). С. 6–12.

17. Боднар І. Р. Інформаційна безпека як основа національної безпеки. *Механізм регулювання економіки*. 2014. № 1. С. 68–75.

18. Бондаренко В.О., Литвиненко О.В. Інформаційна безпека сучасної держави: концептуальні роздуми. *Стратегічна панорама.* 1999. Вип.1-2. С. 127–133.

19. Борканюк А. Б., Шульмін С. О. Критичне мислення як складова інформаційної безпеки особистості. *Перспективи. Соціально-політичний журнал*. 2025. №2. С. 71–77.

20. Верголяс О. О. Інформаційно-правове забезпечення спеціальних інформаційних операцій. *Інформація і право*. 2018. № 4(27). С. 126–133.

21. Верголяс О.О. Правове забезпечення спеціальних інформаційних операцій. дис… канд. юрид. наук: 12.00.07. Київ, 2020. 287 с.

22. Верголяс О. О. Спеціальні інформаційні операції в системі засобів протидії загрозам національній безпеці України. *Міжнародний науковий журнал «Інтернаука». Серія: «Юридичні науки»*. 2024. № 4. С. 7–16.

23. Війни інформаційної епохи: міждисциплінарний дискурс: монографія за ред. В.А. Кротюка. Харків: Факт, 2021. 592 с.

24. Вітюк Н. Особливості дискурсу політичної пропаганди в умовах інформаційно-психологічної війни. *Збірник наукових праць: психологія*. 2019. №24. С. 29–38.

25. Волошенюк О. Гібридна агресія рф: інформаційна війна та конструювання іміджу НАТО як агресора. *The security architecture of European and Euro-Atlantic space*. 2022. URL: http://www.baltijapublishing.lv/omp/index.php/bp/catalog/download/247/6952/14476-1 (дата звернення: 30.07.2023).

26. Волошина Н. М. Поняття «безпека інформації» та «інформаційна безпека» в сучасному науковому просторі. *Сучасні інформаційні технології у сфері безпеки та оборони*. 2010. № 2. С. 53–56.

27. Галіпчак В. Сучасні виклики та стратегії забезпечення інформаційної безпеки України в умовах російської агресії: перспективи та завдання. *Науковий журнал «Регіональні студії»*. 2023. № 35. С. 65–70.

28. Галіпчак В. Безпека інформаційного простору України в умовах російської агресії на сучасному етапі: основні завдання та виклики. *Науковий журнал «Регіональні студії»*. 2023. № 34. С. 81-85.

29. Галіпчак В. Вплив інформаційних технологій на захист національних інтересів в Україні: виклики та можливості. *X Міжнародна науково-практична конференція «Пріоритетні шляхи розвитку науки і освіти»* (м. Львів, 29-30 листопада 2023 року). URL: http://www.lvivforum.inf.ua/save/2023/29-30.11/Збірник.pdf (дата звернення: 02.01.2024).

30. Гарань О. В. Інформаційна політика України: виклики та загрози національній безпеці. Київ: Фенікс, 2012. 256 с.

31. Гаценко С., Пащенко К., Свередюк Ю., Стариш М. Модель процесу визначення загроз воєнній безпеці, як складової національної безпеки держави. *Сучасні інформаційні технології у сфері безпеки та оборони*. 2021. № 42 (3). С. 111–116.

32. Генеза сучасної інформаційно-когнітивної (гібридної) війни в українському контексті та глобальному вимірі: наукове дослідження / С.Д. Максименко, Л.М. Деркач. Київ: «Видавництво Людмила», 2024. 128 с.

33. Герасименко О. Політична пропаганда як засіб інформаційної війни. *Scientific Collection «InterConf»*. 2022. № 120. С. 102-104.

34. Герасимов С. В., Базарний С. В. Методика розрахунку місцезнаходження агентів соціальних мереж при проведенні інформаційних операцій. *Застосування інформаційних технологій у підготовці та діяльності сил охорони правопорядку* : матеріали Міжнар. наук.-практ. конф. (14 березня 2024 р.). Харків, 2024. С. 56–58.

35. Геращенко А. М., Поліщук І. М. Інформаційна війна: сучасні виклики та загрози національній безпеці. Кондор. Київ, 2016. 155 с.

36. Гіда О. Ф. Інформаційно-психологічні атаки як одна з форм реалізації технологій деструктивного впливу на суспільство. *Боротьба з організованою злочинністю і корупцією (теорія і практика).* 2015. № 1. С. 153–158.

37. Глущенко О. О. Функція забезпечення безпеки держави в умовах воєнного стану. *Часопис Київського університету права.* 2023. № 1. С. 53–56.

38. Гончаренко Г. А. До проблеми визначення та розмежування дефініцій «інформаційна безпека» і «кібербезпека». *Аналітично-порівняльне правознавство*. 2024. № 5. С. 466–471.

39. Горбань Ю. О. Інформаційна війна проти України та засоби її ведення. *Вісник Національної академії державного управління при Президентові України*. 2015. № 1. С. 136–141.

40. Горбулін В. «Гібридна війна» як ключовий інструмент російської геостратегії реваншу. *Дзеркало тижня.* 2015. 23 січня. URL: https://zn.ua/ukr/internal/gibridna-viyna-yak-klyuchoviy-instrument-rosiyskoyi-geostrategiyi-revanshu-_.html (дата звернення: 12.12.2023).

41. Горбулін В. П. Інформаційні операції та безпека суспільства: загрози, протидія, моделювання: монографія. Київ : Інтертехнологія, 2009. 164 с.

42. Горбулін В. П. Світова гібридна війна: український фронт. Київ: Національний інститут стратегічних досліджень. Київ : НІСД, 2017. 496 с.

43. Городнича К. В. Пропаганда як технологія політичного маніпулювання. *Міжнародні наукові дослідження: інтеграція науки та практики*. Київ : ГО «Інститут інноваційної освіти», 2018. С. 82–84.

44. Гривнак Б., Лопушинський І., Сапіжак І. Дезінформація як загроза національній безпеці України в умовах неоголошеної російсько-української війни. *Науковий вісник Вінницької академії безперервної освіти. Серія «Екологія. Публічне управління та адміністрування».* 2024. Вип. 1. С. 52–55.

45. Гриценко В. Гібридна війна Росії проти України: інформаційні аспекти. Інформаційна безпека України: виклики та загрози. Київ, 2017. 220 с.

46. Гулай В., Базюк К. Інформаційно-психологічна складова гібридної війни Російської Федерації проти України (2014-2021 рр.): теоретико-методологічні засади дослідження. The Russian-Ukrainian war (2014–2022): historical, political, cultural-educational, religious, economic, and legal aspects: Scientific monograph. Riga, Latvia: “Baltija Publishing”, 2022. С. 873–882.

47. Гулай В.В. Загрози інформаційно-психологічній безпеці особи в реаліях інформаційно-психологічної війни як складової «гібридної війни» Російської Федерації проти України. *Людина і техніка у визначних битвах світових воєн XX століття (до 70-річчя завершення Другої світової війни)*: Збірка тез доповідей Міжнародної наукової конференції 21-23 жовтня 2015 р. Вип. 25. Львів: НАСВ. С. 233–244.

48. Гулай В., Сеник В., Базилюк К. Проблеми формування та практичного застосування окремих дефініцій у галузі національної безпеки. *Social Development and Security*. 2025. № 15 (1). С. 11–18.

49. Гурковський В. Механізми використання інформації в умовах Російської гібридної агресії. *Освіта регіону*. 2016. № 4. С. 16–23.

50. Гурковський В. І. Організаційно-правові питання взаємодії органів державної влади у сфері національної інформаційної безпеки. Київ, 2004. 225 с.

51. Гурковський В. І. Розбудова інформаційного суспільства в Україні в умовах сьогодення: практичні аспекти. *Державне управління: удосконалення та розвиток.* 2010. № 12. URL: http://www.dy.nayka.com.ua/?op=1&z=228 (дата звернення: 12.12.2023).

52. Денисюк С., Фокін Ю. Національна ідентичність як чинник міжнародної безпеки: політико-правовий аналіз. *Вісник Харківського національного університету імені В. Н. Каразіна. Питання політології*. 2023. № 44. С. 19–25.

53. Дергильова О. Модель науково-технічної сфери системи забезпечення воєнної безпеки держави. *Сучасні інформаційні технології у сфері безпеки та оборони*. 2021. Вип. 40 (1). С. 175–180.

54. Дерев’янко І. П. Гібридна війна як різновид асиметричних дій. *Міжнародні відносини: теоретико-практичні аспекти*. 2023. №11. С. 6–16.

55. Дерев’янко С. М. Безпековий вимір народовладдя в умовах гібридної війни. *Держава і право: зб. наук. пр. Серія. Політичні науки.* Ін-т держави і права ім. В. М. Корецького НАН України. Київ, "Юридична думка", 2020. Вип. 87. С. 308–318.

56. Дерев'янко С. М. Гібридна війна: інформаційно-безпековий вимір.

Вісник Прикарпатського університету. Серія: Політологія. 2024. Вип. 18. С. 11–18.

57. Дерев'янко С. Народовладдя у безпековому вимірі. Актуальні проблеми політики, інформації та безпеки: монографія. Прикарпат. нац. ун-т ім. В. Стефаника. Івано-Франківськ : «Ярина», 2022. С. 4–29.

58. Дзьобань О. П., Соснін О.В. Інформаційна безпека: нові виміри загроз, пов'язаних із інформаційно-комунікаційною сферою. *Гуманітарний вісник Запорізької державної інженерної академії.* 2015. № 61. URL: http://vestnikzgia.com.ua/article/view/47745/44014 (дата звернення: 12.05.2024).

59. Дзьобань О. П. Національна безпека в умовах соціальних трансформацій (Методологія дослідження та забезпечення). Харків: Константа, 2006. 324 с.

60. Дзьобань О. П. Формування інформаційної картини світу як результат відображення генезису базових форм буття. Матеріали "круглого столу" *Проблема інформаційного суспільства: соціально-правовий аналіз.* Полтава, ТОВ "Фірма "Техсервіс", 28 лют. 2013. С. 26–36.

61. Ділай А., Кротченко В. Війна за Україну: від інформаційних операцій до прямого вторгнення. *Вісник Львівського університету. Серія: Журналістика.* 2019. № 45. С. 13–20.

62. Дослідження соціально-психологічного стану населення України в умовах війни: виклики для фахової спільноти : матеріали круглого столу (м. Київ, 20 червня 2024 р.) / за наук. ред. М. М. Слюсаревського, С. Л. Чуніхіної ; Інститут соціології НАН України, Інститут соціальної та політичної психології НАПН України. Київ : Талком, 2024. 45 с.

63. Дубас О. П. Інформаційний розвиток сучасної України у світовому контексті. Київ : Генеза, 2014. 276 с.

64. Дубняк К. А. Інформаційний простір: структура функціональні параметри. *Держава та регіони. Серія: Соціальні комунікації*. 2015. № 4 (24). С. 21–25.

65. Дуцик Д. Українська інформаційна політика в умовах війни: критичні

зауваження. Протидія російській інформаційній агресії: спільні зусилля задля захисту демократії. Аналітичний звіт. Телекритика. Київ. 2015. 77 с.

66. Журибіда Н. Р. Цільові орієнтири та функціональні аспекти економічної безпеки банків. *Вісник Одеського національного університету. Серія: Економіка*. 2019. Вип. 24 (4). С. 123–127.

67. Заболотний А. Г. Пропаганда: визначення, основні елементи та види. *Актуальні проблеми технічних та соціально-гуманітарних наук у забезпеченні діяльності служби цивільного захисту*: Матеріали Всеукраїнської науково-практичної конференції. 4 квітня 2014 року, м. Черкаси. Черкаси: ЧІПБ імені Героїв Чорнобиля НУЦЗ України, 2014. С. 216–218.

68. Золотар О. О. Критичне мислення як необхідна умова безпеки людини в інформаційному суспільстві: соціально-правовий аналіз. *Інформаційна безпека людини, суспільства, держави*. 2018. № 1. С. 98–105.

69. Зубар Н., Рущенко, І. П. Когнітивна зброя і когнітивна безпека: постановка питання. *Українське суспільство в умовах війни: виклики сьогодення та перспективи.* 2017. С. 267–270.

70. Індекс медіаграмотності українців за 2024 рік / ГО «Детектор медіа». Київ: ГО «Детектор медіа», 2025. URL: https://www.stopfake.org/uk/indeks-mediagramotnosti-ukrayintsiv-za-2024-rik/ (дата звернення: 02.05.2025).

71. Інформаційний вимір гібридної війни: досвід України: матеріали міжнародної науково-практичної конференції. Київ : НУОУ, 2017. 104 с.

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

73. Єрмакова Т. В., Іванов О. Ф. Медіаграмотність як складова національної стійкості в умовах когнітивної війни. *Вісник Національного авіаційного університету. Серія: Філософія. Культурологія*. 2023. № 2 (38). С. 45–51.

74. Кобець Т. Аналіз загроз когнітивній безпеці українського суспільства: класифікаційні підстави. *Вісник Прикарпатського університету. Серія: Політологія.* 2024. Випуск 19. С. 67-72.

75. Кобець Т. Використання технологій інформаційних операцій у політичній практиці. *Літопис Волині*. 2024. № 31. С. 134–139.

76. Кобець Т. Інформаційні спеціальні операції: особливості реалізації в сучасних умовах. *Вісник Прикарпатського університету. Серія: Політологія*. 2025. Випуск 20. С. 256–263.

77. Кобець Т. Когнітивна безпека в умовах гібридної війни. *Вісник Прикарпатського університету. Серія: Політологія*. 2024. Випуск 17. С. 67–73.

78. Кобець Т. Основні підходи до розуміння «когнітивна безпека» в сучасній науці: політичний та інформаційний аспект. *Вісник Львівського університету. Серія філософсько-політологічні студії.* 2023. Вип. 49. С. 278–285.

79. Кобець Т. Порівняльний аналіз технологій пропаганди та контрпропаганди в умовах воєнного стану. *Вісник Прикарпатського університету*. Серія: Політологія. 2023. Випуск 15. С. 33–42.

80. Кобільник Б.Ю., Гізун А.І. Роль інформаційно-психологічних впливів у інформаційній війні. *Актуальні задачі та досягнення у галузі кібербезпеки* : матеріали Всеукраїнської науково-практичної конференції, 23-25 листопада 2016 р. Кропивницький, 2016. С. 28–29.

81. Коваль З. Психоісторичні операції та війни як засіб управління минулим і сьогоденням: механізми правової протидії. *Актуальні проблеми державного управління*. 2018. Вип. 2. С. 79–84.

82. Колосовська І. І. Концептуалізація феномену ідентичності як складової національної безпеки: публічно-управлінський виміри. *Проблеми сучасних трансформацій. Серія: право, публічне управління та адміністрування*. 2025. №15. URL: https://reicst.com.ua/pmtl/article/view/2025-15-02-02 (дата звернення: 23.11.2025).

83. Конституція України: Закон України № 254к/96-ВР від 28.06.1996 № (зі змінами та доповненнями). URL: https://zakon.rada.gov.ua/laws/show/254к/96-вр#Text (дата звернення: 10.07.2023).

84. Король В., Любовець Г. Контент негативу. Як захистити себе та країну

в умовах тотального інформаційного протистояння: монографія. Київ : Видавничий дім «Києво-Могилянська академія», 2021. 266 с.

85. Крайнов В. О. Перспективні напрямки удосконалення безпеки інформаційного середовища органів управління військами. *Актуальні проблеми управління інформаційною безпекою держави*: зб. матер. наук.-практ. конф. (Київ, 18.03.2016): у 2 ч. Ч. 1. Київ : Нац. акад. СБУ, 2016. С. 24–27.

86. Криволап Є.В. Співвідношення понять «інформаційна безпека», «безпека інформації», «кібербезпека», «когнітивна безпека» як стійкість проти інформаційно психологічних впливів на людину і суспільство. *Свобода, безпека та незалежність: правовий вимір: Матеріали XIII Міжнародної науково-практичної конференції*, м. Київ, Національний авіаційний університет, 24 лютого 2023 р. С. 195–197.

87. Кузнєцова О. Технології рефлексивного управління людьми в російських ЗМІ та протидія їм. *Вісник Національного університету «Львівська політехніка». Серія: Журналістські науки.* Львів : Вид-во Львівської політехніки, 2018. № 896. С. 63–70.

88. Курбан О. В. Сучасні інформаційні війни в мережевому он-лайн просторі. Київ : ВІКНУ, 2016. 286 с.

89. Курило В. С., Караман О. Л., Степаненко В. І. Критичне мислення і протидія маніпулятивному впливу в контексті безпеки особистості в інформаційно-психологічному вимірі війни. *Соціальна педагогіка. Інноваційна педагогіка.* 2023. Вип. 60. С. 167–172.

90. Куруч А. В. Формування національної ідентичності як основа національної безпеки України. *Проблеми інженерно-педагогічної освіти».* 2020 № 67. С. 147–154.

91. Кухоцька Т. Російська пропаганда в політичній комунікації під час війни. V International Scientific and Practical Conference «*Theoretical and empirical scientific research: concept and trends*» (june 23, 2023). Oxford, UK, 2023. С. 193–194.

92. Лемак О. В. Національна самосвідомість як найбільш пріоритетний об’єкт забезпечення національної безпеки. *Науковий вісник Ужгородського Національного Університету. Серія Право*. 2024. Випуск 86. Частина 1. С. 78–89.

93. Лизанчук В. Українська мова – життя державного основа. *Тоталітаризм як система знищення національної пам’яті:* збірник наукових праць за матеріалами всеукраїнської науково-практичної конференції з міжнародною участю 11 – 12 червня 2020 року / науковий редактор Тетяна Єщенко. Львів: Друкарня Львівського національного медичного університету імені Данила Галицького, 2020. С. 126–130.

94. Лисенко Ю. В. Соціальна безпека: виклики в умовах політичної нестабільності українського суспільства. *Науковий журнал «Політикус».* 2022. Вип. 6. С. 24–28.

95. Лисянський П.В. Смислова розвідка (Cemint) як нова парадигма когнітивної безпеки України. *Український політико-правовий дискурс*. 2025. URL: https://ppdnz.com.ua/index.php/home/article/download/428/327 (дата звернення: 10.12.2025).

96. Любченко А. В. Ключові питання публічного управління безпекою політичних інтернет-комунікацій. *Журнал «Наукові інновації та передові технології»*. 2024. № 3 (31). С. 1104–1114.

97. Макух-Федоркова І. Сучасні методологічні підходи до визначення понять смислові/когнітивні війни: аналіз інструментів впливу. *Історико-політичні проблеми сучасного світу: Збірник наукових статей*. 2024. № 49. С. 120–136.

98. Малик І. Р. Когнітивна війна: людська свідомість як поле бою. *Регіональні студії.* 2024. № 39. С. 45–50.

99. Манойленко О. В., Ягі М. Когнітивне моделювання забезпечення безпеки національної економіки України. *Причорноморські економічні студії.* 2018. Вип. 18-1. С. 188–193.

100. Марчук В. В. До проблеми політичної консолідації і збереження національної ідентичності українського інформаційного простору. Аксіологічні аспекти трансформації сучасного українського суспільства. Івано-Франківськ: «Ярина», 2012. С. 113–115.

101. Матвієнків С., Головчинський Н. Теоретико-методологічні засади дослідження поняття «війна». *Вісник Прикарпатського університету. Сер. Політологія.* 2020. Вип. 14. С. 103–113.

102. Матвієнків С. М. Державна інформаційна політика в контексті інтеграції України в Європейський Союз. *Вісник Прикарпатського університету. Політологія.* 2018. Вип. 12.С. 227–234.

103. Матвієнків С. М. Інструментарій протидії загрозам в інформаційній сфері. *Держава і право: Збірник наукових праць. Юридичні і політичні науки*. Випуск 41. Київ: Інститут держави і права ім. В.М. Корецького НАН України, 2008. С. 646–653.

104. Матвієнків С. М. Інформаційний простір сучасної України як складова національної безпеки і суверенітету держави. *Політична наука: теорія, методологія, практика: монографія.* [за ред. Климончука В.Й.]; Прикарпатський національний університет імені В. Стефаника; Факультет історії, політології і міжнародних відносин. Івано-Франківськ: Супрун В.П., 2021. С. 207–225.

105. Матвієнків С. М. Інформаційний простір України як чинник інтеграції суспільства. *Українознавчі студії. Науково-теоретичний журнал Інституту українознавства.* Івано-Франківськ: Видавничо-дизайнерський відділ ЦІТ, 2007-2008. № 8–9. С. 252–258.

106. Матвієнків С. М. Інформаційні війни: їх суть та вплив на політичну сферу суспільства. *Науковий вісник Ужгородського університету. Серія: Політологія. Соціологія. Філософія*. Випуск 10. Ужгород : Вид-во УжНУ «Говерла», 2008. С. 113–119.

107. Матвієнків С. М. Інформаційний простір сучасної України: законодавчий аспект. *Держава і право: Збірник наукових праць. Серія Політичні науки.* Випуск 83. Київ : Вид-во «Юридична думка», 2019. С. 74–84.

108. Матвієнків С. М., Шмаленко Ю. І., Кольцов В. М. Національний інформаційний простір України: проблеми та перспективи розвитку. *Актуальні проблеми філософії та соціології*. 2022. Вип. 37. С. 223–227.

109. Мельничук В. В., Горохова Л. В. Критичне мислення як складова інформаційної безпеки. *Вісник Львівського університету. Сер.: філософські науки*. 2022. №29. С. 7–13.

110. Мєлєкєсцев К. І. Про трактування інформаційної війни: від технічно-кібернетичної до історико-психологічної парадигми. *Південний архів (історичні науки).* 2022. № 38. С. 62-67.

111. Міненко Є. С. Розвиток інститутів інформаційної безпеки сучасної України як чинник суспільно-політичної стабільності. дис.. за спец. Політологія. Український державний університет імені Михайла Драгоманова, Київ, 2024. 257 с.

112. Михальчук В. Спеціальні інформаційні операції в контексті інформаційних війн. *Науковий часопис Українського державного університету імені Михайла Драгоманова. Серія 2. Комп'ютерно-орієнтовані системи навчання*. 2009. №7 (14). С. 207-210.

113. Младьонова О. Д. Інформаційна безпека як складова національної безпеки України. *Вісник Харківського національного університету імені В.Н. Каразіна. Серія "Питання політології".* 2017. №31. С. 87–92.

114. Монолатій І. Зоосад революції. Західноукраїнська державність 1918–1923 років і теорії випадковостей XX – початку XXI сторіч. Івано-Франківськ: Лілея-НВ, 2020. 352 с.

115. Монолатій І. Між «реліктовим» і «етнічним» регіоном: західноукраїнські ідентичності в етнополітичній ретроспективі. *Вісник Прикарпатського університету. Серія: Політологія*. 2024. Випуск 17. С. 155–170.

116. Монолатій І. «Чорні лебеді» Української революції: (не)ймовірні випадки західноукраїнської державності. *Український історичний журнал*. 2020. №6 (555). С. 120–138.

117. Мороз О. Як не стати овочем. Інструкція з виживання в інфопросторі Харків: Віват, 2021. 208 с. (Серія «Актуальна тема», ISBN 978-617-690-089-4).

118. Мороз Ю., Твердохліб Ю. Інформаційно-психологічні операції в умовах ведення гібридної війни. *Вісник Львівського університету. Серія міжнародні відносини*. 2016. Вип. 38. С. 97–105.

119. Москаленко В. В. Особливості когнітивного компоненту творчого мислення в процесі розв'язання суб'єктом надситуативної проблемності. *Актуальні проблеми психології*. Том VI: Психологія обдарованості. 2019. Вип. 15. С. 107–113.

120. Наумкіна С. М., Кокорєв О. В., Тарасов А. В. Політико-правові основи людського виміру національної безпеки України: стратегії виживання та протидії когнітивним загрозам. *Політичне життя*. 2025. № 3. С. 98–102.

121. Національна безпека України в реаліях масштабної військової агресії : колективна монографія / Д. А. Біленець, В. С. Веселий, К. А. Возняковська, Т. А. Латковська та ін. ; за заг. ред. К. А. Возняковської. Чернівці, 2024. 380 с.

122. Некрасов А. О. Пропаганда як предмет дослідження. Матеріали звітної науково-практичної конференції здобувачів вищої освіти і молодих учених «*Молодіжна наука КНУКіМ - 2021. Культурно-мистецька освіта у викликах часу»* (24 листопада 2021 року) [Текст] : зб. матеріалів конф. / Київ. нац. ун-т культури і мистецтв [та ін.]. Київ : КНУКіМ, 2021. С. 116–120.

123. Нерсесян Г. А. Інформаційні спецоперації в умовах війни в історії. *Вчені записки Таврійського національного університету імені В.І Вернадського*. Серія: Державне управління. 2018. № 1. С. 223–228.

124. 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.

125. Нечай Л. О. Інформаційна безпека суб'єктів господарювання та фактори її розвитку. *Управління розвитком*. 2013. № 17. С. 145–148.

126. Новікова О. Ф. Формування соціальної безпеки людини на засадах резільєнтності в умовах гібридної війни. *Соціальна безпека людини в умовах*

війни: сутність, особливості та шляхи забезпечення : матеріали круглого столу 28–30 червня 2023 р. Київ – Одеса : Знання України, 2023. С. 54–61.

127. Новицький В. А. Генеза поняття «інформаційна безпека»: походження та становлення. *Вчені записки ТНУ імені В.І. Вернадського. Серія: Публічне управління та адміністрування*. 2024. № 35(74). С. 38–44.

128. Новоскольцева Л., Меженська О., Бадер А. Когнітивна стійкість як складова оборонного потенціалу: проблема інформаційної вразливості Збройних Сил України. *Вісник Львівського університету. Серія філос.-політол. студії.* 2025. Вип. 59. С. 353–359.

129. Основні поняття. НД ТЗІ 1.1-003-99: Термінологія в галузі захисту інформації в комп'ютерних системах від несанкціонованого доступу. Київ : Департамент спеціальних телекомунікаційних систем та захисту інформації Служби безпеки України, 1999. URL: https://tzi.ua/assets/files/1.1_003_99.pdf (дата звернення: 10.09.2023).

130. Остроухов В., Петрик В. До проблеми забезпечення інформаційної безпеки України. *Політичний менеджмент*. 2008. № 4. С. 135–141.

131. Оцінка громадянами ситуації в країні, довіра до соціальних інститутів, політиків, посадовців та громадських діячів (травень 2023 р.) / Центр Разумкова. Київ: Центр Разумкова, 2023. URL: https://razumkov.org.ua/napriamky/sotsiologichni-doslidzhennia/otsinka-gromadianamy-sytuatsii-v-kraini-dovira-do-sotsialnykh-instytutiv-politykiv-posadovtsiv-ta-gromadskykh-diiachiv-traven-2023r (дата звернення: 10.12.2025).

132. Оцінка ситуації в країні, довіра до соціальних інститутів, політиків, посадовців та громадських діячів, ставлення до виборів під час війни, віра в перемогу (лютий–березень 2025 р.) / Центр Разумкова. Київ: Центр Разумкова, 2025. URL: https://razumkov.org.ua/napriamky/sotsiologichni-doslidzhennia/otsinka-sytuatsii-v-kraini-dovira-do-sotsialnykh-instytutiv-politykiv-posadovtsiv-ta-gromadskykh-diiachiv-stavlennia-do-vyboriv-pid-chas-viiny-vira-v-peremogu-liutyiberezen-2025r (дата звернення: 10.12.2025).

133. Пашковський В. Ф. Ідентифікація політико-правових механізмів інформаційної безпеки держави в умовах гібридної війни. *Політичне життя.* 2025. № 3. С. 114–120.

134. Перемога на виборах: технології, кампанії, принципи: практичний посібник. [Городок М. Д., Карташов А. В., Романенко Є. О., Стасюк В. Ю.], за заг. ред. М. Д. Городка. Київ : 2016. 264 с.

135. Перепелиця Г. Російсько-український конфлікт: гібридний мир проти гібридної війни. *Універсум*. 2017. № 1-2. С. 34.

136. Петренко Л. А. Логіка еволюції узагальнюючих макроекономічних показників. *Формування ринкової економіки*: зб. наук. праць. 2009. №22. URL: http://www.nbuv.gov.ua/portal/Soc_Gum/fre/2009_22.pdf (дата звернення: 10.09.2025).

137. Петрик В. Сутність інформаційної безпеки держави, суспільства та особи. URL: http://www.justinian.com.ua/article.php?id=3222 (дата звернення: 10.10.2025).

138. Покровська А. В. Когнітивна стійкість в контексті протидії терористичній загрозі. *Актуальні проблеми управління інформаційною безпекою держави* : зб. тез наук. доп. наук.-практ. конф. (Київ, 30 березня 2018 р.). Київ : Нац. акад. СБУ, 2018. С. 260–262.

139. Почепцов Г. Війна в когнітивному просторі. *Ї: журнал*. 2017. URL: https://www.ji-magazine.lviv.ua/2017/Pocheptsov_Vijna_v_kognityvnomu_ prostori.htm (дата звернення: 11.06.2025).

140. Почепцов Г. Когнітивний простір та інформаційні війни. *Media Sapiens*. 20 серпня 2017. URL: http://osvita.mediasapiens.ua/trends/1411978127/kognitivnoe_prostranstvo_i_informatsionnye_voyny/ (дата звернення: 11.06.2025).

141. Про Доктрину інформаційної безпеки України: Указ Президента України № 514/2009 від 08.07.2009. URL: https://zakon.rada.gov.ua/laws/show/514/2009 (дата звернення: 01.05.2024).

142. Про Доктрину інформаційної безпеки: Указ Президента України №47/2017 від 25. 02. 2017 року. URL: https://www.president.gov.ua/documents/472017-21374 (дата звернення: 01.05.2024).

143. Про інформацію: Закон України № 2657-XII в редакції від 14.06.2025. URL: https://zakon. rada.gov.ua/laws/show/2657-12#Text (дата звернення: 12.12.2025).

144. Про медіа: Закон України № 2849-IX від 13.12.2022. URL: https://zakon.rada.gov.ua/laws/show/2849-20#Text (дата звернення: 12.12.2024).

145. Про національну безпеку України: Закон України № 2469-VIII від 21. 06. 2018. URL: https://zakon.rada.gov.ua/laws/show/2469-20#Text (дата звернення: 12.12.2024).

146. Про основи національної безпеки України: Закон України № 964-IV від 19. 06. 2003. URL: https://zakon.rada.gov.ua/laws/show/964-15#Text (дата звернення: 12.12.2024).

147. Про основні засади державної політики у сфері утвердження української національної та громадянської ідентичності: Закон України №2834-IX від 13.12.2022. URL: https://zakon.rada.gov.ua/laws/show/2834-20#Text (дата звернення: 12.12.2024).

148. Про правовий режим воєнного стану: Закон України № 389-VIII від 12. 05. 2015. URL: https://zakon.rada.gov.ua/laws/show/389-19#Text (дата звернення: 12.12.2024).

149. Про рішення Ради національної безпеки і оборони України від 2 вересня 2015 року «Про нову редакцію Воєнної доктрини України» : Указ Президента України № 555 від 24.09.2015 URL: https://zakon.rada.gov.ua/laws/show/555/2015#Text (дата звернення: 12.12.2024).

150. Про рішення Ради національної безпеки і оборони України від 25 березня 2021 року “Про Стратегію воєнної безпеки України”: Указ Президента України від 25.03.2021 №121/202. Офіційний вісник Президента України: офіц.

вид. від 02.04.2021. № 9. С. 122. Ст. 370. URL: https://zakon.rada.gov.ua/laws/show/121/2021#Text17 (дата звернення: 12.12.2024).

151. Про рішення Ради національної безпеки і оборони України від 15 жовтня 2021 року «Про Стратегію інформаційної безпеки» : Указ Президента України № 685/2021 від 28.12.2021. URL: https://zakon.rada.gov.ua/laws/show/685/2021#Text (дата звернення: 12.12.2024).

152. Про рішення Ради національної безпеки і оборони України від 14 травня 2021 року «Про Стратегію кібербезпеки України»: Указ Президента України № 447/2021 від 26 серпня 2021. URL: https://www.president.gov.ua/documents/4472021-40013 (дата звернення: 12.12.2024).

153. Про рішення Ради національної безпеки і оборони України від 06.05.2015 «Про Стратегію національної безпеки України» : Указ Президента України № 287/2015 від 26.05.2015. *Офіційний вісник Президента України: офіц. вид.* 03.06.2015. № 13. С. 50. Ст. 874. URL: https:// zakon.rada.gov.ua/laws/show/287/2015/paran29#n29 (дата звернення: 12.12.2024).

154. Про рішення Ради національної безпеки і оборони України від 14 вересня 2020 року «Про Стратегію національної безпеки України» : Указ Президента України №392/2020. URL: https://president. gov.ua/documents/3922020-35037 (дата звернення: 12.12.2024).

155. Про рішення Ради національної безпеки і оборони України від 2 вересня 2015 року «Про нову редакцію Воєнної доктрини України» : указ Президента України від 24 вересня 2015 р. № 555. URL: https://zakon.rada.gov.ua/laws/show/555/2015#Text (дата звернення: 12.12.2024).

156. Про схвалення Концепції Державної цільової соціальної програми з утвердження української національної та громадянської ідентичності на період до 2028 року: Розпорядження КМУ № 141-р. від 16 лютого 2024. URL: https://zakon.rada.gov.ua/laws/show/141-2024-%D1%80#Text (дата звернення: 12.12.2024).

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

158. Птащенко О. В. Політика боротьби з дезінформацією: виклики для національної безпеки України. *Public Management and Policy*. 2024. № 2. С. 48–55.

159. Результати дослідження «Оцінка власного психологічного стану українцями», вересень 2022 р. URL: https://gradus.app/documents/308/Gradus_Research___Mental_Health_Report_short_version.pdf (дата звернення: 01.12.2024).

160. Різник Н. С. Теоретичні засади формування системи діагностики економічної безпеки банку. *Вісник Харківського національного технічного. університету сільського господарства: Економічні науки.* Харків: ХНТУСГ, 2007. Вип. 66. С. 118-123.

161. Ротар Н. Діджиталізація політичної участі громадян Європейського Союзу як інструмент подолання дефіциту демократії. *Історико-політичні проблеми сучасного світу.* 2022. № 45. С. 163–175.

162. Рущенко І. П., Зубар Н. В. Війна інформації. *Оборонний вісник.* 2017. № 8. С. 4–9.

163. Сардак А. Феномен національної ідентичності в умовах інформаційної війни. *Журнал соціальної та практичної психології.* 2024. № 3. С. 87–91.

164. Сащук Г. Інформаційна безпека в системі забезпечення національної безпеки. *Бізнес і безпека.* 2014. № 1. С. 46–50.

165. Северина С. В. Інформаційна безпека та методи захисту інформації. *Вісник Запорізького нац. ун-ту. Економічні науки.* 2016. № 1. С. 155–161.

166. Селіна М. Б. Спеціальна інформаційна операція: історія становлення. *Часопис Київського університету права*. 2019. № 4. С. 132–137.

167. Сікора Л. С., Лиса Н. К., Ткачук Р. Л. Когнітивні та інформаційні технології підтримки прийняття рішень для оперативного управління при

нечіткості ситуаційних даних. *Комп'ютерні технології друкарства.* 2020. № 2. С. 15–24.

168. Сила Західноукраїнської Народної Республіки: вибрані питання потенціалу, безпеки і дипломатії держави. Івано-Франківськ: Лілея-НВ, 2020. 88 с.

169. Сніцаренко П. М. Інформаційна операція Збройних Сил України як інтегруюча форма воєнних дій в інформаційному просторі. *Наука і оборона.* 2020. № 1. С. 37–42.

170. Сопілко І. М. Інформаційна безпека та кібербезпека: порівняльно-правовий аспект. *Наукові праці Нац. авіаційного ун-ту. Серія: Юридичний вісник «Повітряне і космічне право».* 2021. № 2(59). С. 110–115.

171. Спасітєлєва С., Жданова Ю., Чичкань І. Проблеми безпеки універсальних платформ управління даними. *Кібербезпека: освіта, наука, техніка.* 2019. Вип. 2(6). С. 122–133.

172. Стрельбицький М., Гринь М. Когнітивна війна росії проти України. *Наукові праці Міжрегіональної Академії управління персоналом. Юридичні науки*. 2023. № 1 (64). С. 46–52.

173. Тараненко Г. Г. Когнітивна безпека як вимір російсько-української війни. *Політологічний вісник.* 2024. № 92. С. 371–382.

174. Ткаченко В. В. Стандарти вищої освіти у сфері кібербезпеки – важливий інструмент модернізації освітнього процесу та запорука національної безпеки України. *Актуальні проблеми управління інформаційною безпекою держави* : зб. матеріалів наук.-практ. конф. Київ : Нац. акад. СБУ, 2017. С. 135–137.

175. Топчій О. Види інформаційної безпеки неповнолітніх: новий погляд на усталені підходи. *Jurnalul juridic national: teorie şi practică*. 2019. Вип. 35(1). С. 122–126.

176. Троян С. С. Спеціальні інформаційні операції. Велика українська енциклопедія. URL: https://vue.gov.ua/Спеціальні інформаційні операції (дата звернення: 01.12.2024).

177. Федоров В. Д. Когнітивна війна як елемент гібридної агресії: інструменти та методи протидії. *Інформаційна безпека: виклики та рішення.* 2023. № 2 (10). С. 108–117.

178. Фурашев В. М. Сутність та визначення понять «інформаційна безпека» і «безпека інформації». *Правова інформатика*. 2012. № 2. С. 51–59.

179. Фурашев В. М., Ланде Д. В. Інформаційні операції крізь призму системи моніторингу та інтеграції інтернет ресурсів. *Правова інформатика*. 2009. № 2(22). С. 49–57.

180. Харченко С. О. Наукові підходи до класифікації загроз інформаційній безпеці. *Держава та регіони. Серія: Державне управління*. 2019. № 2 (66). URL: http://pa.stateandregions.zp.ua/archive/2_2019/35.pdf (дата звернення: 01.12.2024).

181. Хроніка війни, день третій. Битва за Київ. *Forbes Ukraine.* Лютий 2022. URL: https://forbes.ua/news/khronika-viyni-den-tretiy-bitva-za-kiiv-tilki-perevirena-informatsiya-26022022-3912 (дата звернення: 01.12.2024).

182. Шевців М. Б., Гончарук К. А. Пропаганда як соціально-політичне явище: проблеми розуміння. *Південноукраїнський правничий часопис*. 2019. № 1. С. 119–122.

183. Шевченко С. М., Жданова Ю. Д., Гаркушелко А. М. Когнітивний підхід в інформаційній та кібербезпеці. *Кібербезпека: освіта, наука, техніка.* 2025. №1 (29). С. 854–866.

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

185. Шопін А. Ю. Інформаційна безпека як фактор забезпечення конкурентоспроможності підприємства. *Управління розвитком.* 2013. № 17. С. 155–157.

186. Шугаєв А. В. Феномен інформаційної війни. *Вчені записки ТНУ імені В. І. Вернадського. Серія: Філологія. Соціальні комунікації*. 2019. № 4 (2). С. 151–156.

187. Яворська Г. М. Гібридна війна як дискурсивний конструкт. *Стратегічні комунікації.* 2016. № 4 (41). С. 41–48.

188. Як регулюють штучний інтелект у ЄС та Україні: огляд ключових ініціатив. *Manimama.* 2025. URL: https://manimama.eu/uk/yak-regulyuyut-shtuchnij-intelekt-u-yes-ta-ukrayini-oglyad-klyuchovih-initsiativ/ (дата звернення: 01.12.2025).

189. Юринець Ю. Л., Сопілко І. М., Бєлкін Л. М., Бєлкін М. Л. Дослідження проблем інформаційної безпеки України на засадах міждисциплінарного підходу: соціологія, психологія, право. *Юридичний науковий електронний журнал. Електронне наукове фахове видання.* 2020. № 7. С. 300-307.

190. A Primer on Russian Cognitive Warfare. Institute for the Study of War. 2025. URL: https://understandingwar.org/research/cognitive-warfare/a-primer-on-russian-cognitive-warfare/ (дата звернення: 11.11.2025).

191. Abraham D., Houmb S. H., Erdodi L. Cyber-Attacks on Energy Infrastructure. *A Literature Overview and Perspectives on the Current Situation. Applied Sciences*. 2025. Vol. 15. № 17. P. 9233.

192. Alieva I., Ng L., Carley K. Investigating the Spread of Russian Disinformation about Biolabs in Ukraine on Twitter Using Social Network Analysis. 2022 IEEE International Conference on Big Data (Big Data). 2022. URL: https://ieeexplore.ieee.org/document/10020223 (дата звернення: 01.11.2023).

193. Analysis of methods, methods, mechanisms, tools theories of decision-making for modeling information protection system / O. Avtushenko et al. *Cybersecurity: Education, Science, Technique*. 2022. Vol. 16. № 4. P. 159–171.

194. Army cyber institute at West Point. URL: https://cyber.army.mil/Research/Research-Labs/Cognitive-Security/ (дата звернення: 02.09.2023).

195. Armstrong M. Data as a Weapon: Psychological Operations in the Age of Irregular Information Threats. Modern War Institute. 2022. URL: https://mwi.westpoint.edu/data-as-a-weapon-psychological-operations-in-the-age-

of-irregular-information-threats (дата звернення: 02.09.2023).

196. Bachmann S.-D. D., Putter D., Duczynski G. Hybrid warfare and disinformation: A Ukraine war perspective. *Global Policy*. 2023. Vol. 14, № 5. P. 858–869.

197. Bahar H. M. Social media and disinformation in war propaganda: how Afghan government and the Taliban use Twitter. *Media Asia*. 2020. №47 (1-2). P.34–46.

198. Baker K. What is Cognitive Security? Protecting Your Mind in the Age of AI. URL: https://em360tech.com/tech-articles/what-cognitive-security-protecting-your-mind-age-ai (дата звернення: 02.10.2024).

199. Balan S., Balan L., Vorotynskyy V., Rybak I., Tarasiuk V. State Information Policy in the Context of Hybrid Threats: Legal and Political Aspects. *Social & Legal Studies*. 2024. № 8 (1). P. 165–178.

200. Beverley J., Limbaugh D. Ontological Foundations of State Sovereignty [Preprint]. arXiv. 2025. URL: https://arxiv.org/abs/2507.21172 (дата звернення: 02.09.2023).

201. Beznosiuk M. Russian Hybrid Warfare: Ukraine's Success Offers Lessons for Europe. Atlantic Council. 2022. URL: https://www.atlanticcouncil.org/blogs/ukrainealert/russian-hybrid-warfare-europe-should-study-ukraines-unique-experience/ (дата звернення: 02.02.2024).

202. Bidova B. B., Belyaeva G. S., Yakhyaeva M. U. National Interests and Their Relationship to the Law. In: Social and Cultural Transformations in the Context of Modern. *Globalism. European Proceedings of Social and Behavioural Sciences.* 2021. Vol. 117. P. 262–270.

203. Bilal A. Hybrid Warfare - New Threats, Complexity, and «Trust» as the Antidote. Official site of NATO. 2021. URL: https://www.nato.int/docu/review/articles/2021/11/30/hybrid-warfare-new-threats-complexity-and-trust-as-the-antidote/index.html (дата звернення: 20.04.2024).

204. Bjola C., Papadakis K. Digital propaganda, counterpublics, and the disruption of the public sphere: The Finnish approach to building digital resilience.

Cambridge Review of International Affairs. 2019. №33 (1). URL: https://www.tandfonline.com/doi/full/10.1080/09557571.2019.1704221?utm_source=researchgate.net&utm_medium=article (дата звернення: 20.04.2024).

205. Bösch M., Divon T. The sound of disinformation: TikTok, computational propaganda, and the invasion of Ukraine. *New Media & Society*. 2024. Vol. 26. № 9. P. 5081–5106.

206. Casino F. Unveiling the Multifaceted Concept of Cognitive Security: Trends, Perspectives, and Future Challenges. *Technology in Society*. 2025. Vol. 83. 102956. URL: https://www.sciencedirect.com/science/article/pii/S0160791X25001460 (дата звернення: 20.10.2025).

207. Castells M. The Rise of the Network Society, with a New Preface: Volume I. The Information Age: Economy, Society, and Culture. Wiley-Blackwell, 2010. 656 p.

208. CCDCOE. IT Army of Ukraine's Cyber Campaign against Targets in Russia (since 2022). 2025. URL: https://cyberlaw.ccdcoe.org/wiki/IT_Army_of_Ukraine%E2%80%99s_cyber_campaign_against_targets_in_Russia_(since_2022) (дата звернення: 20.04.2024).

209. Cimbala S. J. Countering cognitive warfare: awareness and resilience. NATO Review. 2021. URL: https://www.nato.int/docu/review/articles/2021/05/20/countering-cognitive-warfare-awareness-and-resilience/index.html (дата звернення: 20.12.2022).

210. Claverie B., du Cluzel F. The Cognitive Warfare Concept. NATO ACT Innovation Hub. 2021. URL: https://innovationhub-act.org/wp-content/uploads/2023/12/CW-article-Claverie-du-Cluzel-final_0.pdf (дата звернення: 20.04.2024).

211. Cheatham M. J., Geyer A. M., Nohle P. A., Vazquez J. E. Cognitive Warfare: The Fight for Gray Matter in the Digital Gray Zone. Joint Force Quarterly. 2024. № 114. P. 84–91.

212. Correcting misinformation about the Russia-Ukraine War reduces belief in false claims. PMC, 2024. URL: https://pmc.ncbi.nlm.nih.gov/articles/PMC11419341/ (дата звернення: 14.04.2024).

213. Danyk Y., Briggs C. M. Modern Cognitive Operations and Hybrid Warfare. Journal of Strategic Security. 2023. Vol. 16, № 1. P. 1–24.

214. Decoding manipulative narratives in cognitive warfare: a case study. Frontiers in AI. 2025. URL: https://www.frontiersin.org/journals/artificial-intelligence/articles/10.3389/frai.2025.1566022/full (дата звернення: 20.10.2025).

215. Denisa-Liepniece S. With Media Literacy Towards Cognitive Resilience: Updates from the Baltic States, and Lessons Learned from Ukraine, Moldova, and Georgia. 2022. URL: https://bcme.eu/wp-content/uploads/2025/04/ML_Policy_Brief_2022.pdf (дата звернення: 04.11.2022).

216. Deppe C., Schaal G. S. Cognitive warfare: a conceptual analysis of the NATO ACT cognitive warfare exploratory concept. *Front. Big Data.* 2024. Vol. 7. URL: https://public-pages-files-2025.frontiersin.org/journals/big-data/articles/10.3389/fdata.2024.1452129/pdf (дата звернення: 04.12.2024).

217. Dickinson P. Wartime Ukraine Ranks Among World's Top Performers in Anti-Corruption Index. UkraineAlert, Atlantic Council. 2024. URL: https://www.atlanticcouncil.org/blogs/ukrainealert/wartime-ukraine-ranks-among-worlds-top-performers-in-anti-corruption-index/ (дата звернення: 04.12.2024).

218. Disinformation about the blackout went around the world. EDMO. 2025. URL: https://edmo.eu/publications/disinformation-about-the-blackout-went-around-the-world-impersonated-media-rare-atmospheric-phenomenon-and-russian-networks/ (дата звернення: 04.10.2025).

219. Disinformation Stops With You. Cybersecurity and Infrastructure Security Agency. Washington: Cybersecurity and Infrastructure Security Agency, 2020. URL: https://www.cisa.gov/sites/default/files/publications/disinformation_stops_with_you_infographic_set_508.pdf (дата звернення: 04.12.2024).

220. DHS Needs a Unified Strategy to Counter Disinformation Campaigns: звіт / Office of Inspector General, Department of Homeland Security. – Washington:

Office of Inspector General, 2022. OIG-22-58. URL: https://www.oig.dhs.gov/sites/default/files/assets/2022-08/OIG-22-58-Aug22.pdf (дата звернення: 08.12.2023).

221. Ehrett C., Linvill D. L., Smith, H., Warren P. L., Bellamy L., Moawad M., Moody M. Inauthentic newsfeeds and agenda setting in a coordinated inauthentic information operation. Social Science Computer Review. 2022. № 40(6). P. 1595–1613.

222. Enhancing Cognitive Security and Societal Resilience: Countering Cognitive Warfare. GCSP, 2025. URL: https://www.gcsp.ch/publications/enhancing-cognitive-security-and-societal-resilience-counter-cognitive-warfare (дата звернення: 09.11.2025).

223. European Union Institute for Security Studies. Smoke and mirrors: Building EU resilience against manipulation through cognitive security. EUISS, 2024. URL: https://www.iss.europa.eu/publications/briefs/smoke-and-mirrors-building-eu-resilience-against-manipulation-through-cognitive (дата звернення: 20.12.2024).

224. Fact-checking the war in Ukraine, or when the screens have become battlefields. EDMO. 2023. URL: https://edmo.eu/blog/fact-checking-the-war-in-ukraine-or-when-the-screens-have-become-battlefields/ (дата звернення: 08.12.2023).

225. Foreign Disinformation: Defining and Detecting Threats: звіт / U.S. Government Accountability Office. Washington: U.S. Government Accountability Office, 2024. GAO-24-107600. URL: https://www.gao.gov/assets/gao-24-107600.pdf (дата звернення: 10.12.2024).

226. Foucault M. Discipline and Punish: The Birth of the Prison (A. Sheridan, Trans.). Vintage Books, 1995. 333 p.

227. Gates R. A. Balanced Strategy: Reprogramming the Pentagon for a New Age. *Foreign Affairs.* 2009. 44 p.

228. Gies Business reaches 33K learners in Ukraine through free online courses. University of Illinois. 2024. URL:

https://giesonline.illinois.edu/news/2024/09/11/gies-business-reaches-33k-learners-in-ukraine-through-free-online-courses (дата звернення: 10.12.2024).

229. Habermas J. The Theory of Communicative Action: Reason and the Rationalization of Society, Volume 1. Beacon Press, 1984. 465 p.

230. How Ukraine uses AI to fight Russian information operations. Global Governance. 2024. URL: https://www.globalgovernance.eu/publications/how-ukraine-uses-ai-to-fight-russian-information-operations (дата звернення: 10.12.2024).

231. Huang R.Y., Zheng Z.Q., Shang Y. On challenges of AI to cognitive security and safety. *Security and Safety*. 2023. № 2. URL: https://sands.edpsciences.org/articles/sands/full_html/2023/01/sands20230010/sands20230010.html (дата звернення: 10.12.2024).

232. Institute for the Study of War. A Primer on Russian Cognitive Warfare. ISW, 2025. URL: https://understandingwar.org/research/cognitive-warfare/a-primer-on-russian-cognitive-warfare/ (дата звернення: 10.12.2025).

233. Klymonchuk V., Matviienkiv S., Boychuk I., Dotsiak I., Trebyk L. The role of mass media in the information security public management system: El papel de los medios de comunicación en el sistema de gestión pública de la seguridad de la información. *Cuestiones Políticas.* 2023. №41(78). P. 612–627.

234. Klymonchuk V., Matviienkiv S., Buslenko V., Rozik M., Anisimovych-Shevchuk O. The Role of Information Policy in Shaping Public Opinion on Corruption in the Visegrad Group Countries. *Pakistan Journal of Criminology*. 2024. Vol. 16, № 02. P. 189–204.

235. Kott A., Paziuk A., Galaitsi S. E., Trump B. D., Linkov I. Russian Cyber Onslaught Was Blunted by Ukrainian Cyber Resilience, Not Merely Security. 2024. arXiv preprint arXiv:2408.14667. URL: https://arxiv.org/pdf/2408.14667 (дата звернення: 17.12.2024).

236. Kravchenko O., Veklych V., Krykhivskyi M., Madryha T. Cybersecurity in the face of information warfare and cyberattacks. *Multidisciplinary Science Journal*.

2024. №6. 2024ss0219. URL: https://malque.pub/ojs/index.php/msj/article/view/1938 (дата звернення: 10.12.2025).

237. Kumar N., Kundu A. SecureVision: Advanced Cybersecurity Deepfake Detection with Big Data Analytics. Sensors (Basel). 2024. Vol. 24. № 19. P. 6300. URL: https://www.mdpi.com/1424-8220/24/19/6300 (дата звернення: 10.12.2025).

238. Kurylo B. Ukrainian Civil Society Has Redefined Security in Wartime. LSE EUROPP Blog. 2025. URL: https://blogs.lse.ac.uk/europpblog/2025/09/18/ukrainian-civil-society-has-redefined-security-in-wartime/ (дата звернення: 10.12.2025).

239. Lenz T., Burilkov A., Viola L. A. Legitimacy and the Cognitive Sources of International Institutional Change: The Case of Regional Parliamentarization. *International Studies Quarterly*. 2019. Vol. 63, № 4. P. 1094–1107.

240. Lenz T., Viola L. A. Legitimacy and Institutional Change in International Organisations: A Cognitive Approach. *Review of International Studies*. 2017. Vol. 43, № 5. P. 939–961.

241. Lessons from the Ukraine Conflict: Modern Warfare in the Age of Autonomy, Information, and Resilience. CSIS. 2025. URL: https://www.csis.org/analysis/lessons-ukraine-conflict-modern-warfare-age-autonomy-information-and-resilience (дата звернення: 10.12.2025).

242. Linvill D. L., Warren P. L. Engaging with others: How the IRA coordinated information operation made friends. *Harvard Kennedy School Misinformation Review*. 2020. № 1(2). URL: https://misinforeview.hks.harvard.edu/article/engaging-ira-coordinated-information-operation/ (дата звернення: 10.12.2022).

243. Lytvynenko J. I Can’t Stop Watching a Livestream of Kyiv. The Atlantic. 2022. URL: https://www.theatlantic.com/author/jane-lytvynenko/ (дата звернення: 10.08.2024).

244. Malhan M., Dewani P. P. Propaganda as communication strategy: Historic and contemporary perspective. *Academy of Marketing Studies Journal*. 2020. № 24 (4). P. 1-15.

245. Manufacturing Impunity: Russia's Use of Information Alibis and How They Materially Contribute to the Planning, Execution and Cover-up of International Crimes. Global Rights Compliance, The Reckoning Project. 2025. URL: https://globalrightscompliance.org/manufacturing-impunity-russian-information-operations-in-ukraine/ (дата звернення: 10.10.2025).

246. Mattis J. N., Hoffman F. Future Warfare: The Rise of Hybrid Wars. U.S. Naval Institute. 2005. Vol. 131. URL: https://www.usni.org/magazines/proceedings/2005/november/future-warfare-rise-hybrid-wars (дата звернення: 10.08.2025).

247. Mattingly D. C., Yao E. How soft propaganda persuades. Comparative Political Studies. 2022. №55(9). P. 1569-1594.

248. Monolatii I. The Western Ukrainian Statehood 1918–1923 and the Theories of Randomness in the 20th – early 21st Centuries. *Wschód Europy. Studia humanistyczno-społeczne.* Lublin, 2023. Vol.9 (2). P. 219–233.

249. Monti C., Aiello L. M., De Francisci Morales G., Bonchi F. The Language of Opinion Change on social media under the Lens of Communicative Action. Scientific Reports. 2022. №12(1), Article 17920. URL: https://www.nature.com/articles/s41598-022-21720-4 (дата звернення: 10.08.2025).

250. Morais R., Piñeiro-Naval V., Blanco-Herrero D. Beyond Information Warfare: Exploring Fact-Checking Research About the Russia–Ukraine War. *Journalism and Media*. 2025. Vol. 6. № 2. P. 48.

251. National Defense University. Cognitive Warfare: The Fight for Gray Matter in the Digital Gray Zone. NDU, 2023. URL: https://ndu.edu/News/Article-View/Article/3856627/cognitive-warfare-the-fight-for-gray-matter-in-the-digital-gray-zone/ (дата звернення: 10.08.2024).

252. National Survey of Ukraine (September–October 2024) / Sociological Group "Rating", Center for Insights in Survey Research (IRI). Kyiv: Sociological Group "Rating", 2024. URL: https://www.ratinggroup.ua/en/news/nationwide-survey-of-the-international-republican-institute-iri-october-2024 (дата звернення: 17.07.2025).

253. NATO. Information warfare. URL: https://www.nato.int/nato_ static_fl2014/assets/pdf/ 2020/5/pdf/2005-deepportal4-information-warfare.pdf (дата звернення: 10.08.2025).

254. NATO's ACT. Cognitive Warfare. NATO. 2023. URL: https://www.innovationhub-act.org/sites/default/files/2021-05/Cognitive%20Warfare%20%20The%20battle%20for%20your%20brain.pdf (дата звернення: 10.08.2024).

255. Nikoula D., McMahon D. Cognitive Warfare: Securing Hearts and Minds. University of Ottawa Information Integrity Lab. 2024. URL: https://infolab.uottawa.ca/common/Uploaded%20files/PDI%20files/InfoLab%20-%20Cognitive%20Warfare%2C%20Securing%20Hearts%20and%20Minds.pdf (дата звернення: 10.08.2024).

256. OECD. Government at a Glance 2025: Estonia / OECD. – Paris: OECD Publishing, 2025. URL: https://www.oecd.org/en/publications/government-at-a-glance-2025-country-notes_da3361e1-en/estonia_89797d03-en.html (дата звернення: 10.08.2025).

257. OECD Digital Government Index: Results and Key Findings / OECD Public Governance Policy Papers. Paris: OECD Publishing, 2024. 38 p.

258. Office of Inspector General, Department of Homeland Security (*DHS needs a unified strategy to counter disinformation campaigns* (OIG-22-58). Office of Inspector General. 2022. URL: https://www.oig.dhs.gov/sites/default/files/assets/2022-08/OIG-22-58-Aug22.pdf (дата звернення: 07.08.2025).

259. Parachini J. Debunking Russian Lies About Biolabs at Upcoming U.N. Meetings. RAND Corporation. 2022. URL: https://www.rand.org/pubs/commentary/2022/09/debunking-russian-lies-about-biolabs-at-upcoming-un.html (дата звернення: 10.07.2024).

260. Parsons T. The Social System. Routledge & Kegan Paul Ltd, 1951. 575 p.

261. Paziuk A., Lande D., Shnurko-Tabakova E., Kingston P. Decoding manipulative narratives in cognitive warfare: a case study of the Russia-Ukraine conflict. *Frontiers in Artificial Intelligence.* 2025. Vol. 8. URL: https://www.frontiersin.org/journals/artificial-intelligence/articles/10.3389/frai.2025.1566022/full (дата звернення: 10.12.2025).

262. Pohle J. Social Networks, Functional Differentiation of Society, and Data Protection. ResearchGate. 2012. URL: https://www.researchgate.net/publication/225307670_Social_Networks_Functional_Differentiation_of_Society_and_DataProtection (дата звернення: 10.09.2025).

263. Rajamae-Soosaar K., Nikiforova A. Bridging the Gap: Unravelling Local Government Data Sharing Barriers in Estonia and Beyond. 2024. URL: https://arxiv.org/pdf/2406.08461v2.pdf (дата звернення: 10.09.2025).

264. Revutska S., Ostapenko S., Udovichenko H., Dmytruk L. Language and national identity as a foreword for ensuring national security. *Challenges and paradigm of national and international security of the XXI century:* economic and technogenic discourse, chapter 2, 2022. P. 26-42.

265. Ruohonen J. The Treachery of Images in the Digital Sovereignty Debate. *Minds and Machines*. 2021. № 31(3). P. 439–456.

266. Russia's Digital Battlefield: A New Front in Information Warfare. International Relations Review. 2025. URL: https://www.irreview.org/articles/2025/8/28/russias-digital-battlefield-a-new-front-in-information-warfare (дата звернення: 10.09.2025).

267. Russia's Manipulation of Telegram: A Case Study of Foreign Information Manipulation and Interference (FIMI). Community Democracies. 2025. URL: https://community-democracies.org/app/uploads/2025/01/Russia-Manipulation-Telegram-X.pdf (дата звернення: 10.09.2025).

268. Seven Security Scenarios on Russian War in Ukraine for 2025–2026. GLOBSEC. 2025. URL: https://www.globsec.org/what-we-do/publications/seven-security-scenarios-russian-war-ukraine-2025-2026-implications-and (дата звернення: 10.11.2025).

269. Stancu C., Cazanaru G. Psychological Operations in the Context of the War in Ukraine. *Revista Academiei Forțelor Terestre*. 2024. № 3. URL: https://www.armyacademy.ro/reviste/rev3_2024/Stancu_Cazanaru_RAFT_3_2024.pdf (дата звернення: 10.11.2025).

270. Taherdoost H. Cybersecurity vs. Information Security. *Procedia Computer Science.* 2022. № 215. P. 483–487.

271. The Russia-Ukraine Conflict From a Hybrid Warfare Cognitive Perspective. TDHJ, 2024. URL: https://tdhj.org/blog/post/russia-ukraine-hybrid-cognitive-warfare/ (дата звернення: 10.10.2024).

272. Telegram as a Battlefield: Kremlin-related Communications during the Russia-Ukraine Conflict. arXiv. 2025. URL: https://arxiv.org/html/2501.01884v3 (дата звернення: 10.11.2025).

273. Ukrainian bank's service for military donations targeted by 'massive' DDoS attack. The Record. 2024. URL: https://therecord.media/ukraine-monobank-ddos-attack-donations (дата звернення: 01.02.2025).

274. Walter N., Murphy S. T. How effective are TikTok misinformation debunking videos?. HKS Misinformation Review. 2025. URL: https://misinforeview.hks.harvard.edu/article/how-effective-are-tiktok-misinformation-debunking-videos/ (дата звернення: 01.02.2025).

275. Zakharchenko A. Advantages of the Connective Strategic Narrative during the Russian–Ukrainian War. *Frontiers in Political Science*. 2025. Vol. 7. URL: https://www.frontiersin.org/journals/political-science/articles/10.3389/fpos.2025.1434240 (дата звернення: 01.02.2025).

ДОДАТКИ

Додаток А

Список публікацій здобувача за темою дисертації та відомості про апробацію результатів дисертації

Статті у наукових фахових виданнях України категорії Б:

1. Кобець Т. Основні підходи до розуміння «когнітивна безпека» в сучасній науці: політичний та інформаційний аспект. *Вісник Львівського університету. Серія філософсько-політологічні студії.* 2023. Вип. 49. С.278–285.

DOI: https://doi.org/10.30970/PPS.2023.49.34

URL: http://fps-visnyk.lnu.lviv.ua/archive/49_2023/34.pdf

2. Кобець Т. Когнітивна безпека в умовах гібридної війни. *Вісник Прикарпатського університету. Серія: Політологія*. 2024. Випуск 17. С.67–73.

DOI: https://doi.org/10.32782/2312-1815/2024-17-9

URL: https://journals.pnu.if.ua/index.php/politology/article/view/116/114

3. Кобець Т. Аналіз загроз когнітивній безпеці українського суспільства: класифікаційні підстави. *Вісник Прикарпатського університету. Серія: Політологія.* 2024. Випуск 19. С.67–72.

DOI: https://doi.org/10.32782/2312-1815/2024-19-8

URL: https://journals.pnu.if.ua/index.php/politology/article/view/182/178

4. Кобець Т. Використання технологій інформаційних операцій у політичній практиці. *Літопис Волині*. 2024. № 31. С.134–139

DOI: https://doi.org/10.32782/2305-9389/2024.31.21

URL: http://litopys.volyn.ua/index.php/litopys/article/view/562/493

5.Кобець Т. Інформаційні спеціальні операції: особливості реалізації в сучасних умовах. *Вісник Прикарпатського університету. Серія: Політологія*. 2025. Випуск 20. С.256–263.

DOI: https://doi.org/10.32782/2312-1815/2025-20-30

URL: https://journals.pnu.if.ua/index.php/politology/article/view/246/241

Публікації, у періодичних наукових виданнях інших держав, які індексуються у базах даних Scopus:

6.Ivanytska B., Kobets T., Savchenko V., Pugachov V., Kursyk O. Countering Disinformation in the Hybrid Information Environment: A Cross-Sectoral Analysis of Public Policy, Education, and Media Strategies. *Ianna Journal of Interdisciplinary Studies*. 2026. № 8 (1). P.327–343.

DOI: https://doi.org/10.5281/zenodo.17710407

URL: https://scopus.com/pages/publications/105028731483?origin=resultslist

Наукові праці, які засвідчують апробацію матеріалів дисертації:

7.Кобець Ю. В., Кобець Т. А. Теоретико-методологічні підходи до дослідження політичної безпеки. *Політичні процеси сучасності: глобальний та регіональні виміри*. Збірник матеріалів IV Всеукраїнської науково-практичної конференції (м. Івано-Франківськ, 27-28 жовтня 2022 р.). Івано-Франківськ, 2022. С.45–51.

URL: https://kpol.pnu.edu.ua/wp-content/uploads/sites/102/2024/07/zbirnyk-materialiv-vseukrainskoi-konferentsii-politychni-protsesy-suchasnosti-hlobalnyj-ta-rehionalnyj-vymiry-27-28-zhovtnia-2022r.-ch-i.pdf

14. Кобець Т. Безпека в умовах воєнного стану. *Освітній процес в умовах війни та у повоєнний період: виклики, правила, перспективи* : матеріали всеукраїнського науково-педагогічного підвищення кваліфікації, 4 березня – 14 квітня 2024 року. Львів – Торунь : Liha-Pres, 2024. С.146–149.

URL:https://cuesc.org.ua/images/informlist/%D0%9C%D0%B0%D0%BA%D0%B5%D1%82%20advanced_training_UDU.pdf

15. Кобець Ю.В., Кобець Т.А. Когнітивна війна як сучасна форма ведення мережево-центричного протистояння. *Політичні процеси сучасності: глобальний та регіональний виміри*. Збірник матеріалів V Міжнародної науково-практичної конференції (м. Івано-Франківськ, 25-26 квітня 2024 р.). Івано-Франківськ, 2024. С.217–238.

URL: https://kpol.pnu.edu.ua/wp-content/uploads/sites/102/2024/12/zbirnyk-materialiv-v-mizhnarodnoi-naukovo-praktychnoi-konferentsii-politychni-protsesy-suchasnosti-hlobalnyj-ta-rehionalnyj-vymiry-2024r.pdf

16. Кобець Т. А. Вплив національної ідентичності на формування інформаційної та когнітивної безпеки українського суспільства. *Політичні процеси сучасності: глобальний та регіональні виміри :* збірник матеріалів VI Міжнародної науково-практичної конференції (м. Івано-Франківськ, 8–9 квітня 2025 р.). Електронне видання. Івано-Франківськ : Карпат. нац. ун-т ім. В.Стефаника, 2025. С.171–174.

URL: https://kpn.cnu.edu.ua/wp-content/uploads/sites/197/2025/11/zbirnyk-materialiv-vi-mizhnarodnoi-naukovo-praktychnoi-konferentsii.pdf

17. Кобець Т.А. Особливості верифікації даних журналістом в епоху штучного інтелекту. *Global Trends in the Development of Information Technology and Science:* Collection of Scientific Papers "International Scientific Unity" with Proceedings of the 3rd International Scientific and Practical Conference. April 2-4, 2025. Stockholm, Sweden. P. 135–138.

DOI: https://doi.org/10.70286/isu-02.04.2025

URL: https://isu-conference.com/wp-content/uploads/2025/04/Stockholm_Sweden_02.04.25.pdf

18. Кобець Т.А. Контекстуальна верифікація як елемент фактчекінгу. *Modern Scientific Research: Theoretical and Practical Aspects* (August 25-27, 2025, Riga, Latvia). European Open Science Space, 2025. P.48–52.

DOI: https://doi.org/10.70286/EOSS-25.08.2025

URL: https://www.eoss-conf.com/wp-content/uploads/ 2025/08/Riga_Latvia_25.08.25.pdf

Праці, які додатково відображають наукові результати дисертації:

19. Кобець Т. Порівняльний аналіз технологій пропаганди та контрпропаганди в умовах воєнного стану. *Вісник Прикарпатського університету*. Серія: Політологія. 2023. Випуск 15. С.33–42.

DOI: https://doi.org/10.32782/2312-1815/2024-1-5

URL: https://journals.pnu.if.ua/index.php/politology/article/view/51/50

Додаток Б

Методи інформаційно-психологічного впливу

**Джерело: створено автором згідно з даними [72; 96; 176]*

Додаток В

Ключові функції когнітивної безпеки в контексті легітимності влади

Назва функції	Основна мета	Методи та інструменти	Вплив на суспільство	Об'єкт протидії
Запобігання дезінформації	Виявлення, аналіз та нейтралізація дезінформаційних кампаній у реальному часі	Обробка природної мови, машинне навчання, аналіз великих даних, системи раннього попередження	Коригування спотворень у сприйнятті діяльності влади, автоматизоване спростування неправдивої інформації	Когнітивна війна, маніпулятивні наративи, поширення дезінформації як зброї
Зміцнення медіаграмотності	Розвиток критичного мислення та формування колективної когнітивної імунної системи	Інтерактивні платформи, освітні кампанії, адаптивний контент, децентралізовані мережі суб'єктів	Створення когнітивного щита, розвиток емоційного інтелекту, зміцнення суспільної єдності	Маніпулювання свідомістю, фейки, спроби впливу на вразливі соціальні групи
Забезпечення стратегічної комунікації	Побудова прозорих каналів взаємодії та формування довіри між державою і суспільством	Автоматизований моніторинг суспільної думки, генерація контенту, управління кризовими ситуаціями	Оперативне реагування на запити громадян, забезпечення цілісності інформаційного простору	Ерозія довіри до державних інституцій, штучний розкол суспільства
Захист інституційної легітимності	Виявлення спроб підриву довіри до національних установ через маніпулювання образами	Аналіз когнітивної емуляції, моніторинг когнітивних еталонів та схем, робота з наративами	Захист від штучних легітимаційних криз, розвиток критичного розуміння конструкту легітимності	Когнітивні атаки, механізми психологічного зараження, підрив довіри до інституцій-еталонів

**Джерело: створено автором згідно з даними [11; 215; 240]*

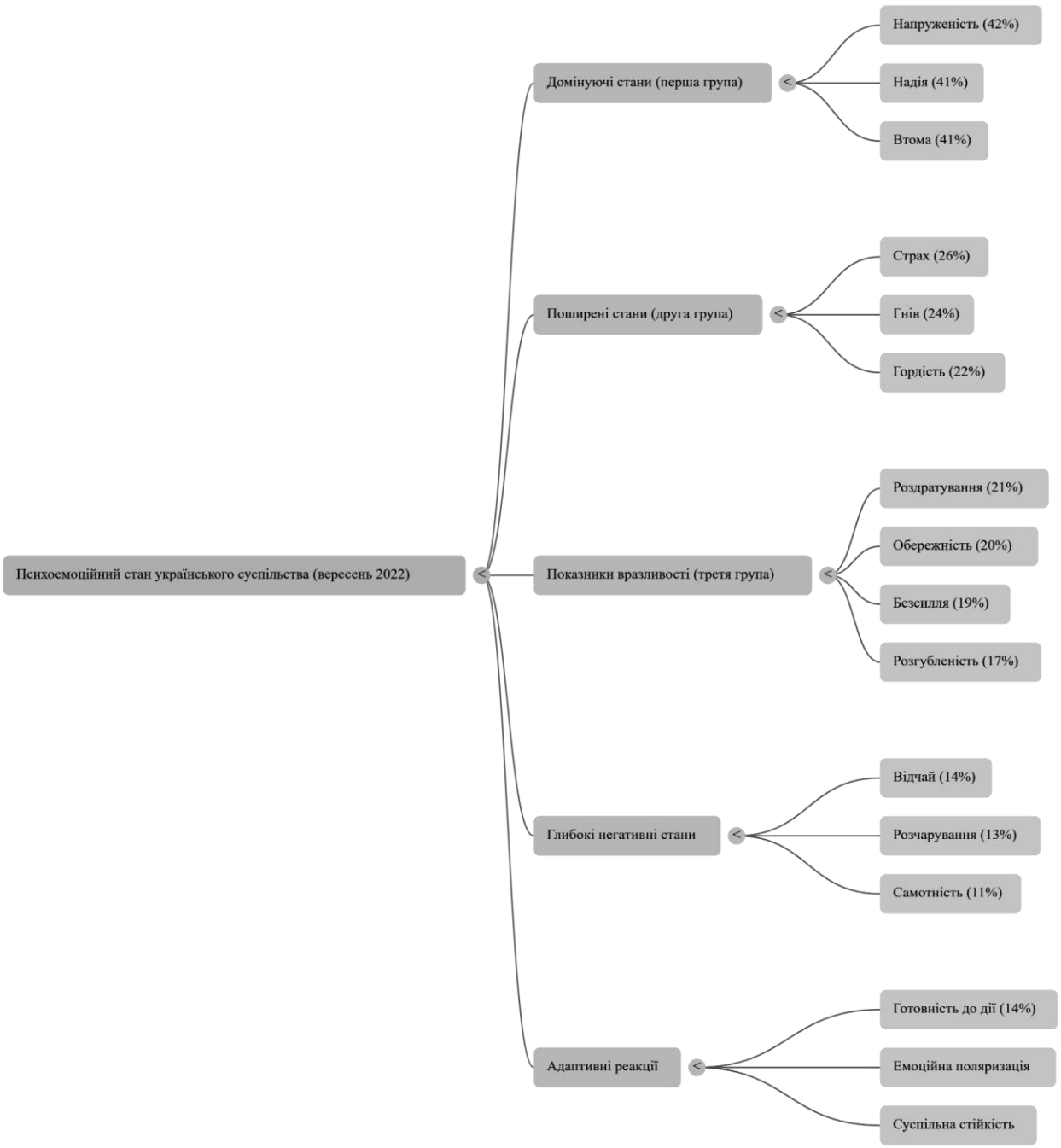
Додаток Г

Динаміка суспільної довіри в Україні

**Джерело: створено автором згідно з даними [131-132; 252].*

Додаток Ґ

Психоемоційний стан українського суспільства



**Джерело: створено автором згідно з даними [159].*

Додаток Д

Візуальне подання тексту

«Формування когнітивної стійкості (резильєнтності) в суспільстві як компоненту когнітивної безпеки в сучасній Україні»