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

Савлюк Михайло Іванович

УДК 004.77:681.3.06+354.42.44

ДИСЕРТАЦІЯ
ЗАГРОЗИ ІНФОРМАЦІЙНІЙ БЕЗПЕЦІ В СОЦІАЛЬНИХ МЕРЕЖАХ ПІД ЧАС ВІЙНИ ЗА НЕЗАЛЕЖНІСТЬ 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 _____ М.І.Савлюк

Науковий керівник: Кобець Юлія Василівна, кандидат політичних наук, доцент

Івано-Франківськ – 2026

АНОТАЦІЯ

Савлюк М. І. Загрози інформаційній безпеці в соціальних мережах під час Війни за Незалежність 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 здійснено комплексне політологічне дослідження сучасних загроз інформаційній безпеці України в середовищі соціальних мереж у контексті Війни за Незалежність України. Соціальні мережі розглядаються як середовище стратегічного впливу, у якому інформаційні потоки використовуються для формування громадської думки, мобілізації/демобілізації аудиторій, впливу на політичні процеси та підриву стійкості держави. Актуальність дослідження зумовлена експоненційним зростанням викликів інформаційній безпеці в умовах цифровізації суспільних комунікацій та трансформації інформаційного простору на один із ключових вимірів національної безпеки. У XXI столітті інформація виступає не лише ресурсом управління й розвитку, а й інструментом впливу, здатним визначати суспільні настрої, поведінкові моделі, легітимність політичних інститутів і стійкість держави до зовнішнього тиску. Відтак інформаційна безпека набуває характеру системоутворюючого чинника державності, оскільки безпосередньо пов'язана із захистом суверенітету, демократичних процедур, ціннісних орієнтирів і спроможності держави здійснювати ефективну політику в умовах кризових викликів.

Мета дослідження полягає у всебічному аналізі загроз інформаційній безпеці в соціальних мережах в умовах Війни за Незалежність України та обґрунтуванні механізмів захисту й підвищення стійкості інформаційного простору України на основі українського та міжнародного досвіду. Відповідно до мети визначено такі завдання: розкрити сутність поняття інформаційної

безпеки як політологічної категорії та визначити її структурні компоненти, функції й особливості; узагальнити теоретичні підходи та методи дослідження інформаційної безпеки й обґрунтувати методологічний інструментарій дисертації; проаналізувати нормативно-правову базу у сфері забезпечення інформаційної безпеки України; дослідити соціальні мережі як інструмент стратегічного впливу; охарактеризувати інформаційно-психологічні операції в соціальних мережах; проаналізувати кіберзагрози та технічні інструменти ведення гібридної війни; здійснити аналіз ключових кейсів інформаційного впливу на Україну у 2014–2025 рр.; узагальнити вітчизняний і світовий досвід протидії інформаційним загрозам; розробити практичні рекомендації щодо удосконалення механізмів захисту та підвищення стійкості інформаційного простору України.

Об'єктом дослідження є особливості формування та функціонування інформаційної безпеки України в умовах зовнішніх загроз і впливів. Предметом дослідження є загрози інформаційній безпеці України в соціальних мережах в умовах гібридної війни, механізми та закономірності їх виявлення й нейтралізації, з урахуванням вітчизняного та міжнародного досвіду.

Методологічну основу становить поєднання системного та компаративного аналізу, документального аналізу нормативно-правової бази, контент- та івент-аналізу, кейс-стаді, SWOT-аналізу й елементів прогнозування, що забезпечує комплексне вивчення загроз, інструментів впливу та практик протидії. Аналітичний метод застосовано під час опрацювання історіографії, концептуальних підходів і ключових категорій. Метод системного аналізу дав змогу розглядати інформаційну безпеку як складну систему взаємопов'язаних елементів – нормативно-правової бази, інституційної архітектури, механізмів координації, комунікаційних практик, технологічних чинників та зовнішніх впливів. Для оцінювання регуляторних засад і практик державного реагування застосовано метод документального аналізу; для зіставлення підходів України з практиками держав-партнерів – компаративний метод; для глибокого вивчення конкретних проявів інформаційного впливу – метод кейс-стаді; для виявлення

структури, змісту й динаміки інформаційних повідомлень – контент-аналіз; для оцінювання внутрішніх і зовнішніх чинників, що визначають спроможність держави забезпечувати інформаційну безпеку, – SWOT-аналіз. Метод моделювання використано для побудови узагальнених моделей інституційного механізму, а метод прогнозування – для визначення потенційних сценаріїв розвитку інформаційно-безпекової ситуації в Україні.

У першому розділі закладено теоретичний фундамент дослідження та сформовано категорійно-понятійний каркас аналізу. Розкрито сутність інформаційної безпеки, її структурні компоненти, функції та особливості як складника національної безпеки; показано, що інформаційна безпека у політологічному вимірі виходить за межі технічного захисту й включає політичні, соціальні та правові параметри управління інформаційними потоками. Встановлено, що поняття «інформаційна безпека» увійшло до наукового обігу наприкінці 1980-х років і з суто технічної категорії поступово трансформувалося в комплексний науковий конструкт, що охоплює проблеми захисту інформаційних ресурсів, стабільності інформаційного простору, протидії інформаційним загрозам і забезпечення національних інтересів держави. Обґрунтовано, що в сучасному розумінні інформаційна безпека – це стан захищеності основних інтересів особи, суспільства та держави в інформаційній сфері, що охоплює інформаційну та телекомунікаційну інфраструктуру, а також саму інформацію з її характеристиками: повнотою, об'єктивністю, доступністю та конфіденційністю. Проаналізовано багаторівневий характер сучасних загроз, які охоплюють: технологічний вимір (кібератаки, компрометація акаунтів, витоки даних); когнітивно-психологічний вимір (маніпуляції, дезінформація, нав'язування деструктивних наративів); інституційно-політичний вимір (підрив довіри до державних інституцій, вплив на електоральні процеси); соціальний вимір (поляризація, фрагментація суспільства); міжнародний вимір (вплив на міжнародну підтримку України). Здійснено аналіз нормативно-правової бази забезпечення інформаційної та кібербезпеки України, розглянуто її роль як інструменту державного управління

й політичного регулювання інформаційних процесів та окреслено значення законодавчих і стратегічних документів для превентивного виявлення загроз і координації дій суб'єктів безпеки.

Другий розділ присвячено розкриттю логіки гібридної війни в інформаційному вимірі та демонстрації того, як соціальні мережі стають платформним середовищем реалізації впливів. Соціальні мережі розглянуто як інструмент стратегічного впливу: обґрунтовано їхню роль у формуванні суспільної думки, політичних процесів і безпекових ризиків; показано, що мережна архітектура платформ, швидкість поширення контенту, алгоритмічна персоналізація та низький поріг входу для продукування інформаційних повідомлень створюють сприятливі умови для реалізації деструктивних впливів. Проаналізовано інформаційно-психологічні операції (ІПсО) в соціальних мережах як ключовий механізм інформаційної війни: окреслено їхні цілі – підрив легітимності влади, зниження суспільної згуртованості, деморалізація населення, формування вигідних агресору поведінкових моделей, – а також специфіку їхньої результативності завдяки швидкому доступу до великих аудиторій і механізмам мікротаргетингу. Виявлено, що ІПсО спрямовані одночасно на внутрішню аудиторію (деморалізація, поляризація, підрив довіри до влади) та зовнішню (дискредитація України в очах міжнародної спільноти). Розкрито кіберзагрози та технічні інструменти гібридної війни: від зламів акаунтів і фішингових атак до автоматизованих мереж (ботів, «сокпапетів») і технологій маніпуляції контентом (діпфейки, генеративний штучний інтелект). Встановлено, що кіберзагрози функціонують у взаємодоповнювальній єдності з ІПсО, формуючи синергетичний ефект.

У третьому розділі здійснено аналіз ключових кейсів інформаційного впливу на Україну у 2014–2025 рр., що дозволяє простежити еволюцію інструментів і наративів впливу та показати їхній зв'язок із політико-історичними передумовами й загальною ревізіоністською логікою російської політики. Виявлено, що впродовж зазначеного періоду відбулася системна трансформація методів і масштабів інформаційної агресії: від відносно

локалізованих операцій у 2014–2015 рр. до тотального інформаційного наступу в умовах повномасштабного вторгнення 2022–2025 рр. Встановлено стійкі наративні конструкти, що системно відтворюються у різних кейсах і є складниками єдиної стратегії підриву державності та легітимності України. Проаналізовано інституційні механізми протидії: діяльність Центру протидії дезінформації, Центру стратегічних комунікацій та інформаційної безпеки, Державної служби спеціального зв'язку та захисту інформації, Оперативного центру реагування на кіберінциденти та інших суб'єктів. Розглянуто досвід держав-партнерів (Естонія, Фінляндія, Латвія, Литва, Польща, Швеція, США, Великобританія та ін.) у побудові систем протидії дезінформації та кіберзагрозам. Обґрунтовано необхідність комплексного підходу, що включає нормативно-правові, інституційні, комунікаційні та освітні інструменти, а також підвищення стійкості суспільства до дезінформаційних кампаній, розширення міжнародної кооперації та розвиток спроможностей реагування.

Наукова новизна отриманих результатів зумовлена комплексним політологічним осмисленням сучасних загроз інформаційній безпеці в соціальних мережах в умовах гібридної війни та поглибленим аналізом інституційних механізмів протидії таким загрозам. У дисертації соціальні мережі концептуалізовано не лише як канал комунікації, а як середовище стратегічного впливу, де поєднуються ІПсО, маніпулятивні технології, алгоритмічне підсилення контенту, кібератаки та практики координованої неавтентичної поведінки. *Уперше*: комплексно досліджено сучасні загрози інформаційній безпеці України у соціальних мережах як складник гібридної війни; розроблено механізм інституційної взаємодії у сфері протидії загрозам, що враховує багаторівневість суб'єктів (державні органи, сектор безпеки й оборони, медіа, громадянське суспільство, міжнародні партнери, платформи); здійснено типологізацію загроз у соціальних мережах та визначено індикатори їх виявлення; проаналізовано ключові кейси інформаційного впливу (2014–2025 рр.); застосовано SWOT-аналіз і прогнозування до сфери інформаційної безпеки у соціальних мережах. *Удосконалено*: теоретико-методологічні засади

аналізу інформаційної безпеки в умовах диджиталізації; категорійно-понятійний апарат через уточнення співвідношення понять «інформаційна безпека» – «інформаційна агресія» – «ІПсО» – «дезінформація» – «стратегічні комунікації» – «стійкість інформаційного простору»; підхід до аналізу інституційних чинників шляхом виокремлення функційної параметризації завдань (моніторинг, превенція, реагування, кризові комунікації, міжвідомча координація). *Набули подальшого розвитку* положення про роль соціальних мереж у гібридній війні; про значення інституційної спроможності держави у протидії загрозам; про оптимальні моделі поєднання реактивних і проактивних підходів до політики інформаційної безпеки; про механізми міжнародної взаємодії у протидії дезінформації та ІПсО.

Теоретичне значення дослідження визначається тим, що його результати розширюють політологічне розуміння інформаційної безпеки як складника національної безпеки в умовах гібридної війни та цифровізації політичних комунікацій. Сформульовані положення, висновки й узагальнення можуть бути використані у подальших гуманітарних студіях – насамперед у межах політичної науки, а також соціології, культурології, прикладної лінгвістики та соціолінгвістики. Теоретичний внесок роботи полягає також у розкритті ролі інституційних чинників у формуванні стійкості інформаційного простору, виявленні закономірностей розгортання ІПсО та уточненні понятійно-категоріального апарату дослідження загроз інформаційній безпеці в соціальних мережах.

Практичне значення результатів полягає у можливості використання висновків і рекомендацій у діяльності органів публічної влади та сектору безпеки й оборони, у вдосконаленні державної інформаційно-безпекової політики щодо соціальних мереж, посиленні міжвідомчої координації та розвитку технологічних інструментів моніторингу й реагування. Матеріали дисертації можуть бути використані при формуванні й оновленні навчальних курсів за напрямами підготовки «Політологія», «Національна безпека», «Міжнародні відносини», «Інформаційна безпека» та спорідненими

спеціальностями. У ширшій перспективі результати роботи спрямовані на підтримку формування сприятливих умов для розвитку інформаційного суспільства в Україні та зміцнення національної безпеки в умовах тривалої агресії.

Ключові слова: інформаційна безпека, соціальні мережі, гібридна війна, інформаційна агресія, дезінформація, ІПсО, кіберзагрози, стратегічні комунікації, інституційні механізми, стійкість інформаційного простору, національна безпека.

SUMMARY

Savliuk M. I. Threats to Information Security in Social Media during Ukraine's War of Independence. – Qualification scientific work in the rights of a manuscript.

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

The dissertation presents a comprehensive political-science study of contemporary threats to Ukraine's information security in the social media environment in the context of the War of Independence of Ukraine. Social media are examined as a domain of strategic influence in which information flows are employed to shape public opinion, mobilise and demobilise audiences, affect political processes, and undermine state resilience. The relevance of the study is driven by the exponential growth of challenges to information security amid the digitalisation of public communications and the transformation of the information space into one of the key dimensions of national security. In the twenty-first century, information serves not merely as a resource for governance and development but as an instrument of influence capable of shaping public sentiment, behavioural patterns, the legitimacy of political institutions, and state resilience to external pressure. Accordingly, information security acquires the character of a system-forming factor of statehood, as it is directly linked to the protection of sovereignty, democratic procedures, value

orientations, and the capacity of the state to implement effective policy under conditions of crisis.

The purpose of the study is to provide an exhaustive analysis of information-security threats in social media under conditions of hybrid warfare and to substantiate protection mechanisms and approaches to enhancing the resilience of Ukraine's information space on the basis of domestic and international experience. In pursuance of this purpose, the following tasks were defined: to clarify the essence of information security as a political-science category and determine its structural components, functions, and specific features; to synthesise theoretical approaches and research methods in information-security studies and substantiate the methodological toolkit of the dissertation; to analyse Ukraine's regulatory and legal framework in the field of information security; to examine social media as an instrument of strategic influence; to characterise information and psychological operations in social media; to analyse cyber threats and the technical instruments of hybrid warfare; to conduct a case-study analysis of key instances of information influence on Ukraine in 2014–2025; to synthesise domestic and international experience in countering information threats; and to develop practical recommendations for improving protection mechanisms and strengthening the resilience of Ukraine's information space.

The object of the study is the specific features of the formation and functioning of Ukraine's information security under conditions of external threats and influences. The subject of the study is the threats to Ukraine's information security in social media under conditions of hybrid warfare, as well as the mechanisms and regularities underlying their identification and neutralisation, taking into account both domestic and international experience.

The methodological framework integrates systems and comparative analysis, documentary analysis of the regulatory and legal base, content analysis and event analysis, case-study methodology, SWOT analysis, and elements of forecasting, thereby enabling a comprehensive examination of threats, instruments of influence, and countermeasure practices. The analytical method was applied in processing the historiography, conceptual approaches, and key categories of the field. Systems

analysis enabled information security to be examined as a complex system of interrelated elements – the regulatory and legal base, institutional architecture, coordination mechanisms, communication practices, technological factors, and external influences. Documentary analysis was used to assess regulatory foundations and state response practices; comparative analysis to juxtapose Ukraine's approaches with those of partner states; case-study methodology for in-depth examination of specific manifestations of information influence; content analysis to identify the structure, content, and dynamics of information messages; and SWOT analysis to evaluate internal and external factors determining state capacity to ensure information security. Modelling was employed to construct generalised models of the institutional mechanism, while forecasting was used to identify potential scenarios for the development of the information-security situation in Ukraine.

Chapter 1 establishes the theoretical foundations of the study and develops the conceptual and categorical framework for analysis. It clarifies the essence of information security, its structural components, functions, and specific features as a component of national security, demonstrating that in political-science terms information security extends beyond technical protection and encompasses political, social, and legal parameters of governing information flows. It is established that the concept of "information security" entered scholarly discourse in the late 1980s and gradually evolved from a purely technical category into a complex scientific construct encompassing the protection of information resources, the stability of the information space, the countering of information threats, and the safeguarding of state interests. It is substantiated that in its contemporary understanding information security constitutes a state of protection of the fundamental interests of the individual, society, and the state in the information sphere, covering information and telecommunication infrastructure as well as information itself in terms of its completeness, objectivity, accessibility, and confidentiality. The chapter analyses the multi-level character of contemporary threats, spanning the technological dimension (cyberattacks, account compromise, data leaks); the cognitive-psychological dimension (manipulation, disinformation, the imposition of destructive narratives);

the institutional-political dimension (undermining trust in state institutions, influencing electoral processes); the social dimension (polarisation, fragmentation of society); and the international dimension (influencing international support for Ukraine). Ukraine's regulatory and legal framework for information and cyber security is analysed, its role as an instrument of public administration and political regulation of information processes is examined, and the significance of legislative and strategic documents for the preventive identification of threats and the coordination of security actors is outlined.

Chapter 2 elucidates the logic of hybrid warfare in the informational dimension and demonstrates how social media become platform-based environments for the operationalisation of influence. Social media are examined as instruments of strategic influence: their role in shaping public opinion, political processes, and security risks is substantiated, and it is shown that the network architecture of platforms, the speed of content dissemination, algorithmic personalisation, and the low entry threshold for producing information messages create favourable conditions for the realisation of destructive influences. Information and psychological operations (IPsO) in social media are analysed as a key mechanism of information warfare: their objectives are identified, undermining the legitimacy of public authority, weakening social cohesion, demoralising the population, and fostering behavioural patterns advantageous to the aggressor and their effectiveness is explained through rapid access to mass audiences and microtargeting mechanisms. It is found that IPsO are directed simultaneously at domestic audiences (demoralisation, polarisation, undermining trust in government) and external ones (discrediting Ukraine in the eyes of the international community). Cyber threats and the technical instruments of hybrid warfare are explicated, from account compromise and phishing attacks to automated networks (bots and sockpuppets) and content-manipulation technologies (deepfakes, generative artificial intelligence), and it is established that cyber threats operate in complementary unity with IPsO, producing a synergistic effect.

Chapter 3 analyses key cases of information influence on Ukraine in 2014–2025, tracing the evolution of instruments and narratives of influence and

demonstrating their linkage to political-historical preconditions and the broader revisionist logic of Russian policy. It is found that over the period under review a systemic transformation of the methods and scale of information aggression took place: from relatively localised operations in 2014–2015 to a total information offensive under conditions of full-scale invasion in 2022–2025. Persistent narrative constructs are identified that are systematically reproduced across different cases and constitute components of a unified strategy aimed at undermining Ukrainian statehood and legitimacy. The institutional mechanisms of counteraction are analysed, including the activities of the Centre for Countering Disinformation, the Centre for Strategic Communications and Information Security, the State Service of Special Communications and Information Protection, the Operational Centre for Responding to Cyber Incidents, and other actors. The experience of partner states (Estonia, Finland, Latvia, Lithuania, Poland, Sweden, the United States, the United Kingdom, and others) in building systems to counter disinformation and cyber threats is examined. The need for a comprehensive approach is substantiated, encompassing regulatory, institutional, communication, and educational instruments, as well as strengthening societal resilience to disinformation campaigns, expanding international cooperation, and developing response capacities.

The scholarly novelty of the study lies in the comprehensive political-science examination of contemporary information-security threats in social media under conditions of hybrid warfare and the in-depth analysis of institutional mechanisms for countering such threats. In the dissertation, social media are conceptualised not merely as a communication channel but as a domain of strategic influence in which IPsO, manipulative technologies, algorithmic content amplification, cyberattacks, and coordinated inauthentic behaviour converge. For the first time: the contemporary threats to Ukraine's information security on social media as a component of hybrid warfare have been comprehensively examined; a mechanism for institutional interaction in the field of threat countermeasures has been developed, incorporating the multi-level structure of actors (state bodies, the security and defence sector, media, civil society, international partners, and platforms); a typology of threats on

social media has been constructed and indicators for their identification have been defined; key cases of information influence operations (2014–2025) have been analysed; SWOT analysis and forecasting methods have been applied to the domain of information security on social media.

Further developed are: the theoretical and methodological foundations of information-security analysis under conditions of digitalisation; the conceptual and categorical apparatus through the clarification of the relationships among "information security", "information aggression", "IPsO", "disinformation", "strategic communications", and "information-space resilience"; and the approach to analysing the institutional factors of information-security policy through the identification of functional task parameters (monitoring, prevention, response, crisis communications, inter-agency coordination). The following propositions have been further developed: the role of social media in hybrid warfare as an instrument of strategic influence; the significance of state institutional capacity in countering threats in social media; optimal models for combining reactive and proactive approaches to information-security policy in wartime; and mechanisms of international cooperation in countering disinformation and IPsO.

The theoretical significance of the study lies in the fact that its results broaden the political-science understanding of information security as a component of national security under conditions of hybrid warfare and the digitalisation of political communications. The formulated propositions, conclusions, and generalisations may be employed in further humanities research – primarily within political science and also within sociology, cultural studies, applied linguistics, and sociolinguistics. The theoretical contribution of the work also consists in elucidating the role of institutional factors in building the resilience of the information space, identifying regularities in the deployment of IPsO, and refining the conceptual and categorical apparatus for studying information-security threats in social media.

The practical significance of the results consists in the possibility of employing the findings and recommendations in the activities of public authorities and the security and defence sector, in improving state information-security policy with

respect to social media, in strengthening inter-agency coordination, and in developing technological tools for monitoring and response. The materials of the dissertation may be used in developing and updating curricula in the fields of Political Science, National Security, International Relations, Information Security, and related specialisations. In a broader perspective, the results of the work are aimed at supporting the creation of favourable conditions for the development of the information society in Ukraine and the strengthening of national security under conditions of protracted aggression.

Keywords: information security; social media; hybrid warfare; information aggression; disinformation; information and psychological operations; cyber threats; strategic communications; institutional mechanisms; information-space resilience; national security.

СПИСОК ОПУБЛІКОВАНИХ ПРАЦЬ ЗА ТЕМОЮ ДИСЕРТАЦІЇ

Статті у фахових виданнях України категорії Б:

1. Савлюк М. Теоретико-методологічні засади дослідження інформаційної безпеки. *Вісник Прикарпатського університету. Серія: Політологія*. 2023. Випуск 15. 2023. С.60-68

DOI: https://doi.org/10.32782/2312-1815/2024-1-8

URL: https://journals.pnu.if.ua/index.php/politology/article/view/54

2. Савлюк М. Гібридна війна в Україні: сучасні підходи. *Вісник Прикарпатського університету. Серія: Політологія*. 2024. Випуск 17. С.187-197.

DOI: https://doi.org/10.32782/2312-1815/2024-17-23

URL: https://journals.pnu.if.ua/index.php/politology/article/view/130

3. Савлюк М. Важливість інформаційної безпеки в соціальних мережах для загальнонаціональної безпеки: безпековий вимір України. *Вісник Прикарпатського університету. Серія: Політологія.* 2024. Випуск 18. С.300-309.

DOI: https://doi.org/10.32782/2312-1815/2024-18-30

URL: https://journals.pnu.if.ua/index.php/politology/article/view/167

4. Пролорензо А. Савлюк М. Кіберзахист як складник інформаційної безпеки держави в умовах гібридної війни. *Національні інтереси України*. 2025. №6 (11). С.198-213

DOI: https://doi.org/10.52058/3041-1793-2025-6(11)-198-213

URL: https://perspectives.pp.ua/index.php/niu/article/view/25245/25222

Наукові праці, які засвідчують апробацію матеріалів дисертації:

5. Савлюк М. Інформаційна безпека в соціальних мережах: безпековий вимір для держави. *Публічне управління та адміністрування в Україні: Євроінтеграційний поступ:* збірник матеріалів ІІ Всеукраїнської науково-практичної конференції за міжнародної участі (м. Івано-Франківськ, 30 травня 2025 р.). Івано-Франківськ, 2025. С.101-104.

URL: https://nung.edu.ua/sites/default/files/2025-06/Збірник_тез_ІФНТУНГ_Т.2_2025_0.pdf

6. Савлюк М. Політика забезпечення інформаційної безпеки: міжнародний контекст. *Проблеми забезпечення інформаційної безпеки в міжнародному співробітництві*: матеріали міжнародної науково-практичної конференції, 5 вересня 2025 року. Ужгород, 2025. С.211-218.

7. Савлюк М. Теоретико-методологічні засади дослідження інформаційної безпеки як складник організаційно-правових засад функціонування системи безпеки критичної інфраструктури України. *Національна стійкість (резилієнтність) як ключовий елемент національної безпеки: архітектура, виклики та шляхи посилення*. Збірник матеріалів І Міжнародної науково-практичної конференції (м. Івано-Франківськ, 27 листопада 2025 р.). Івано-Франківськ, 2025. С.199-202.

URL: https://nung.edu.ua/sites/default/files/2025-12/Збірник_тез_ІФНТУНГ_2025.pdf

8. Савлюк М. Сучасна протидія інформаційним загрозам: вітчизняний та світовий досвід. *Всеукраїнська науково-практична конференція здобувачів вищої освіти та молодих учених: Національна безпека України в умовах воєнного стану: проблеми та шляхи їх вирішення*: зб. матеріалів всеукраїнської наук.-практ. конф. (м. Одеса, 20 березня 2026 р.). Одеса: Військова академія, 2026. С.359-360.

ЗМІСТ

ПЕРЕЛІК СКОРОЧЕНЬ І УМОВНИХ ПОЗНАЧЕНЬ

АРТ	Аргетовані атаки
ГУР МО	Головне управління розвідки Міністерства оборони України
ДССЗІ	Державна служба спеціального зв'язку та захисту інформації України
ЄС	Європейський Союз
ЗМІ	Засоби масової інформації
ЗСУ	Збройні сили України
ЗУ	Закон України
ІпСО	Інформаційно-психологічні спеціальні операції
НУО	Неурядова організація
ОЦРК	Оперативний центр реагування на кіберінциденти
ПЗ	Програмне забезпечення
РНБО	Рада безпеки і оборони України
рф	російська федерація
Ст	Стаття
ЦЕДЕМ	Центр демократії та верховенства права
ЦПД	Центр протидії дезінформації
ЦСКІБ	Центр соціальних комунікацій та інформаційної безпеки при Міністерстві культури та інформаційної політики
ШІ	Штучний інтелект
DDoS-атака	Denial of service attack
DSA	Digatal Services Act

ВСТУП

Актуальність теми дослідження зумовлена експоненційним зростанням викликів інформаційній безпеці в умовах цифровізації суспільних комунікацій та трансформації інформаційного простору на один із ключових вимірів національної безпеки. У XXI столітті інформація виступає не лише ресурсом управління й розвитку, а й інструментом впливу, здатним визначати суспільні настрої, поведінкові моделі, легітимність політичних інститутів і стійкість держави до зовнішнього тиску. Відтак інформаційна безпека набуває характеру системоутворюючого чинника державності, оскільки безпосередньо пов’язана із захистом суверенітету, демократичних процедур, ціннісних орієнтирів і спроможності держави здійснювати ефективну політику в умовах кризових викликів.

Особливої гостроти зазначена проблематика набула для України внаслідок російської агресії та тривалого гібридного протиборства, у межах якого інформаційний компонент функціонує як самостійний «театр» дій і водночас як інструмент забезпечення результативності військових, політичних, економічних і дипломатичних заходів агресора. Гібридний характер конфлікту передбачає поєднання класичних воєнних засобів із невоєнними технологіями тиску, серед яких інформаційно-психологічні операції, масовані кампанії дезінформації, маніпуляції порядком денним, використання бот-мереж, інструментів мікротаргетингу, а також кібератаки на об’єкти державної влади й критичної інфраструктури. У таких умовах інформаційна безпека перестає бути вузькоспеціалізованою технічною категорією та постає як комплексне політико-соціальне явище, що потребує цілісного наукового осмислення й прикладних рішень.

Соціальні мережі у цьому контексті відіграють особливу роль, оскільки є одночасно головним каналом масової комунікації й простором підвищеної вразливості. Їхня мережна архітектура, швидкість поширення контенту, алгоритмічна персоналізація та низький поріг входу для продукування

інформаційних повідомлень створюють сприятливі умови для реалізації деструктивних впливів. Унаслідок цього соціальні платформи перетворюються на середовище конкуренції наративів, де зовнішній актор може оперативно масштабувати маніпулятивні повідомлення, конструювати фрагментовані картини реальності та ініціювати інформаційні кризи, спрямовані на підрив довіри до інститутів влади, деморалізацію населення, поляризацію суспільства й делегітимацію державної політики. Водночас у воєнний період соціальні мережі залишаються критично важливим ресурсом комунікації держави з громадянами, інструментом мобілізації й самоорганізації, що загострює потребу у виробленні збалансованих механізмів захисту, які не руйнують демократичні свободи, але мінімізують ризики ворожого впливу.

Зазначені обставини спродукували потребу в оперативному та стратегічному реагуванні держави на поточні загрози із формуванням відповідних політичних концепцій, інституційних механізмів, стратегій та практик забезпечення інформаційної безпеки. Пріоритетність такого реагування визначається необхідністю підвищення стійкості інформаційного простору до наявних і потенційних вразливостей, а також побудови сценаріїв протидії загрозам з урахуванням динамічного характеру інформаційного середовища. У цьому сенсі наукове дослідження загроз інформаційній безпеці в соціальних мережах має не лише теоретичне, а й прикладне значення: воно сприяє конкретизації вразливих сегментів інформаційного простору, окресленню ефективних моделей реагування та пошуку оптимального балансу між безпекою, свободою слова й правами людини.

Актуальність теми посилюється й тим, що сучасні загрози інформаційній безпеці мають багаторівневий характер. Вони охоплюють: *технологічний вимір* (кібератаки, компрометація акаунтів, витоки даних, уразливості платформ); *когнітивно-психологічний вимір* (маніпуляції, дезінформація, конструювання фейкових подій, нав’язування деструктивних наративів); *інституційно-політичний вимір* (підрив довіри до державних інституцій, дискредитація управлінських рішень, вплив на електоральні процеси, формування протестних

або капітуляційних настроїв); *соціальний вимір* (поляризація, фрагментація суспільства, радикалізація, руйнування горизонтальної довіри); *міжнародний вимір* (перенесення протистояння на зовнішні аудиторії, вплив на міжнародну підтримку України). Така комплексність визначає потребу у міждисциплінарному та водночас політологічному аналізі, який дозволяє пояснити не лише «як» реалізуються загрози, а й «чому» вони набувають ефективності в конкретному політичному й соціальному контексті.

Показово, що теоретико-методологічне осмислення категорії національної безпеки в діджиталізаційному вимірі відкриває можливість глибшого аналізу інформаційної безпеки як геополітичної детермінанти державності та чинника збереження суверенного політичного порядку. У свою чергу, аналіз безпеки інформаційного простору України з екстраполяцією сучасних викликів і залученням міжнародного досвіду дає змогу виокремити специфіку українського контексту: поєднання умов повномасштабної війни, високої цифрової мобільності населення, активної ролі соціальних мереж у повсякденній комунікації, а також одночасної необхідності модернізації нормативно-інституційної архітектури відповідно до європейських стандартів і практик. У цьому вимірі актуальність дослідження пов’язана і з потребою систематизації концептуальних підходів до визначення інформаційної безпеки, уточнення її змістових параметрів у політичній науці та вироблення дієвих стратегій функціонування інформаційно-безпекової політики в умовах сучасних цифровізаційних і геополітичних загроз.

Отже, вибір теми дослідження детермінований не лише високою суспільно-політичною значущістю аналізованої проблематики, а й потребою у виробленні ґрунтовного, комплексного та вичерпного підходу до розуміння й захисту інформаційного простору України. У межах дисертації інформаційний простір розглядається як середовище, в якому перетинаються комунікативні процеси, інституційні практики, технологічні інструменти та політичні інтереси; його безпека є передумовою сталого розвитку, стабільності й здатності держави до генези та адаптації в умовах війни. Це зумовлює потребу

в поглибленому аналізі інституційних чинників і виробленні ефективних стратегій протидії наявним та потенційним загрозам, насамперед у сегменті соціальних мереж як ключового каналу сучасного інформаційного протиборства.

Зв'язок роботи з науковими програмами, планами, темами. Тема дисертаційного дослідження затверджена Вченою радою Карпатського національного університету імені Василя Стефаника (протокол № 10 від 06 грудня 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 механізмів протидії загрозам інформаційній безпеці в соціальних мережах в умовах гібридної війни, типологізації інструментів інформаційно-психологічного впливу та формуванні практичних рекомендацій щодо підвищення стійкості інформаційного простору України.

Мета і завдання дослідження. Метою дисертаційної роботи є комплексне та всебічне дослідження сучасних загроз інформаційній безпеці України в соціальних мережах в умовах Війни за Незалежність України, з'ясування їхньої природи, механізмів продукування та поширення, а також обґрунтування ефективних інституційно-правових, організаційних і технологічних механізмів захисту та підвищення стійкості інформаційного простору України з урахуванням українського і світового досвіду протидії інформаційним впливам.

Відповідно до мети, змісту та структури дисертації визначено такі завдання дослідження:

– розкрити сутність поняття інформаційної безпеки як політологічної категорії, визначити її структурні компоненти, функції та особливості у сучасному інформаційному середовищі;

– узагальнити теоретичні підходи та методи дослідження інформаційної безпеки, обґрунтувати методологічний інструментарій дисертації та визначити його евристичні можливості для аналізу загроз у соціальних мережах, а також

проаналізувати нормативно-правову базу у сфері забезпечення інформаційної безпеки України, встановити її спроможність реагувати на виклики гібридної війни та окреслити проблемні зони правового регулювання;

– дослідити соціальні мережі як інструмент стратегічного впливу, визначити їхні функціональні характеристики, уразливості та роль у формуванні інформаційного порядку денного в умовах конфлікту;

– охарактеризувати інформаційно-психологічні операції в соціальних мережах, визначити їхні цілі, технології, механізми маніпулятивного впливу та безпекові наслідки для держави і суспільства;

– проаналізувати кіберзагрози та технічні інструменти ведення гібридної війни, релевантні для функціонування соціальних платформ та цифрових комунікацій, а також їхній вплив на стійкість інформаційного простору;

– здійснити аналіз ключових кейсів інформаційного впливу на Україну у 2014–2025 рр., визначити типологію та логіку реалізації загроз у соціальних мережах, виявити характерні наративи, механізми масштабування й цільові аудиторії;

– узагальнити український і світовий досвід протидії інформаційним загрозам, визначити ефективні практики, інституційні моделі та інструменти підвищення стійкості інформаційного простору;

– розробити практичні рекомендації щодо удосконалення механізмів захисту та підвищення стійкості інформаційного простору України в умовах Війни на Незалежність України, зокрема у частині нормативно-правового, інституційного, комунікаційного та технологічного забезпечення.

Об’єктом дослідження є особливості формування та функціонування інформаційної безпеки України в умовах зовнішніх загроз і впливів.

Предметом дослідження є загрози інформаційній безпеці України в соціальних мережах в умовах гібридної війни, механізми та закономірності їх виявлення й нейтралізації, з урахуванням вітчизняного та міжнародного досвіду.

Методи дослідження. Специфіка мети, об’єкта та предмета дисертаційного дослідження зумовила застосування комплексу наукових методів, що забезпечують цілісне опрацювання проблематики інформаційної безпеки України в умовах зовнішніх загроз, зокрема в сегменті соціальних мереж. Методологічну основу роботи становить поєднання загальнонаукових, спеціально-наукових і філософсько-світоглядних підходів як системно організованих способів аналізу, що уможливлюють виявлення закономірностей формування та реалізації інформаційно-безпекової політики, її інституційних параметрів і практик протидії інформаційним впливам.

Для осмислення теоретико-методологічних засад проблеми використано аналітичний метод, який застосовано під час опрацювання історіографії, концептуальних підходів і ключових категорій (інформаційна безпека, національна безпека, інформаційна агресія, гібридна війна тощо) з метою локалізації провідних принципів, підходів і викликів у досліджуваній сфері. Метод системного аналізу дав змогу розглядати інформаційну безпеку як складну систему взаємопов’язаних елементів (нормативно-правова база, інституційна архітектура, механізми координації, комунікаційні практики, технологічні чинники та зовнішні впливи), а також простежити характер їхньої взаємодії в умовах гібридної війни.

З метою оцінювання регуляторних засад і практик державного реагування застосовано метод документального аналізу, який використано під час роботи з нормативно-правовими актами, стратегічними документами, офіційними повідомленнями органів державної влади, матеріалами інституцій та іншими релевантними джерелами. Для зіставлення підходів України з практиками держав-партнерів залучено компаративний (порівняльний) метод, що забезпечив можливість виокремлення ефективних моделей протидії інформаційним впливам і визначення перспектив їх адаптації та імплементації у національний контекст.

Для глибокого вивчення конкретних проявів інформаційного впливу використано метод кейс-стаді, який дозволив детально проаналізувати вибрані

кейси інформаційних атак, інформаційно-психологічних операцій, кіберінцидентів і практик протидії у 2014–2025 рр., визначаючи їхню логіку, інструменти, цільові аудиторії та наслідки.

Для виявлення структури, змісту й динаміки інформаційних повідомлень у масмедіа та соціальних мережах застосовано контент-аналіз, що уможливив ідентифікацію дезінформаційних осередків, наративів, маніпулятивних технологій, а також типових механізмів поширення неправдивих даних. Івент-аналіз (аналіз подій) використано для систематизації релевантних подій, які впливають на інформаційно-безпекову ситуацію (інформаційні кампанії, кібератаки, політичні заяви, регуляторні рішення тощо), та встановлення причинно-наслідкових зв'язків між ними, динамікою інформаційних потоків і реакціями державних та недержавних інституцій.

Для оцінювання внутрішніх і зовнішніх чинників, що визначають спроможність держави забезпечувати інформаційну безпеку, застосовано SWOT-аналіз, який дозволив унаочнити сильні й слабкі сторони національної інформаційно-безпекової політики, можливості та загрози її розвитку, а також обґрунтувати напрями вдосконалення. З метою формування практико-орієнтованих висновків використано метод моделювання, що став інструментом побудови узагальнених моделей інституційного механізму забезпечення інформаційної безпеки та можливих сценаріїв реагування на загрози у соціальних мережах. Метод прогнозування застосовано для визначення потенційних сценаріїв розвитку інформаційно-безпекової ситуації в Україні з урахуванням впливу російської агресії, технологічних трансформацій та внутрішніх викликів.

Теоретико-методологічне підґрунтя дослідження когнітивної безпеки України в умовах гібридної війни формують міждисциплінарні праці та джерела, у яких розглядаються інформаційні впливи, механізми маніпулювання свідомістю, інформаційно-психологічні операції, цифрові загрози й питання захисту інформаційного простору. У вітчизняному науковому дискурсі ці проблеми осмислюються через безпековий, управлінський і комунікаційний

виміри, що представлено у працях Алещенко В., Андрущенко Д., Аніщенко О. Б., Богуш В., Боднар І. Р., Горбулін В., Дерев'янко С. М., Магда Є. В., Матвієнків С. М., Петрик В., Курбан О. В., Ліпкан В.А., Шеломенцев В. П. Важливим є також масив матеріалів, що відображають актуальні прояви інформаційних впливів і маніпулятивних практик у цифровому середовищі та в соціальних мережах, зокрема публікації й аналітика Адамович Н. та інші тематично близькі джерела зі списку.

У міжнародному та порівняльному вимірі теоретичні рамки аналізу інформаційного протиборства й цифрових ризиків доповнюються роботами авторів, представлених у бібліографії, зокрема Аро Ж., Хоффман Ф. Г., Пол С., фон Солмс R., Шакаріан Р., Ларасі Ж. Р., Марлоу Т., Максвіні С., Оремус В., Крейг А., Клаузіус М. та інших. У сукупності ці праці й джерела репрезентують сучасний стан наукових і прикладних підходів до дослідження когнітивних загроз, а їх узагальнення забезпечує підстави для формування авторської позиції щодо чинників когнітивної стійкості та механізмів протидії інформаційним впливам в умовах гібридної війни.

До напряму кібербезпеки (кіберпростір, кібератаки, хактивізм, кіберзагрози, кіберзахист тощо) належать праці, представлені авторами: Базиляк І.О., Бразалук М.Ю., Варналій Є.О., Голуб А., Гончаренко Г.А., Гриник Р.О., Гук О.М., Діордіца І. В., Жарикова А., Єрема М., Єсіна О.Г., Коваленко Є., Кравченко О., Крижний А., Крихівський М., Лоза В.В., Мадрига Т., Машталір В.В., Михайлов Д., Мурасов Р.К., Некрасов В., Омельченко А. В., Панченко В. М., Пилипенко В.М., Пфо О. М., Рібейро А., Савчук С.О., Тарасюк А. В., Цимбалюк В.С., Шакаріан Р., Шевченко Л., Шеломенцев В. П., Веклич В., Аро Ж.

Інформаційна безпека. До напряму інформаційної безпеки (інформаційна війна, пропаганда, дезінформація, ІПсО, маніпуляції, стратегічні комунікації, загрози в соцмережах, захист інформаційного простору тощо) належать джерела, представлені авторами: Адамович Н., Алещенко В., Андрущенко Д., Аніщенко О. Б., Арабаджиєв Д. Ю., Сергієнко Т. І., Архипов О, Архипова Є.,

Баран М. В., Биков О. М., Білодід К.С., Благодарний А. М., Штельмах О. В., Богданович В., Богуш В., Боднар І. Р., Горбулін В., Даниленко С., Данільян О., Дерев'янко С. М., Дзьобан О., Дуцик Д., Єрмак О., Єсімов С., Захаренко К., Зіма І., Зозуля О., Калюжний Р., Кобець Т., Козьміних А., Конах В., Кондратьєв Я., Копійка М., Кормич Б., Корнієнко С., Косогоров О., Кочубей Л., Кравець Є., Кравченко Ю., Крилова Н., Кузьмінська Р., Левченко О., Литвин М., Литвиненко О., Ліпкан В.А., Лісовський О., Логінов О., Логовський І., Магда Є. В., Макаренко Є., Максименко Ю., Манжай О., Марков В., Марутян Р., Марчук В., Матвієнків С. М., Махній М., Мороз О., Нижник Н., Ніколаєв І., Ніщименко О., Новицька Н., Носов В., Олійник О., Олуйко В., Отрешко В., Павловський В., Панов М., Панченко О., Петрик В., Пилипчук В., Поліщук І., Почепцов Г., Присяжнюк М., Приходько Д., Проноза І., Радковець Ю., Рачковська Л., Романчук Ю., Рудь І., Рущенко І., Ситник Г., Сірик А., Сливка В., Сопілко І., Соснін О., Степаненко В., Суббот А., Ткачук Т., Турчак А., Харченко Л., Холод О., Хоружий Г., Чмельов В., Шадур А., Шамрай В., Шаповалов О., Шевченко С., Шевчук П., Шульга В., Юдін О., Яремчук М., Ященко В.

Наукова гіпотеза дослідження полягає в припущенні, що інституційні чинники інформаційно-безпекової політики України в умовах гібридної війни мають самобутню модель функціонування, зумовлену специфікою українського політичного контексту, характером російської інформаційної агресії та особливостями національного інформаційного простору, зокрема середовища соціальних мереж. Відповідно, результативність українських політичних стратегій, кампаній і практик у сфері інформаційної безпеки визначається не лише реактивним стримуванням загроз, а насамперед спроможністю інституційної системи діяти проактивно: формувати стійкість суспільства, підтримувати позитивний і правдивий інформаційний порядок денний, мінімізувати ефекти дезінформації та маніпуляцій.

Виходячи з цього, обґрунтовується, що підвищення ефективності інформаційно-безпекової політики України потребує цілеспрямованої імплементації та адаптації міжнародного досвіду (стратегій, практик,

стандартів, протоколів реагування) із паралельною динамізацією співпраці з іноземними партнерами як необхідної передумови зміцнення державної стійкості. Водночас така імплементація не може бути механічним запозиченням: її результативність залежить від здатності українських інституцій узгодити зовнішні практики з національними умовами війни, ресурсними можливостями, правовими рамками та суспільними запитами.

Гіпотеза також передбачає, що ефективна інформаційно-безпекова політика має розглядатися як комплексний інструмент довгострокового впливу, який охоплює: розвиток медіаграмотності та критичного мислення населення; підтримку незалежних медіа та відповідальних комунікацій; удосконалення стратегічних державних комунікацій; протидію інформаційно-психологічним операціям у соціальних мережах; а також посилення кіберстійкості цифрової інфраструктури. Відтак, нарощування інституційного потенціалу у сфері інформаційної безпеки (через удосконалення законодавства, професіоналізацію кадрів, розвиток міжвідомчої координації та впровадження передових технологій моніторингу й реагування) здатне суттєво підвищити стійкість України до інформаційного впливу держави-агресора.

Джерельну базу дисертаційної роботи становить комплекс офіційних документів і матеріалів, що відображають нормативно-правові, інституційні та практичні засади формування і реалізації інформаційно-безпекової політики України в умовах зовнішніх загроз та гібридної війни. Питомими джерелами дослідження є нормативно-правові акти України, зокрема закони України, укази та розпорядження Президента України, постанови Верховної Ради України, постанови й розпорядження Кабінету Міністрів України, а також нормативно-правові документи центральних органів виконавчої влади (міністерств, служб, агентств), що регламентують питання інформаційної політики, кібербезпеки, стратегічних комунікацій, протидії дезінформації та захисту національного інформаційного простору. Важливу частину джерельної бази складають рішення органів державного управління та місцевого самоврядування, які фіксують практику впровадження державних рішень у сфері інформаційної

безпеки на різних рівнях публічної влади, а також дають змогу простежити інституційну взаємодію та механізми реагування на інформаційні інциденти й загрози. Сукупність зазначених джерел забезпечує можливість об’єктивного аналізу еволюції нормативного регулювання, оцінювання спроможності інституційного механізму забезпечення інформаційної безпеки та визначення напрямів його удосконалення з урахуванням викликів, актуалізованих російською інформаційною агресією, зокрема у середовищі соціальних мереж.

Наукова новизна отриманих результатів зумовлена комплексним політологічним осмисленням сучасних загроз інформаційній безпеці в соціальних мережах в умовах гібридної війни в Україні та поглибленим аналізом інституційних механізмів протидії таким загрозам. У дисертації соціальні мережі концептуалізовано не лише як канал комунікації, а як середовище стратегічного впливу, де поєднуються інформаційно-психологічні операції, маніпулятивні технології, алгоритмічне підсилення контенту, кібератаки та мережеві практики координованої неавтентичної поведінки. Це дозволило заповнити низку лакун у вітчизняній політичній науці щодо визначення загроз, логіки їхнього розгортання та інституційної спроможності держави реагувати на них у воєнний період.

уперше:

– комплексно досліджено сучасні загрози інформаційній безпеці України у соціальних мережах як складник гібридної війни, визначено їхню політичну природу, механізми продукування та поширення, а також безпекові наслідки для держави й суспільства;

– розроблено та обґрунтовано механізм інституційної взаємодії у сфері протидії загрозам у соціальних мережах, що враховує багаторівневість суб’єктів (державні органи, сектор безпеки й оборони, медіа, громадянське суспільство, міжнародні партнери, платформи) та потребу гнучкої координації в умовах швидкозмінних інформаційних кампаній;

– здійснено типологізацію наявних і потенційних загроз у соціальних мережах (дезінформаційні кампанії, маніпулятивні наративи, ІПсО, бот-мережі

та мережі координованої поведінки, мікротаргетинг, дискредитаційні кампанії, інформаційне “засмічення”, кібератаки на акаунти/канали комунікації) та визначено індикатори їх виявлення в рамках інституційного реагування;

– проаналізовано ключові кейси інформаційного впливу на Україну (2014–2025 рр.) у соціальних мережах як емпіричну основу для виявлення закономірностей еволюції інструментів агресора, змін у наративній структурі та ефективності протидії;

– застосовано SWOT-аналіз і прогнозування саме до сфери інформаційної безпеки у соціальних мережах, що дало змогу визначити пріоритети зміцнення стійкості (resilience) та сформувати практико-орієнтовані рекомендації щодо оптимізації державної політики.

удосконалено:

– теоретико-методологічні засади аналізу інформаційної безпеки в умовах диджиталізації та платформізації політичних комунікацій, що дозволило точніше розкрити специфіку загроз у соціальних мережах як окремого сегмента інформаційного простору;

– категорійно-понятійний апарат дослідження інформаційної безпеки через уточнення змісту й співвідношення понять «інформаційна безпека» – «інформаційна агресія» – «ІПсО» – «дезінформація» – «стратегічні комунікації» – «стійкість інформаційного простору» у контексті гібридної війни;

– підхід до аналізу інституційних чинників інформаційно-безпекової політики України шляхом виокремлення функційної параметризації завдань у сфері соціальних мереж (моніторинг, превенція, реагування, кризові комунікації, міжвідомча координація, взаємодія з платформами та громадянським суспільством).

набули подальшого розвитку положення про:

– роль соціальних мереж у гібридній війні як інструменту стратегічного впливу, що здатний одночасно формувати політичний порядок денний, підривати довіру до інститутів, поляризувати суспільство й впливати на міжнародне сприйняття України;

– значення інституційної спроможності держави у протидії загрозам у соціальних мережах – через професіоналізацію кадрів, удосконалення нормативно-правової бази, розвиток міжвідомчої координації та технологічних інструментів моніторингу/реагування;

– оптимальні моделі поєднання реактивних (виявлення, нейтралізація, блокування, спростування) та проактивних (побудова стійкості, медіаграмотність, стратегічні комунікації, підтримка незалежних медіа) підходів до політики інформаційної безпеки у воєнний період;

– механізми міжнародної взаємодії у протидії дезінформації та ІПсО в соціальних мережах як чинник посилення стійкості України й гармонізації практик із партнерами (обмін даними, спільні стандарти, координація реагування, підтримка спроможностей).

Теоретичне значення дослідження визначається тим, що його результати розширюють політологічне розуміння інформаційної безпеки як складника національної безпеки в умовах гібридної війни та цифровізації політичних комунікацій. Сформульовані положення, висновки й узагальнення можуть бути використані у подальших гуманітарних студіях, насамперед у межах політичної науки, а також соціології, культурології, історії культури, культурної антропології, прикладної лінгвістики та соціолінгвістики, оскільки дослідження фіксує й інтерпретує трансформації сучасного політичного дискурсу в соціальних мережах як середовищі стратегічного впливу. Теоретичний внесок роботи полягає також у можливості використання її результатів для аналізу політичних практик і стратегій у межах інформаційно-безпекової політики, зокрема через розкриття ролі інституційних чинників у формуванні стійкості інформаційного простору, виявлення закономірностей розгортання інформаційно-психологічних операцій та уточнення понятійно-категоріального апарату дослідження загроз інформаційній безпеці в соціальних мережах. Окремо слід наголосити, що представлені у дисертації підходи унаочнюють актуальну тенденцію до міждисциплінарної інтеграції гуманітарних наук у дослідженні модерного державотворення, належного врядування та

національної стійкості, у межах якої інформаційна безпека осмислюється також у соціокультурному вимірі як чинник стабільності держави.

Практичне значення роботи полягає у можливості застосування її результатів у навчальному процесі закладів вищої освіти під час підготовки та проведення лекційних і семінарських занять, розроблення контрольних заходів, навчально-методичного забезпечення, а також у процесі написання кваліфікаційних наукових праць. Матеріали дисертації можуть бути використані при формуванні й оновленні навчальних курсів і освітніх компонентів за напрямами підготовки «Політологія», «Національна безпека», «Міжнародні відносини», «Європейські студії», «Інформаційна безпека» та спорідненими спеціальностями, зокрема в тематиці гібридних конфліктів, стратегічних комунікацій, протидії дезінформації та кіберзагрозам. Практико-орієнтована цінність результатів дослідження також полягає в тому, що сформульовані висновки й рекомендації можуть бути враховані під час удосконалення державної інформаційно-безпекової політики, розроблення інституційних механізмів реагування на загрози у соціальних мережах, посилення міжвідомчої координації та підвищення стійкості інформаційного простору до зовнішніх і внутрішніх викликів. У ширшій перспективі результати роботи спрямовані на підтримку формування сприятливих умов для розвитку інформаційного суспільства в Україні та зміцнення національної безпеки в умовах тривалої агресії.

Особистий внесок здобувача полягає в самостійному виконанні всіх етапів роботи – від постановки проблеми та формування дослідницького дизайну до отримання, узагальнення й інтерпретації результатів, що виносяться на захист. Здобувачем опрацьовано та систематизовано широкий масив наукової літератури й джерельної бази (зокрема нормативно-правові та стратегічні документи у сфері національної, інформаційної та кібербезпеки), що стало підґрунтям для концептуалізації соціальних мереж як середовища стратегічного впливу в гібридній війні та для уточнення ролі інформаційної безпеки у структурі національної безпеки України. На цій основі здобувач уточнив

понятійно-категоріальний апарат дослідження, виокремив ключові ознаки та параметри загроз у соціальних мережах, а також визначив їхній безпековий потенціал у контексті російської інформаційної агресії. Важливим складником особистого внеску є самостійне здійснення аналітичної частини: проведено системний аналіз механізмів і технологій інформаційного впливу в соціальних мережах (зокрема інформаційно-психологічних операцій, маніпулятивних кампаній, дезінформаційних практик, координованої неавтентичної поведінки та кіберзагроз), а також проаналізовано ключові кейси впливу на Україну у 2014–2025 рр. із визначенням їхніх інструментів, наративів, цільових аудиторій та наслідків для інформаційної стійкості держави й суспільства. Здобувачем також узагальнено вітчизняний і міжнародний досвід протидії загрозам у соціальних мережах та виокремлено практики, релевантні для українського контексту.

Крім того, здобувачем застосовано комбінований методологічний інструментарій (системний і компаративний аналіз, контент-аналіз, івент-аналіз, кейс-стаді, елементи моделювання та прогнозування), що забезпечило комплексний характер дослідження та дозволило сформувати практико-орієнтовані рекомендації щодо удосконалення механізмів захисту й підвищення стійкості інформаційного простору України в умовах гібридної війни, з акцентом на середовище соціальних мереж. Усі теоретичні положення, висновки та рекомендації, що виносяться на захист, отримані здобувачем самостійно, є обґрунтованими, логічно узгодженими з метою і завданнями дисертації та можуть бути відтворені за умови використання аналогічної джерельної бази й методів дослідження.

Апробація результатів дослідження. Основні положення, висновки та результати дисертаційної роботи пройшли апробацію в процесі їх обговорення на засіданнях кафедри політичних наук Карпатського національного університету імені Василя Стефаника, що забезпечило наукову верифікацію теоретичних узагальнень, методологічних підходів і практичних рекомендацій. Результати дослідження також оприлюднено та представлено у вигляді

доповідей на науково-практичних конференціях, зокрема: Всеукраїнській науково-практичній конференції «Публічне управління та адміністрування в Україні: Євроінтеграційний поступ» (м. Івано-Франківськ, 30 травня 2025 р.); Міжнародній науково-практичній конференції «Проблеми забезпечення інформаційної безпеки в міжнародному співробітництві» (м. Ужгород, 5 вересня 2025 р.); І Міжнародній науково-практичній конференції «Національна стійкість (резилієнтність) як ключовий елемент національної безпеки: архітектура, виклики та шляхи посилення» (м. Івано-Франківськ, 27 листопада 2025 р.); Всеукраїнській науково-практичній конференції здобувачів вищої освіти та молодих учених: Національна безпека України в умовах воєнного стану: проблеми та шляхи їх вирішення: (м. Одеса, 20 березня 2026 р.).

Публікації. Основні наукові результати дисертаційного дослідження відображено у 8 наукових працях здобувача, з яких: 4 статті опубліковано у наукових фахових виданнях України; 4 публікації (статей/тез), що додатково висвітлюють результати дисертації та відображають окремі аспекти проведеного дослідження.

Структура та обсяг дисертації. Дисертація складається зі вступу, трьох розділів, що поділяються на вісім підрозділів, висновків, списку використаних джерел та літератури, який налічує 386 позиції, а також 13 додатків. Загальний обсяг дисертації становить 282 сторінки, з них основний текст – 202 сторінки.

РОЗДІЛ 1. ТЕОРЕТИКО-МЕТОДОЛОГІЧНІ ЗАСАДИ ДОСЛІДЖЕННЯ ІНФОРМАЦІЙНОЇ БЕЗПЕКИ

1.1. Інформаційна безпека: сутність поняття, структурні компоненти, функції та особливості

Інформаційна безпека виступає ключовим компонентом сучасної системи національної безпеки, оскільки вона забезпечує захист державних, суспільних та індивідуальних інтересів у інформаційному просторі. У політологічному вимірі інформаційна безпека розглядається як комплексна категорія, що охоплює не лише технічний захист даних, але й політичні, соціальні та правові аспекти управління інформаційними потоками. Вивчення її сутності дозволяє визначити базові принципи організації інформаційного простору, встановити функціональні зв’язки між різними складовими системи та розкрити роль інформаційних ресурсів як елементу державної влади та стратегічного управління.

Аналіз поняття інформаційної безпеки передбачає системне вивчення його змістовного наповнення, структурних елементів і функціонального призначення в сучасному політичному процесі. У цьому контексті особливо важливо простежити еволюцію трактувань інформаційної безпеки - від техніко-інструментального розуміння до комплексного політико-соціального феномена, що безпосередньо пов’язаний із забезпеченням національних інтересів, стабільності політичної системи та захисту інформаційного суверенітету держави.

Наукове осмислення інформаційної безпеки неможливе без аналізу базового поняття «інформація». Ця дефініція має латинське походження й походить від слова «informatio», яке в класичному значенні означало «надання форми», «пояснення», «повідомлення» або «уявлення про щось».

Уже на етимологічному рівні це поняття відображає не лише процес передачі відомостей, а й акт упорядкування знань, формування смислів і створення уявлень про навколишню дійсність. У такому розумінні інформація постає не як пасивний набір даних, а як результат інтерпретації, що безпосередньо впливає на пізнавальну та соціальну діяльність людини [338].

У науковому дискурсі інформація розглядається як універсальна категорія, що охоплює процеси створення, збереження, обробки та поширення знань у різних сферах суспільного життя. У політичній науці інформація набуває особливого значення, оскільки виступає ключовим ресурсом влади, інструментом політичної комунікації та засобом формування суспільної свідомості. Вона забезпечує циркуляцію смислів між суб'єктами політики, впливає на прийняття управлінських рішень і визначає характер взаємодії між державою та громадянським суспільством.

Подальший аналіз поняття інформації дозволяє виокремити його багатовимірний характер. З одного боку, інформація може трактуватися як сукупність відомостей незалежно від форми їхнього подання, з іншого - як соціально значущий зміст, що набуває цінності лише в контексті сприйняття, інтерпретації та використання. Саме цей аспект є принципово важливим для дослідження інформаційної безпеки, адже загрози виникають не лише на рівні технічного захисту даних, а й у площині смислових впливів, маніпуляцій та дезінформації.

Дослідник В. Шульга пропонує розглядати інформацію на макро- та мікрорівнях, що дає змогу комплексно оцінити її роль у соціально-економічних і політичних процесах та підкреслити її системний характер. На макрорівні інформація виступає чинником державної могутності: володіння сучасними інформаційно-комунікаційними технологіями забезпечує ефективне управління інформаційним простором, захист національних інтересів і підвищення конкурентоспроможності держави. На мікрорівні інформація розглядається як ключовий ресурс управління організаціями й підприємствами, від якості та

своєчасності якого залежать ефективність управлінських рішень і стабільний розвиток суб'єктів господарювання [338].

Щодо поняття «безпека», то воно позначає стан, за якого особа, група, організація або система перебуває у захищеному положенні та не піддається загрозам, що можуть негативно вплинути на їхнє існування, функціонування чи розвиток. Такий стан передбачає мінімізацію ризиків і потенційної шкоди від зовнішніх або внутрішніх факторів [54, с.34].

Безпеку слід розглядати як соціокультурне явище, що включає не лише фізичний чи правовий захист, а й забезпечення стабільності соціальних структур і культурних цінностей. Вона передбачає стан захищеності людини, родини, етносу, народу або держави разом із їхніми традиціями, звичаями, правами, соціальними нормами, способом життя та системою цінностей. Такий підхід до безпеки підкреслює її комплексний характер, у якому переплітаються соціальні, культурні та правові аспекти, а її підтримання вимагає одночасного врахування інтересів окремих індивідів і суспільства загалом [13, с.396].

В. Пивовар та С. Драчук у своїх наукових розвідках пропонують філософське осмислення категорії «безпека», трактуючи її не як статичний стан, а як безперервний і змінний процес. У такому підході безпека постає фундаментальною потребою, притаманною як окремій людині, так і ширшим соціальним утворенням - нації та державі. Її значущість зумовлюється тим, що стабільне функціонування індивіда й суспільства загалом неможливе без гарантування умов безпечного існування. Відповідно, безпека набуває характеру базової цінності, задоволення якої визначає здатність соціальних і політичних систем до самозбереження, розвитку та адаптації до внутрішніх і зовнішніх викликів. У цьому контексті вона розглядається не лише як результат певної політики чи комплексу заходів, а як постійний процес підтримання рівноваги між потребами, загрозами та ресурсами їх нейтралізації [215, с.77].

Категорія «безпека» постає як багатовимірне явище, що відображає здатність соціальних і політичних систем забезпечувати умови стабільного та сталого існування. Вона передбачає формування такого рівня захищеності, який

уможливлює реалізацію прав, свобод і потреб різних суб’єктів суспільних відносин. Водночас безпека є результатом цілеспрямованої та узгодженої діяльності державних інституцій і громадянського суспільства, спрямованої на збереження та захист базових цінностей і інтересів. Її сутність розкривається не як фіксований стан, а як безперервний процес адаптації до змінного середовища, у межах якого постійно виникають і трансформуються внутрішні та зовнішні загрози. Саме тому безпека завжди має відносний характер і перебуває у діалектичному взаємозв’язку з небезпекою, що зумовлює потребу в постійному оновленні підходів до її забезпечення [19, с.25].

Термін «інформаційна безпека» увійшов до наукового обігу наприкінці 1980-х років і пов’язується з працями німецького дослідника Г. Одермана, який одним із перших акцентував увагу на зростанні ролі інформаційного чинника в системі міжнародної безпеки. У своїх дослідженнях він обґрунтував необхідність комплексного осмислення безпекових викликів, зумовлених поширенням інформаційних технологій, інформаційних впливів та нових форм загроз, що виходять за межі традиційного військово-політичного протистояння. Саме в цей період інформаційна складова починає розглядатися як самостійний вимір безпеки поряд із політичним, економічним і військовим [234; 93].

Подальшого розвитку проблематика інформаційної безпеки набула на початку 1990-х років. У вітчизняних і зарубіжних наукових публікаціях кінця 1991 - початку 1992 років простежується стійка тенденція до активного теоретичного та прикладного осмислення інформаційної безпеки як окремого напряму досліджень. У цей період поняття «інформаційна безпека» поступово виходить за межі суто технічного розуміння захисту інформації та трансформується в комплексну наукову категорію, що охоплює проблеми захисту інформаційних ресурсів, стабільності інформаційного простору, протидії інформаційним загрозам і забезпечення національних інтересів держави в умовах глобалізації та інформатизації суспільства.

Формування поняття “інформаційної безпеки” як самостійного об’єкта наукового аналізу стало відповіддю на глибинні трансформації міжнародних і

внутрішньодержавних суспільно-політичних процесів, пов’язаних із зростанням ролі інформації та інформаційних технологій у сучасному світі.

У сучасній науковій літературі не сформовано уніфікованого підходу до визначення поняття «інформаційна безпека», що зумовлено його складною, багаторівневою та міждисциплінарною природою.

Згідно з класифікацією В. Ліпкана, існують різні підходи до визначення сутності феномена інформаційної безпеки, що дозволяє розглядати її як багатовимірне явище. У цьому контексті інформаційна безпека трактується, зокрема, як стан захищеності інформаційного простору, а також як процес протидії загрозам і небезпекам, спрямований на захист інформаційного середовища, інформації та національних інтересів держави у відповідній сфері. Водночас вона постає як гарантія дотримання законодавчо встановлених норм під час здійснення державних інформаційних процесів і виконання ключових функцій держави, а також як стан безпеки інформаційного середовища і даних, що в ньому функціонують. Окремий акцент робиться на забезпеченні дотримання нормативно-правових вимог у процесі реалізації державної інформаційної політики, що загалом відображає системний і комплексний характер інформаційної безпеки [158, с. 25–30]..

На початкових етапах розвитку інформаційна безпека мала переважно технічний характер, однак із часом еволюціонувала відповідно до змін у комп’ютерних і мережевих технологіях [386, с.97-102].

Інформаційна безпека - це стан захищеності основних інтересів особи, суспільства та держави в інформаційній сфері, що охоплює інформаційну та телекомунікаційну інфраструктуру, а також саму інформацію з її характеристиками: повнотою, об’єктивністю, доступністю та конфіденційністю [108, с.8].

Водночас вона постає й як постійний процес забезпечення її стійкості та адаптивності до внутрішніх і зовнішніх загроз, вона визначається як інтегрована спроможність держави, суспільства та інших суб’єктів зберігати конфіденційність, цілісність та доступність ділової інформації [378]. Таке

узагальнення дозволяє осмислювати інформаційну безпеку як системну характеристику соціальних, політичних і технічних утворень, що забезпечує захист національних інтересів і умови стабільного розвитку в умовах глобалізаційних трансформацій [234].

У трактуванні дослідника М. В. Барана інформаційна безпека постає як комплексний стан захищеності національних інтересів особи, суспільства та держави в межах інформаційної сфери. Йдеться про такі умови, за яких мінімізується або повністю усувається можливість завдання шкоди внаслідок використання неповної, несвоєчасної чи недостовірної інформації, а також у результаті цілеспрямованого негативного інформаційного впливу. Важливим елементом цього підходу є акцент на загрозах, пов’язаних із витоком державної та службової інформації, а також із небажаними наслідками впровадження й застосування сучасних інформаційних технологій [12, с. 33].

На думку О. Рижука, інформаційну безпеку слід розглядати одночасно як стан і процес, оскільки вона покликана забезпечувати захист майбутніх інтересів суб’єктів і об’єктів, що піддаються різноманітним інформаційним впливам. В її концепції виділяються такі ключові ознаки: стан, властивість і управління загрозами та ризиками. Саме завдяки цим ознакам можливо визначити оптимальні стратегії усунення або мінімізації негативних наслідків, що виникають у сфері інформаційної діяльності держави. Такий підхід підкреслює динамічний і комплексний характер інформаційної безпеки, поєднуючи аспекти оцінки поточного рівня захищеності з процесами планування та реалізації заходів протидії інформаційним загрозам [234].

Дослідник В. Богуш визначає інформаційну безпеку, як стан захищеності інформаційного середовища суспільства, який забезпечує його формування, використання та розвиток в інтересах громадян, організацій і держави [19, с. 54].

В.Ліпкан переконаний, що інформаційна безпека виступає однією з ключових складових сталого розвитку держави, оскільки стан інформаційного середовища безпосередньо впливає на ефективність функціонування

політичних інститутів, економічної системи, оборонного сектору та соціокультурної сфери. У цьому контексті процес її забезпечення доцільно розглядати як стратегічне й пріоритетне завдання органів державної влади, реалізація якого потребує узгодження та підпорядкування політичних, економічних, воєнних, культурних та інших напрямів діяльності системи державного управління єдиній меті - захисту національних інтересів в інформаційному просторі та створенню умов для стабільного розвитку держави [157, с. 6; 264, с.97].

Науковець В. М. Фурашев визначає інформаційну безпеку як «…стан захищеності життєво важливих інтересів людини, суспільства і держави, за якого запобігається завданню шкоди через негативний інформаційний вплив, який здійснюється, насамперед, шляхом несанкціонованого створення, поширення та використання свідомо спрямованої за визначеною метою неповної, несвоєчасної, недостовірної або упередженої інформації» [323, с.5].

Водночас інформаційну безпеку доцільно розглядати і як окремий аспект регулювання інформаційних відносин у межах чинного інформаційного законодавства, що відображає правовий вимір забезпечення захисту інформації та пов’язаних із нею процесів [155, с. 48; 264, с.98].

Інформаційна безпека визначається як поточний стан, який оцінюється через потенційний рівень шкоди, здатної вплинути на його існування, функціонування або діяльність у разі реалізації цих загроз. До основних джерел таких загроз, згідно поглядів дослідниці Г. Сащук, належать:

а) використання неповної, несвоєчасної або недостовірної інформації;

б) здійснення негативного інформаційного впливу на об’єкт;

в) протиправне або некоректне застосування інформаційних технологій;

г) несанкціоноване розповсюдження, використання інформації або порушення її цілісності, конфіденційності та доступності [259, с.46.].

Такий підхід дозволяє розглядати інформаційну безпеку як комплексний показник, що відображає ступінь захисту інформаційних ресурсів і процесів від різнопланових загроз [8; 189].

Відповідно до соціально-філософського визначення Є. Архипової, інформаційної безпеки – це стан захищеності свідомості та буття соціальних суб'єктів від інформаційних загроз, який оцінюється через рівень реальної або потенційної шкоди, що може виникнути внаслідок деструктивного інформаційного впливу або порушень інформаційної безпеки. [9, с.9]

Дослідники О. Селецький та Н. Костюченко трактують інформаційну безпеку, як стан захищеності інформаційного простору, який забезпечує комплексний захист інтересів окремої особи, суспільства та держави від інформаційних загроз. Вона передбачає збереження цілісності, достовірності та конфіденційності інформації, а також підтримку належного функціонування інформаційної інфраструктури, що є критично важливим для стабільності соціальних, економічних і політичних процесів [272, с.98].

За твердженням В. Гурковського, інформаційна безпека визначається як сукупність суспільних відносин, що забезпечують захист життєво важливих інтересів окремої особи, громадян, суспільства та держави від реальних та потенційних загроз в інформаційному просторі. Вона передбачає збереження та примноження духовних і матеріальних цінностей держави, підтримку її існування, самозбереження та прогресивного розвитку. Інформаційна безпека, таким чином, є необхідною умовою стабільності та сталого розвитку країни [63, с. 74].

У науковій інтерпретації інформаційну безпеку доцільно розглядати як такий стан інформації, за якого гарантовано дотримання та підтримання її ключових характеристик, визначених відповідною політикою безпеки. Йдеться насамперед про забезпечення встановлених вимог до цілісності, доступності та конфіденційності інформації в межах функціонування інформаційних систем і управлінських процесів. Інформаційну безпеку слід розуміти також як стан, у якому національні та міжнародні ресурси забезпечують захист від інформаційного впливу на свідомість особи та суспільства, перешкоджають маніпуляціям у прийнятті рішень державними інститутами, гарантують недоторканність приватних і державних цифрових баз даних та їх швидке

відновлення у разі протиправних дій, а також передбачають відповідальність зловмисників [131, с. 244].

Загалом, у широкому теоретичному тлумаченні інформаційну безпеку можна визначити як системно організовану сукупність інструментів, підходів і регламентованих дій, спрямованих на охорону інформаційних активів. Вона передбачає підтримання належного рівня надійності та результативності функціонування інформаційних систем, а також збереження функціональної придатності, цілісності й значущості інформації, що створюється, накопичується та обробляється в процесі інформаційної діяльності.

Інформаційна безпека постає не як ізольований сектор безпекової політики, а як структурний компонент більш широкої системи національної безпеки. Захищеність інформаційного простору, стійкість інформаційно-комунікаційної інфраструктури та здатність держави протидіяти деструктивним інформаційним впливам безпосередньо впливають на стан політичної стабільності, суспільної згуртованості, економічного розвитку та обороноздатності. У цьому контексті інформаційна безпека виконує системоутворюючу функцію, оскільки інформаційна сфера пронизує всі ключові складові національної безпеки та забезпечує їх ефективне функціонування.

Відтак національна безпека може бути розглянута як інтегрована категорія, у межах якої інформаційна безпека виступає одночасно самостійним напрямом державної політики й інструментом забезпечення суверенітету, демократичного розвитку та захисту національних інтересів.

У трактуванні Б. Кормича, національна безпека розуміється як стан захищеності держави від внутрішніх і зовнішніх загроз, що забезпечує умови для стабільного існування людини, суспільства та держави відповідно до Конституції та законів України. Відповідно, інформаційна безпека виступає як стан захищеності у сфері обігу інформації, який гарантує стабільність функціонування політичних, соціальних та економічних процесів [136, с. 132].

Будь-які виклики чи загрози, що спрямовані на національну безпеку держави, на переконання О. Панченка, невід’ємно пов’язані з інформаційним

компонентом, адже стан інформаційного середовища визначає ефективність захисту політичних, економічних, оборонних та соціальних інтересів країни. Іншими словами, інформаційна безпека виступає як фундаментальний елемент, без якого неможливе комплексне забезпечення стабільності та стійкого розвитку держави [209].

Генезу інформаційної безпеки, на думку дослідника В. Новицького, можна розглядати через декілька ключових етапів, що відображають еволюцію інформаційних відносин та технологій:

1. До початку XIX століття – інформаційна безпека ґрунтувалася на стихійних засобах комунікації. Основним завданням було захистити інформацію про події, майно, факти та інші життєво важливі дані від фізичного перехоплення, особливо у воєнний час. Важливою складовою було також збереження комерційної та винахідницької інформації.

2. 1816–1935 рр. – початок використання телекомунікаційних і бездротових технологій. Поява передачі інформації через електромагнітні сигнали зумовила необхідність нових методів захисту, включно із завадостійким кодуванням і декодуванням повідомлень.

3. 1935–1946 рр. – розвиток радіолокаційних та підводних акустичних засобів. Основними методами стали організаційні та технічні заходи для протидії активним і пасивним електронним перешкодам. Інформаційна безпека набула особливої значущості під час Другої світової війни, оскільки від неї залежав успіх операцій та виживання військових сил.

4. Середина XX століття – із появою електронних обчислювальних машин (комп’ютерів) постало завдання захисту електронної інформації. Основним способом забезпечення безпеки залишався контроль фізичного доступу до обладнання та носіїв даних.

5. 1960–1970-ті роки – розвиток локальних інформаційно-комунікаційних мереж. Завдання інформаційної безпеки почали включати управління доступом до мережевих ресурсів і захист інформації на підприємствах, оскільки втрата даних могла призвести до збоїв у виробництві.

6. До середини 1980-х років – впровадження ультрамобільних комунікаційних пристроїв. Загрози ускладнилися: з’явилися хакери, бездротові мережі та стандарти безпеки стали критично важливими. Інформація перетворилася на ключовий ресурс держави та бізнесу.

7. З 1985 року до сучасності – розвиток глобальних інформаційно-комунікаційних систем та космічного зв’язку. Поширення автоматизованих виробничих і облікових систем вимагає комплексних заходів інформаційної безпеки, що охоплюють технологічний, програмний та інформаційний рівні, а також впровадження єдиних стандартів і політик безпеки для захисту конфіденційності та цілісності даних [198, с.38].

Інформаційна безпека є багаторівневою системою, що включає взаємопов’язані структурні компоненти, кожен із яких виконує певні функції для забезпечення захищеності інформаційного простору:

Технічний компонент включає засоби захисту інформаційних систем, каналів передачі даних та мереж, а також кібертехнології, алгоритми шифрування, системи виявлення вторгнень, антивірусний захист і резервне копіювання. У політологічному контексті технічний компонент забезпечує стабільність функціонування державних інформаційних ресурсів та надійність прийняття стратегічних рішень.

Інституційний компонент визначає організаційні та нормативно-правові механізми, що регулюють інформаційний простір держави. Охоплює державні органи, законодавство та нормативні акти, системи стратегічних комунікацій, координацію дій між силовими, аналітичними та дипломатичними структурами. Формує рамки допустимого втручання в інформаційні процеси та баланс між безпекою і демократичними свободами.

Соціальний компонент спрямований на підвищення інформаційної стійкості населення через розвиток критичного мислення, медіаграмотності, просвітницьких та фактчекінгових ініціатив, а також підтримку незалежних медіа. Зменшує вразливість суспільства до психологічних операцій і

маніпуляцій, формує культуру відповідального споживання інформації та підтримує соціальну довіру.

Стратегічний (політико-управлінський) компонент реалізує формування та підтримку позитивних державних наративів, спрямованих на консолідацію суспільства, протидію зовнішньому впливу та зміцнення національної єдності. Передбачає планування інформаційної політики, координацію стратегічних комунікацій та інтеграцію національних інтересів у міжнародний інформаційний простір.

Дослідниця В. Світлична виокремлює такі ключові сутнісні характеристики інформаційної безпеки, які розкривають її багатовимірну природу [268, с.99].

По-перше, інформаційна безпека постає як стан захищеності інформаційного простору, що передбачає мінімізацію деструктивних впливів на процеси створення, поширення, зберігання та використання інформації, а також забезпечення його стабільного й прогнозованого функціонування.

По-друге, вона означає захищеність національних інтересів України в інформаційному середовищі, зокрема суверенітету, територіальної цілісності, політичної стабільності та ціннісних орієнтирів суспільства від внутрішніх і зовнішніх інформаційних загроз.

По-третє, інформаційна безпека охоплює захист нормативно закріплених правил здійснення інформаційних процесів у державі, що передбачає дотримання законності в інформаційній сфері, захист прав і свобод суб’єктів інформаційних відносин та ефективне функціонування механізмів правового регулювання.

По-четверте, її слід розглядати як сферу суспільних відносин, пов’язаних із забезпеченням захисту життєво важливих інтересів особи, громадянського суспільства й держави від реальних і потенційних загроз в інформаційному просторі, включно з маніпулятивними впливами, дезінформацією та інформаційною агресією.

По-п’яте, інформаційна безпека є невід’ємною складовою системи національної безпеки, органічно пов’язаною з політичною, економічною, оборонною, соціальною та іншими її вимірами, оскільки стан інформаційного середовища безпосередньо впливає на стійкість держави та її здатність до розвитку в умовах сучасних викликів [268, с.99].

Сучасне розуміння змістових складових інформаційної безпеки передбачає виділення також таких компонентів :

1. Технологічна складова визначається технічними та технологічними можливостями суб’єктів інформаційної сфери. Вона забезпечує захист інформаційних ресурсів і виступає рушійною силою інформаційних трансформацій, впливаючи на розвиток та впровадження інноваційних інформаційних технологій.

2. Правова складова охоплює нормативно-правове регулювання та організацію інформаційних відносин у суспільстві. Вона включає встановлення правил, норм і процедур управління інформаційними процесами, що забезпечують законність, структурованість та ефективність інформаційної діяльності на всіх рівнях.

3. Медіа складова відображає комплексні взаємодії між суб’єктом (зокрема людиною) та інформацією у глобальному інформаційному просторі. Вона охоплює як вплив людини на інформаційні потоки, так і зворотний вплив інформації на свідомість та поведінку суб’єктів, включаючи механізми формування інформаційної культури та захисту від маніпуляцій чи дезінформації.

У сукупності ці три складові формують цілісну систему, яка забезпечує ефективний захист інформаційного середовища та стійкий розвиток інформаційної безпеки на особистісному, суспільному і державному рівнях [299, с. 26-29].

Інформаційна безпека виконує комплекс взаємопов’язаних функцій, які забезпечують захист держави, суспільства та окремих громадян у сучасному інформаційному середовищі. Функціональний вимір інформаційної безпеки

охоплює взаємопов’язану систему напрямів, серед яких базовою є захисна функція, спрямована на запобігання, виявлення та нейтралізацію загроз інформаційному простору, включаючи захист інформаційних ресурсів, критичної інфраструктури та суспільної довіри до політичних інститутів. Контрольна функція забезпечує постійний моніторинг інформаційного середовища, аналіз інформаційних потоків і своєчасне реагування на ризики, тоді як прогностична - орієнтована на передбачення розвитку загроз і формування превентивних механізмів їх нейтралізації на основі аналітичних і технологічних інструментів. Регулятивна функція визначає нормативно-правові засади функціонування інформаційної сфери, встановлюючи правила і стандарти діяльності її суб’єктів. Водночас функція протидії передбачає комплекс заходів із нейтралізації дезінформації, пропаганди та кібератак як через превентивні, так і оперативні інструменти. Завершальною складовою є стратегічна функція, яка спрямована на формування стійкого та позитивного інформаційного середовища, зміцнення національної єдності та забезпечення ефективної державної інформаційної політики.

Функції інформаційної безпеки демонструють її комплексний характер, який поєднує технічні, політичні та соціальні аспекти управління інформаційними процесами. Вони не лише забезпечують оперативний захист інформаційного простору, а й формують стратегічну стійкість держави, підтримують легітимність політичних інститутів та сприяють розвитку інформаційної культури суспільства.

Специфікою інформаційної безпеки виступає також необхідність забезпечення балансу між захистом від загроз і дотриманням демократичних цінностей, таких як свобода слова, право на доступ до достовірної інформації та захист прав людини. Дотримання прав людини залишається невід’ємною складовою правової стратегії держави в умовах цифрових загроз [163, с. 158-160]. Політико-управлінська складова інформаційної безпеки виконує стратегічну функцію підтримки стабільності держави, легітимності політичних інститутів і консолідації суспільства, інтегруючи технічні, організаційні та

соціальні ресурси для реалізації державної політики та протидії зовнішньому впливу.

Особливості та специфіка інформаційної безпеки визначають її як системний, динамічний та стратегічно важливий феномен, що забезпечує захист держави, стабільність політичної системи та соціальну стійкість у сучасному інформаційному просторі, формуючи надійну основу для управління інформаційними процесами в умовах гібридних конфліктів і глобальних інформаційних викликів.

Сучасний розвиток інформаційних технологій та цифрових комунікацій створив нові умови для функціонування інформаційного простору, у якому інформаційна безпека стала критично важливим елементом національної та соціальної стабільності. Особливо це проявляється у контексті глобальної взаємопов'язаності та доступності даних, коли будь-яка інформаційна система чи комунікаційний канал можуть стати об'єктом загроз.

Одним із найбільш актуальних викликів сучасності є використання інформаційного простору як засобу ведення гібридної війни. Гібридна війна поєднує традиційні військові дії з нетрадиційними методами впливу, серед яких інформаційні операції, кібератаки та маніпуляції свідомістю громадян через цифрові платформи. В таких умовах соціальні мережі виступають одночасно як ефективний канал комунікації та як потенційне поле для деструктивного впливу.

Концепт «гібридної війни» вперше був згаданий у вересні 2005 року, коли генерал Джеймс Н. Меттіс представив відповідну ідею на оборонній конференції, організованій Інститутом Військово-морських сил США спільно з Асоціацією Корпусу морської піхоти. Результати цієї конференції згодом були систематизовані та опубліковані у співавторстві з Ф. Гоффманом у статті «Майбутня війна: зліт гібридних воєн» (листопад 2005 р.), що стало першим комплексним науково-практичним обґрунтуванням цього феномена [364]. У цьому дослідженні Гоффман визначає гібридну війну як конфлікт, який поєднує традиційні міждержавні бойові дії з елементами партизанської та асиметричної

війни, використовуючи комплекс сучасних технологій, тактичних прийомів і психологічного впливу на населення [363].

Сучасна гібридна війна стала одним із найпоширеніших інструментів реалізації стратегічних та тактичних цілей, як у внутрішній, так і у зовнішній політиці держав.

Гібридна війна як феномен сучасних міжнародних відносин може бути осмислена як аналітичний та інтелектуальний конструкт, що використовується для пояснення трансформації характеру збройних і політико-стратегічних конфліктів. Насамперед йдеться про такі протистояння, у межах яких поєднується застосування регулярних і іррегулярних сил, а воєнні дії тісно переплітаються з невоєнними формами впливу. У ширшому розумінні гібридна війна охоплює комплекс заздалегідь спланованих і водночас гнучко реалізованих заходів військового, дипломатичного, економічного, політичного, культурного, енергетичного та інформаційного характеру. Ці інструменти використовуються синхронно або послідовно з метою досягнення довгострокових стратегічних цілей без формального оголошення війни. Ключовою особливістю такого типу протиборства є прагнення суб'єкта впливу підпорядкувати політичні, економічні та безпекові інтереси іншої держави власним стратегічним намірам за умов номінального збереження її державного суверенітету та інституційної цілісності [162].

Гібридна війна як форма соціально-політичного конфлікту міждержавного рівня характеризується поступовою ескалацією, що здійснюється через комплекс різноманітних засобів впливу. До них належать психологічний тиск на населення та політичні еліти, маніпуляції масовою свідомістю і розпалювання соціальної напруги, порушення функціонування економічних систем, спотворення демократичних процедур волевиявлення, дестабілізація системи публічної влади та використання дипломатичних технологій для формування сприятливого зовнішньополітичного середовища. Такий підхід дозволяє агресору досягати стратегічних цілей без масштабного застосування традиційних військових методів [88, с.177].

Термін «гібридна війна» у сучасному науковому дискурсі доцільно трактувати як узагальнюючу категорію, що інтегрує різні форми та інструменти сучасного конфлікту. У широкому сенсі під гібридною війною розуміють комплекс дій, які поєднують мілітарні та квазімітарні операції, дипломатичний, інформаційний, економічний та інші засоби впливу, спрямовані на досягнення стратегічних політичних цілей і встановлення переваг однієї сторони над іншою [269].

У щорічній доповіді за 2017 рік Генеральний секретар НАТО Єнс Столтенберг охарактеризував гібридні війни як комплексний тип протиборства, що ґрунтується на поєднанні воєнних і невоєнних інструментів впливу, застосування яких може мати як прихований, так і відкритий характер. До ключових складових такого формату конфлікту він відніс використання інформаційних маніпуляцій, зокрема дезінформації та пропаганди, залучення іррегулярних збройних формувань, а також, за потреби, безпосереднє застосування регулярних збройних сил [153; 154].

Гібридна війна сьогодні розглядається як комплексна форма агресії, що поєднує військові, інформаційні, економічні, політичні та психологічні засоби впливу. За оцінкою Ф. ван Каппена, держави-агресори часто використовують непрямі методи, залучаючи нерегулярні формування та місцеві групи, офіційно дистанціюючись від їхніх дій, що перетворює території на зони потенційного конфлікту [137].

Структурними елементами гібридного протиборства виступають поєднання традиційних і асиметричних загроз, використання терористичних і підривних практик, а також застосування інноваційних та нетипових технологій, покликаних нівелювати або обійти військово-силові переваги супротивника [305, с.173].

Гібридна війна – це вид ворожих дій, де нападник не користується класичним військовим вторгненням, а знищує свого опонента використовуючи ряд секретних операцій, диверсій, кібервійни, а також підтримуючи повстанців, що діють на території супротивника [83, с.60].

На переконання Є. Магди, у період, що передував повномасштабному вторгненню, інформаційний вплив російської федерації на Україну здійснювався через систему взаємопов'язаних методів. До них належали цілеспрямоване поширення дезінформації та використання маніпулятивних технологій, активна пропагандистська діяльність, штучне коригування та фрагментація громадської думки, застосування психологічного й психотропного впливу, а також цілеспрямоване продукування та поширення чуток, покликаних дестабілізувати суспільну свідомість [161, с. 120].

Представники військово-політичного керівництва російської федерації (начальник генштабу В. Герасимов, зокрема, публічно акцентували увагу на перевагах такого формату протиборства. У їхніх концептуальних напрацюваннях гібридна війна постає не лише як сукупність різнорідних засобів впливу, а як стратегія, що дозволяє досягати політичних цілей без формального оголошення війни та з мінімізацією прямих воєнних витрат, надаючи пріоритет невоєнним інструментам тиску над класичними збройними методами [255, с.103].

Події, що відбуваються в сучасній Україні, є наслідком реалізації гібридної війни, в рамках якої інформаційні потоки стають менш контрольованими та більш вразливими до маніпуляцій [7, с.13].

Особливістю будь якої гібридної війни є її синтетичний та багатовекторний характер, що поєднує одночасне використання військових, інформаційних, кібернетичних, економічних та соціальних засобів впливу. Вона відзначається непрямим характером дій, коли основний тиск на державу чи суспільство здійснюється не через відкриті збройні конфлікти, а шляхом інформаційних операцій, політичного та економічного впливу. Гібридна війна носить асиметричний характер: одна зі сторін використовує технологічні, організаційні та інформаційні переваги проти порівняно слабших структур супротивника. Її дії, як правило, тривалі та поступові, без чітко визначених фронтів чи меж, що дозволяє втримувати постійний вплив і уникати прямої ескалації конфлікту. Значну роль у гібридній війні відіграють інформація та комунікаційні

технології, зокрема соціальні мережі та цифрові платформи, які стають основним полем психологічного та інформаційного протистояння. Крім того, гібридна війна відзначається високою гнучкістю та адаптивністю: вона здатна оперативно змінювати стратегії та методи впливу відповідно до зміни політичної, соціальної чи економічної ситуації супротивника, що робить її надзвичайно складним та небезпечним явищем сучасного міжнародного конфліктного середовища.

Згідно з оцінкою науковця О. Ситника, гібридна війна вирізняється низкою специфічних ознак, які відрізняють її від традиційних форм міждержавних конфліктів. По-перше, це агресивні дії без офіційного оголошення війни, що дозволяє країні-агресору зберігати формально легітимні відносини із державою-об’єктом впливу. По-друге, характерною є прихована участь агресора в конфлікті, що часто реалізується через використання нерегулярних або напівзаконних збройних формувань, у тому числі маскування їх під цивільне населення. По-третє, агресор демонструє нехтування міжнародним правом і раніше укладеними угодами, ігноруючи встановлені норми ведення бойових дій. По-четверте, у рамках гібридної стратегії застосовується комплекс політичного та економічного тиску, який здійснюється при формальному збереженні дипломатичних і торговельних зв’язків між сторонами конфлікту. По-п’яте, активне використання пропаганди та контрпропаганди з застосуванням «брудних» інформаційних технологій дозволяє впливати на масову свідомість та дезорганізовувати суспільство. Нарешті, характерним елементом гібридної війни є протистояння в кіберпросторі, що включає кібератаки, інформаційні диверсії та інші форми цифрового впливу [275].

У гібридній війні визначальним є інформаційний вимір, через який за допомогою пропаганди, кібератак і маніпуляцій формується громадська думка, загострюються соціальні суперечності та підривається стабільність держави, що засвідчує перетворення інформації на ключовий інструмент протиборства. Паралельно застосовуються економічні, політичні й військові засоби — від торговельного тиску та втручання в демократичні процеси до використання

нерегулярних збройних формувань - у поєднанні з дипломатичними та психологічними методами впливу. У сукупності це забезпечує досягнення стратегічних цілей без масштабного застосування регулярних військ і відображає комплексний характер сучасної гібридної війни [88, с. 177-178].

Отже, інформаційна безпека є багатокомпонентним явищем, що поєднує технічні, інституційні та соціальні аспекти захисту інформаційного простору та виконує ключову функцію забезпечення стабільності політичної системи й захисту національних інтересів у сучасному інформаційному середовищі. Її структурні компоненти охоплюють технічну складову, що передбачає захист інформаційних систем і каналів передачі даних; інституційну складову, яка забезпечує нормативно-правове регулювання, державне управління та координацію органів влади; а також соціальну складову, що спрямована на формування критичного мислення, підвищення медіаграмотності та протидію дезінформації. Основні функції інформаційної безпеки включають захист інформаційних ресурсів, моніторинг загроз, протидію дезінформаційним, маніпулятивним і психологічним операціям, а також підтримку стратегічних цілей держави у сфері національної та міжнародної безпеки. В умовах гібридної війни інформаційна сфера перетворюється на один із ключових театрів протиборства, де інформаційні впливи поєднуються з політичним, економічним, дипломатичним і воєнним тиском, що суттєво підвищує значущість інформаційної безпеки як інструменту стримування та захисту державного суверенітету. Особливості інформаційної безпеки проявляються у її високій динамічності, багаторівневості та тісному взаємозв’язку між технічними, соціальними й політичними чинниками, що зумовлює необхідність системного, комплексного підходу, який поєднує технологічні, правові та освітні заходи та здатний адаптуватися до трансформації загроз, характерних для гібридної війни та інформаційної агресії. Вивчення сутності, структурних компонентів і функцій інформаційної безпеки створює теоретичну основу для подальшого аналізу нормативно-правових механізмів, технологічних інструментів та державних стратегій протидії інформаційним загрозам, що є критично

важливим для формування стійкого та захищеного інформаційного середовища в умовах сучасних гібридних конфліктів.

1.2. Теоретичні підходи та методологія дослідження інформаційної безпеки

У XXI столітті інформаційна безпека набула статусу одного з ключових елементів системи національної безпеки, що обумовлено трансформацією інформації на стратегічний ресурс управління, розвитку та впливу. В умовах інформатизації та цифровізації суспільства здатність держави забезпечувати ефективне функціонування власного інформаційного простору, використовувати сучасні інформаційно-комунікаційні технології та протидіяти інформаційним загрозам стає визначальним чинником її спроможності конкурувати в економічній, військово-політичній та інших сферах. Інформаційна перевага формує передумови для підвищення стратегічної і тактичної адаптивності, раціоналізації витрат на оборонний розвиток і збереження технологічної першості, що в сукупності істотно впливає на розстановку сил у глобальному середовищі.

Дослідження інформаційної безпеки базується на міждисциплінарних теоретичних підходах, що поєднують політологію, кібернетику, психологію та право. Інформаційна безпека у цьому контексті розглядається не лише як технічний феномен захисту даних, а як комплексний соціально-політичний процес, який забезпечує стабільність держави, консолідацію суспільства та захист національних інтересів у цифровому та інформаційному середовищі.

Проблема інформаційної безпеки розглядається в науковій літературі як багатовимірне явище, що охоплює кілька визначальних напрямків. За К. Захаренком, її слід аналізувати: по-перше, у контексті трансформацій українського суспільства та його політичної системи; по-друге, з огляду на процеси глобалізації сучасного світу; по-третє, у стратегічному вимірі, як перспективу розвитку політичних інститутів, суспільних відносин та процесів,

які забезпечують демократичні зміни та інформаційну безпеку України загалом. [99].

Дослідник М. Баран визначає проблематику інформаційної безпеки через два основні підходи - технологічний та інформаційний. Технологічний підхід зосереджується на технічних і системних параметрах інформації, таких як конфіденційність, цілісність і доступність, і передбачає застосування технічних, програмних та організаційних засобів захисту. Інформаційний підхід орієнтований на соціально-політичні, культурні та психологічні загрози, розглядаючи інформаційну безпеку як складову національної безпеки, спрямовану на запобігання дестабілізації суспільства, підриву довіри до інститутів влади та загрозам державному суверенітету. Інтегративний підхід поєднує обидва напрямки, що дозволяє розглядати інформаційну безпеку як багатовимірне явище сучасного інформаційного простору [12].

У науковому середовищі існують теорії, які безпосередньо або опосередковано стосуються проблем інформаційної безпеки. Вони дозволяють розглядати її як багатовимірне явище, що включає як стан захищеності інформаційної сфери, так і динамічний процес забезпечення її стійкості та адаптивності до різноманітних загроз.

Зокрема, теорія інформаційної війни пропонує модель інформаційної війни, що базується на чотирьох основних елементах: інформаційні ресурси, учасники, наступальні операції та оборонні операції (Д. Деннінг).

Прихильники цієї теорії розглядають інформацію не лише як засіб передачі даних, а як стратегічний ресурс впливу на свідомість, поведінку та рішення суб’єктів у різних сферах – політичній, економічній, військовій та соціальній. Основна ідея теорії полягає в тому, що сучасні конфлікти дедалі частіше включають інформаційні компоненти, де контроль над інформаційними потоками, маніпуляція свідомістю та створення інформаційних переваг стають ключовими чинниками стратегічного протистояння.

Наукове осмислення інформаційної війни охоплює кілька взаємопов’язаних аспектів:

1. **Політичний аспект** – використання інформації для формування громадської думки, легітимації влади, впливу на прийняття рішень державними й недержавними акторами.

2. **Військово-стратегічний аспект** – застосування інформаційних технологій та засобів комунікації для досягнення переваг у воєнних конфліктах, дезорганізації управління противника та забезпечення власної безпеки.

3. **Соціальний аспект** – маніпулювання соціальною свідомістю, створення дезінформаційних кампаній і контроль над інформаційними каналами для управління поведінкою громадян.

4. **Економічний аспект** – вплив на ринки, інвестиційну привабливість, стратегічні галузі через інформаційні операції та технологічні маніпуляції.

У науковій літературі теорія інформаційної війни підкреслює, що сучасні конфлікти не обмежуються традиційним військовим протистоянням, а дедалі більше переходять у сферу інформаційного впливу, де перемога визначається не лише фізичною потужністю, а й ефективністю контролю інформаційних потоків та здатністю формувати переваги в інформаційному просторі [146].

Теорія мотивації захисту (теорія захисної мотивації) прогнозує наміри користувачів захищати себе після отримання рекомендацій, що викликають страх [381]. Ця теорія полягає в поясненні того, як індивіди формують мотивацію до захисної поведінки у відповідь на сприйняті загрози. Теорія була запропонована Р. Роджерсом і широко використовується в дослідженнях ризиків, безпеки, здоров’я, комунікацій та інформаційної безпеки.

Теорія мотивації захисту у контексті дослідження сучасних загроз інформаційній безпеці в соціальних мережах в умовах гібридної війни в Україні дає змогу пояснити механізми формування індивідуальної та колективної готовності до протидії деструктивним інформаційним впливам. У межах цієї теорії сприйняття користувачами соціальних мереж інформаційних загроз - зокрема дезінформації, маніпулятивного контенту, інформаційно-психологічних операцій та ворожої пропаганди - розглядається як результат когнітивної оцінки

рівня небезпеки та власної вразливості в умовах тривалого гібридного протистояння. Водночас важливу роль відіграє оцінка ефективності захисних стратегій, таких як розвиток медіаграмотності, критичне осмислення інформації, використання перевірених джерел та цифрових інструментів безпеки, а також усвідомлення власної здатності реалізувати ці стратегії в повсякденній комунікативній практиці.

З позицій теорії мотивації захисту мотивація до безпечної інформаційної поведінки формується не лише під впливом об'єктивних загроз, а й через суб'єктивне сприйняття їхньої серйозності та ймовірності впливу на особисті, суспільні й державні інтереси. В умовах гібридної війни це набуває особливого значення, оскільки соціальні мережі виступають ключовим середовищем поширення ворожих наративів і водночас простором, де можливе формування стійкості до інформаційних атак. Якщо користувачі оцінюють захисні заходи як ефективні, а витрати на їх застосування - як прийнятні, зростає ймовірність адаптивної поведінки, спрямованої на мінімізацію інформаційних ризиків. Таким чином, застосування теорії мотивації захисту дозволяє глибше зрозуміти поведінкові аспекти інформаційної безпеки в соціальних мережах та обґрунтувати необхідність комплексних стратегій підвищення інформаційної стійкості українського суспільства в умовах гібридної війни.

Водночас кількість теорій, які безпосередньо стосуються інформаційної безпеки, є обмеженою.

Теорію інформаційної безпеки, що розглядає безпеку як процес формування стійких і життєздатних інформаційних ресурсів через систему контрольних заходів у умовах постійних і змінних загроз, запропонували дослідники А. Крейг Горн, Б. Шон Мейнард та А. Атіф Ахмад. У цьому підході інформація трактується як багатоформний і нематеріальний об'єкт, який може існувати на фізичних, цифрових і когнітивних носіях, має різний рівень цінності та чутливості й за відсутності належного захисту неминуче зазнає деградації. Контролі, спрямовані на забезпечення конфіденційності, цілісності та доступності, виступають інструментами захисту інформації від відомих і

невідомих загроз, однак не гарантують її абсолютної недоторканності в умовах динамічного середовища. Основна мета інформаційної безпеки в цій логіці полягає не в самому збереженні інформації, а у перетворенні її на надійний ресурс, здатний підтримувати ефективність діяльності організацій і держави [358].

За своєю галузевою та науковою спрямованістю теорія інформаційної війни належить до категорії високих гуманітарних технологій (high-hum technologies), які включають сукупність знань, культурних і духовних цінностей, а також методів передачі інформації, спрямованих на координацію та стимулювання колективної діяльності людей [146, с.98].

Водночас теорія інформаційної безпеки має низку обмежень, пов’язаних із множинністю її концептуалізацій, різними рівнями застосування та відсутністю універсальних критеріїв достатнього рівня захищеності, що зумовлює потребу подальшого теоретичного уточнення і міждисциплінарного розвитку цього напряму

Різноманітність підходів до визначення інформаційної безпеки обумовлена складністю інформаційної сфери та поєднанням у ній правових, політичних, технологічних і соціокультурних вимірів. У науковій літературі, як відзначає дослідник І. Недохлєбов, виокремлюють два взаємодоповнювальні підходи. Перший, правоцентристський, розглядає інформаційну безпеку як систему правових і інституційних гарантій, що забезпечують реалізацію права на інформацію та її захист, підкреслюючи взаємозв’язок між безпекою і можливістю користування інформаційними правами. Другий, безпекоцентристський, зосереджується на виявленні загроз інформаційній сфері та механізмах їх нейтралізації, трактуючи інформаційну безпеку як складову національної безпеки, спрямовану на захист життєво важливих інтересів особи, суспільства і держави від інформаційних впливів та ризиків [196, с.27]. Поєднання цих підходів забезпечує комплексне розуміння інформаційної безпеки як багатовимірного явища, що враховує одночасно права людини та стійкість суспільства і держави перед інформаційними загрозами.

Щодо гібридної війни, то у західному цивілізаційному дискурсі, зокрема в США та країнах НАТО, концепція «гібридної війни» спирається на класичну модернізаційну теорію та застосовується для аналізу військових операцій у державах, які перебувають на стадії неповної державності або «недорозвинених» політичних структур [89, с.104].

Класичні теоретичні підходи до осмислення процесів модернізації були сформульовані у працях таких визначних соціальних і політичних мислителів, як О. Конт, Г. Спенсер, К. Маркс, М. Вебер, Е. Дюркгейм та Ф. Тьонніс. Саме їхні концепції заклали підґрунтя для подальшого аналізу трансформацій традиційних суспільств у модерні, акцентуючи увагу на змінах соціальної структури, економічних відносин, форм раціональності та типів соціальної взаємодії.

Модернізаційна теорія в політичній науці розглядає суспільний розвиток як поступальний процес переходу від традиційних форм соціальної організації до сучасних, що характеризуються зростанням ролі раціональності, інституційної диференціації, технологічного прогресу та ускладненням комунікативних процесів. У контексті інформаційного суспільства модернізація безпосередньо пов’язана з цифровізацією, розвитком масових і соціальних медіа, розширенням інформаційних потоків та трансформацією механізмів політичної комунікації. Водночас ці процеси не лише сприяють демократизації та відкритості, а й породжують нові ризики, пов’язані з маніпуляцією свідомістю, асиметрією доступу до інформації та зростанням уразливості держави й суспільства до зовнішніх інформаційних впливів. Умови гібридної війни в Україні актуалізують модернізаційну перспективу як інструмент аналізу суперечливого характеру інформаційних трансформацій, у межах яких розвиток цифрових технологій одночасно виступає чинником прогресу та джерелом загроз інформаційній безпеці.

З позицій модернізаційної теорії інформаційна безпека постає не лише як технічна або правова проблема, а як складова загального процесу соціально-політичної трансформації, що вимагає адаптації інституцій, норм і моделей

поведінки до нових комунікативних реалій. Ефективність протидії інформаційним загрозам у соціальних мережах значною мірою залежить від рівня інституційної зрілості держави, розвитку громадянського суспільства та здатності політичної системи забезпечувати баланс між свободою інформації й захистом національних інтересів. Модернізаційна теорія дозволяє інтерпретувати інформаційну безпеку як динамічний процес, тісно пов'язаний із загальним вектором суспільного розвитку та ступенем модернізованості політичних і комунікативних інститутів.

Дискурс гібридної війни виходить за межі традиційних медійних платформ і охоплює широку сферу соціальної комунікації. Він проявляється через різноманітні канали передачі інформації – від класичних друкованих та електронних медіа до інтернет-ресурсів, а також через неформальні комунікаційні практики, включно з приватними обговореннями, експертними дискусіями та офіційними дипломатичними контактами. Така багаторівнева інформаційна структура формує можливості для реалізації інформаційного впливу, моделювання суспільної свідомості та координації політичних і стратегічних дій учасників конфлікту.

Феномен гібридної війни, на переконання дослідниці Г. Яворської, проявляється у двох основних модусах існування: матеріальному (фізичному) та дискурсивному. Ці модуси характеризуються асиметрією: у матеріальному вимірі конфлікт, зокрема російсько-український, локалізується на певних територіях, тоді як дискурсивний вимір охоплює глобальний інформаційний простір. Інтерпретаційна, когнітивна складова гібридної війни реалізується через дискурсивні, вербально-семіотичні механізми, що формують сприйняття конфлікту на міжнародній арені та впливають на соціальну, політичну та економічну поведінку цільових аудиторій [344].

На формування концепції гібридної війни істотно вплинули положення теорії мереже-центричних війн, що виникла наприкінці 1990-х років у контексті трансформації воєнно-стратегічного мислення під впливом інформаційно-комунікаційних технологій. Концепція мережоцентричної війни розглядається

як сучасна теоретична модель ведення збройної боротьби, що ґрунтується на використанні мережевих принципів організації, управління та обміну інформацією між військовими підрозділами. Її розробка пов’язується з діяльністю Управління трансформації Збройних сил США під керівництвом віце-адмірала Артура Себровскі, де вона формувалася як відповідь на зміну характеру сучасних воєнних конфліктів та зростання ролі інформаційних технологій.Він разом із Джоном Гарсткою належать до числа перших дослідників, які концептуально обґрунтували засади мережоцентричної війни (NCW). Вони наголошували на необхідності трансформації традиційної платформо-орієнтованої моделі ведення бойових дій у мережоцентричну, що базується на інтеграції інформаційних, командних і бойових ресурсів у єдину мережу [353].

Ця теорія ґрунтується на ідеї, що визначальним ресурсом сучасного збройного протиборства стає інформація, а ключовою перевагою - здатність ефективно інтегрувати всі елементи військової організації в єдину інформаційно-управлінську мережу.

Однією з центральних тез мережецентричної концепції є твердження про перевагу так званих «мережевих сил» (networked forces) над традиційними збройними формуваннями[162]. Йдеться про збройні сили, у яких забезпечено горизонтальну та синхронізовану взаємодію між різними рівнями управління, підрозділами й функціональними структурами. Така модель дозволяє досягти високого рівня ситуаційної обізнаності, скоротити час ухвалення рішень і підвищити узгодженість дій, що в підсумку трансформується в оперативну й стратегічну ефективність.

Загальна інформатизація та інтелектуалізація систем керування військами якісно змінюють зміст воєнних операцій, розширюючи їх за межі суто військового виміру. У межах мережецентричного підходу війна розглядається як багатовимірний процес, що охоплює не лише фізичний простір бойових дій, а й інформаційний, соціальний і когнітивний виміри. Це означає, що воєнне протиборство може здійснюватися у всіх ключових сферах функціонування

держави та суспільства - політичній, економічній, соціальній, культурній та інформаційній. Другою принциповою тезою теорії мережецентричних війн є надзвичайна роль інформаційної боротьби. У війнах XXI століття стратегічна мета дедалі частіше полягає не у фізичному знищенні противника, а в підриві його морально-психологічної стійкості, дезорганізації систем управління та позбавленні здатності до ефективного спротиву. Саме інформаційні, психологічні та когнітивні впливи розглядаються як ключові інструменти досягнення переваги, оскільки вони дозволяють впливати на процеси прийняття рішень і поведінку як політичних еліт, так і широких верств населення.

Отже, дослідження теоретичних підходів і методів вивчення інформаційної безпеки дозволяє зробити висновок про її комплексний і міждисциплінарний характер. Інформаційна безпека розглядається не лише як технічний феномен захисту даних, а як складний соціально-політичний процес, що поєднує технологічні, інституційні, соціальні та правові складові. Теорії інформаційної війни, мотивації захисту та модернізаційна теорія дозволяють пояснити сучасні інформаційні процеси з різних перспектив: перша підкреслює стратегічне та мережеве використання інформації у конфліктних ситуаціях, друга розкриває механізми формування поведінки користувачів і готовності до протидії загрозам, а третя фокусує увагу на соціально-технологічних трансформаціях, що впливають на інформаційні потоки та уразливість систем. Технічні та кібернетичні методи спрямовані на створення ефективних механізмів захисту інформаційних систем і мереж, а правовий підхід визначає нормативні межі державного втручання та забезпечує баланс між безпекою і демократичними цінностями. Інтеграція цих підходів і методів дозволяє формувати цілісне наукове розуміння інформаційної безпеки як системного феномену, що є критично важливим для розробки стратегій протидії загрозам, підвищення стійкості інформаційного простору та забезпечення національної безпеки в умовах сучасних гібридних конфліктів і глобалізованого інформаційного середовища.

Методологію наукового дослідження доцільно розглядати як цілісну систему концептуальних засад, принципів, методів і організаційних підходів, що визначають логіку та послідовність наукового пізнання конкретної проблеми. Вона забезпечує узгодженість усіх етапів дослідницького процесу та виступає основою для отримання обґрунтованих і достовірних результатів .

Системний підхід до аналізу сучасних загроз інформаційній безпеці в соціальних мережах в умовах Війни за Незалежність дозволяє розглядати інформаційну безпеку як багатовимірне явище, що формується на перетині технологічних, соціальних, політичних, правових та психологічних складових. Соціальні мережі виступають каналами масового поширення інформації, що включає як достовірні, так і маніпулятивні повідомлення, а їхня структура та швидкість розповсюдження інформації визначають потенційну шкоду від дезінформації.

Технологічна складова передбачає вивчення технічних механізмів захисту даних, алгоритмів модерації контенту та вразливостей платформ, а забезпечення інформаційної безпеки в цьому середовищі вимагає комплексного застосування програмних і апаратних засобів, систем моніторингу та автоматизованого виявлення загроз.

Соціально-психологічний аспект системного аналізу дозволяє оцінити вплив інформації на поведінку користувачів, формування громадської думки та рівень довіри до інститутів влади, прогнозуючи можливі соціальні наслідки цільових інформаційних впливів. Політична та стратегічна складові акцентують увагу на ролі інформаційної безпеки як елемента національної стратегії в умовах Війни за Незалежність, що включає координацію дій державних, громадських і медійних інституцій для протидії зовнішнім впливам і захисту національної ідентичності.

Правовий аспект визначає рамки нормативного регулювання цифрового середовища, встановлює відповідальність за поширення дезінформації та кіберзлочини, а системний підхід дозволяє виявляти прогалини в законодавстві та пропонувати комплексні рішення для захисту інформаційного простору.

Використання системного підходу дозволяє оцінювати загрози комплексно, враховуючи взаємозв’язок усіх елементів інформаційного середовища, і сприяє розробці ефективних превентивних та реактивних механізмів протидії загрозам. Завдяки цьому підхід забезпечує інтеграцію технологічних, соціальних, психологічних, політичних і правових рішень, що підвищує стійкість держави та суспільства до інформаційних атак, особливо в умовах інтенсивного інформаційного впливу та Війни за Незалежність.

Системне мислення та системний підхід ґрунтуються на розгляді об’єктів як цілісних утворень, властивості яких формуються не сумою окремих елементів, а характером взаємозв’язків між ними. У межах такого підходу аналітичний фокус зміщується з окремих компонентів на рівні організації системи та їх взаємодію з зовнішнім середовищем, що дозволяє виявляти нові, інтегративні властивості, відсутні на нижчих рівнях складності. Відповідно, інформаційна безпека розглядається як динамічний стан інформаційно-телекомунікаційної системи, що відповідає актуальним потребам її суб’єктів та підтримується через функціонування комплексної системи захисту інформації як невід’ємної підсистеми цієї цілісності [199].

У межах дослідження сучасних загроз інформаційній безпеці в соціальних мережах в умовах Війни за Незалежність системний підхід дозволяє розглядати інформаційну безпеку як цілісне, багаторівневе утворення, функціонування якого зумовлене сукупністю взаємопов’язаних елементів і процесів. Такий підхід орієнтує аналіз не лише на окремі прояви інформаційних загроз, а й на логіку їх виникнення, поширення та нейтралізації в межах єдиного інформаційного простору. З позицій системності ключового значення набуває визначення мети функціонування системи інформаційної безпеки, кола суб’єктів, залучених до її забезпечення, а також об’єктів впливу, які перебувають у політичній, військовій, економічній, технологічній та комунікативній сферах суспільного життя.

Системний підхід передбачає також аналіз механізмів і інструментів, за допомогою яких здійснюється регулювання інформаційних процесів і протидія

деструктивним впливам, зокрема в соціальних мережах як ключовому середовищі сучасного інформаційного протиборства. У цьому контексті інформаційна безпека постає як комплексна система, спрямована на захист інформації, знань та інформаційних систем від несанкціонованого доступу, використання, модифікації, спотворення чи знищення, що може завдати шкоди національним інтересам і суспільній стабільності. Забезпечення такої безпеки здійснюється через поєднання програмних, технічних, організаційно-методичних, інформаційних і правових засобів, які застосовуються як окремими фахівцями, так і спеціалізованими підрозділами державних інституцій та іншими суб'єктами інформаційної політики [349, с.240].

Функціональний підхід передбачає дослідження інформаційної безпеки через призму її ролі та завдань у забезпеченні нормального функціонування соціальних, політичних і технічних систем. У цьому підході безпека розглядається не як ізольований процес, а як функція, що виконує конкретні завдання: захист інформаційних потоків, підтримка цілісності та доступності даних, забезпечення довіри до інформаційного середовища та створення умов для стабільної роботи систем у цілому.

Функціональний підхід до розуміння інформації розвиває В. Богуш, який розглядає її як властивість систем, здатних до самоорганізації [19]. Цей підхід дозволяє виділити ключові функції, які забезпечують стійкість інформаційного простору. Це, зокрема, виявлення та нейтралізація дезінформаційних повідомлень, протидія психологічним операціям та маніпуляціям масовою свідомістю, контроль достовірності інформаційних потоків і координація дій державних, громадських та технічних суб'єктів, відповідальних за безпеку.

Функціональний підхід орієнтує аналіз інформаційних загроз на їхній вплив на реалізацію базових функцій інформаційної системи та соціально-комунікативних процесів, підкреслюючи, що ефективність інформаційної безпеки в соціальних мережах в умовах Війни за Незалежність України визначається поєднанням технологічних, організаційних, правових і соціальних чинників та здатністю системи своєчасно адаптуватися до динамічних викликів.

Відповідно до структурно-функціонального підходу, інформацію доцільно розглядати як стратегічний ресурс, що безпосередньо впливає на стан національної безпеки та потребує цілісної державної політики, заснованої на науково обґрунтованих моделях управління. У цьому контексті структурно-функціональний підхід дозволяє поєднати аналіз цілей, функцій і організаційних елементів системи забезпечення інформаційної та інформаційно-психологічної безпеки, враховуючи їх взаємодію та здатність до адаптації в умовах мінливого інформаційного середовища. Така модель інтерпретує систему інформаційної безпеки як цілеспрямований і динамічний механізм, спроможний ідентифікувати внутрішні й зовнішні загрози, формувати адекватні відповіді на інформаційні виклики та трансформувати власну структуру і функції відповідно до завдань протидії деструктивним інформаційним впливам у межах гібридного протиборства [115, с.16-23].

Соціальний підхід розглядає інформаційну безпеку через призму впливу інформації на суспільство та взаємодії між його суб'єктами. У цьому підході акцент робиться на соціальні процеси, поведінку індивідів і груп, а також на механізми формування суспільної думки, довіри до державних інститутів та соціальної стабільності. Інформаційна безпека в соціальному контексті оцінюється за здатністю протидіяти деструктивним інформаційним впливам, маніпуляціям масовою свідомістю, дезінформаційним кампаніям і психологічним операціям, що можуть дестабілізувати соціальні відносини або політичну систему. У контексті соціальних мереж соціальний підхід дозволяє аналізувати не лише технічні аспекти загроз, а й їхній вплив на поведінку користувачів, культурні та ціннісні орієнтири, рівень соціальної взаємодії та ідентичності. Він підкреслює роль комунікаційних мереж у формуванні інформаційного простору, визначає групи ризику та потенційні «вузькі місця», через які деструктивні інформаційні потоки можуть проникати в суспільство.

Соціальний підхід сприяє розробці комплексних стратегій інформаційної безпеки, що включають освітні програми, підвищення медіаграмотності, формування критичного мислення та створення систем підтримки користувачів.

Він підкреслює, що безпека інформаційного простору неможлива без врахування соціально-психологічних факторів і активної участі суспільства у протидії інформаційним загрозам.

Соціальний вимір поняття інформації акцентує В. А. Ліпкан, який трактує її як продукт життєдіяльності соціальних форм матерії, насамперед людського суспільства. Інформація, за таким підходом, існує об’єктивно, однак її реальний зміст і значення виявляються лише в процесі пізнання людиною навколишнього світу та соціальної взаємодії. Саме соціальний контекст надає інформації ціннісного, нормативного й політичного виміру, що є особливо важливим для дослідження проблем інформаційної безпеки [157].

Важливим складником методології є сукупність наукових методів і прийомів, які використовуються для аналізу, інтерпретації та узагальнення отриманої інформації. До них належать як універсальні пізнавальні інструменти (аналіз і синтез, індуктивні та дедуктивні підходи, порівняння), так і спеціалізовані методики, що враховують специфіку предмета дослідження. Сукупне застосування цих елементів забезпечує цілісність, наукову коректність і аргументованість дослідницьких результатів.

При аналізі сучасних загроз інформаційній безпеці в соціальних мережах в умовах Війни за НезалежністьУкраїни, було використано синергетичний підхід,. У методологічному вимірі синергетика спирається на принципи системного аналізу та теорії змін, водночас формуючи власну дослідницьку оптику. Її специфіка полягає у зосередженні на динаміці розвитку та трансформації складних систем, включаючи як процеси їх упорядкування, так і дезінтеграції. Важливе місце відводиться ролі невпорядкованості, яка розглядається не лише як чинник руйнування, але й як потенційне джерело виникнення нових структур і станів. Суттєвим аспектом є аналіз механізмів самоорганізації, що відбуваються завдяки узгодженій взаємодії елементів системи, а також урахування множинних внутрішніх і зовнішніх зв’язків, які визначають її функціонування. Синергетичний підхід підкреслює значущість середовища як чинника змін і адаптаційних можливостей системи, а також

орієнтується на узагальнене розуміння закономірностей її еволюції, що випливають із природи самих процесів і явищ [175].

Саме він дозволив інтерпретувати інформаційний простір як складну відкриту систему з нелінійною динамікою розвитку. У такій системі інформаційні потоки, поведінка користувачів і комунікаційні взаємодії перебувають у постійному русі та взаємовпливі, що зумовлює появу ефектів самоорганізації та непередбачуваних трансформацій. З позицій синергетики соціальні мережі можна розглядати як середовище, у якому навіть незначні інформаційні імпульси здатні спричиняти масштабні наслідки через механізми резонансу та мультиплікації. Це пояснює, чому окремі дезінформаційні повідомлення або маніпулятивні наративи можуть швидко набувати широкого розповсюдження і впливати на масову свідомість. Практична цінність цього підходу полягала у можливості виявлення критичних точок розвитку інформаційних процесів, тобто моментів, коли система стає особливо чутливою до зовнішніх впливів і може перейти в якісно новий стан. Крім того, синергетика дала змогу проаналізувати формування та функціонування онлайн-спільнот як саморегульованих структур, у межах яких відбувається як поширення, так і підсилення інформаційних впливів. Застосування синергетичного підходу обґрунтувало необхідність комплексної взаємодії різних суб’єктів забезпечення інформаційної безпеки, адже узгоджені дії державних інституцій, цифрових платформ, медіа та громадянського суспільства здатні створювати кумулятивний ефект, що підвищує ефективність протидії інформаційним загрозам.

У дослідженні застосовується поєднання методологій: феноменологічний підхід до типу зібраних даних та методологія обґрунтованої теорії (grounded theory) для збору, аналізу та інтерпретації даних [358].

У межах дослідження сучасних загроз інформаційній безпеці в соціальних мережах ефективним є застосування методів аналізу та синтезу, які дозволяють розчленувати складні інформаційні процеси на окремі компоненти -

загрози, канали поширення, вразливі елементи та заходи контролю - і водночас об’єднати їх у цілісну систему для оцінки взаємозв’язків і ефективності захисту.

Компаративістський метод у політичних дослідженнях спрямований на виявлення спільних закономірностей та відмінних характеристик політичних систем, їхніх інститутів і механізмів функціонування в різних країнах та історичних умовах. Його застосування дає змогу здійснювати системне порівняння політичних явищ з метою визначення як універсальних рис, так і специфічних особливостей їх розвитку [176, с.9]. Метод порівняльного аналізу використовувався для зіставлення національних та міжнародних практик у сфері інформаційної безпеки, оцінки різних моделей реагування на інформаційні загрози та визначення найефективніших стратегій протидії. Компаративістика у цьому випадку виступила інструментом виявлення спільних тенденцій, відмінностей та ефективних моделей реагування на інформаційно-психологічні виклики.

Передусім, порівняльний аналіз дав змогу оцінити особливості інституційного забезпечення протидії інформаційним загрозам в Україні та інших державах, зокрема щодо ролі державних органів, механізмів координації та рівня залучення приватного сектору. Окремий напрям компаративного дослідження був пов’язаний з аналізом практичних інструментів протидії, таких як стратегічні комунікації, системи моніторингу інформаційного простору, співпраця з цифровими платформами та розвиток медіаграмотності. Це дозволило визначити, які з міжнародних практик можуть бути адаптовані до українських реалій з урахуванням специфіки Війни за Незалежність України. Використання порівняльного методу забезпечило не лише аналітичну глибину дослідження, але й практичну орієнтованість отриманих висновків, спрямованих на підвищення рівня інформаційної безпеки України.

Герменевтика як метод інтерпретації спрямована на розуміння змістів, смислів і контекстів текстів, повідомлень та символічних форм комунікації [55, с.45]. У випадку інформаційної війни вона дозволяє аналізувати не лише сам

факт поширення інформації, а й приховані значення, інтерпретаційні рамки та цільові наративи, закладені в повідомленнях у соціальних мережах.

У межах дослідження інформаційної безпеки цей підхід був особливо корисним для: аналізу пропагандистських і дезінформаційних текстів з точки зору їхніх смислових конструкцій; виявлення маніпулятивних стратегій впливу на масову свідомість; розуміння того, як різні аудиторії інтерпретують одні й ті самі інформаційні повідомлення; дослідження контексту формування інформаційних наративів у гібридній війні. Він дозволив не лише фіксувати інформаційні загрози як явище, але й розкрити їхній змістовний і смисловий рівень, що є важливим для глибшого розуміння механізмів інформаційного впливу в соціальних мережах.

Соціологічні методи та метод контент-аналіз дозволяють досліджувати вплив інформаційних кампаній на політичну поведінку громадян, формування громадської думки та рівень суспільної поляризації. Це включає аналіз матеріалів соціальних мереж, медіа, офіційних заяв політичних акторів, що допомагає оцінювати ефективність інформаційних впливів і визначати цільові групи населення, вразливі до дезінформації.

Методи прогнозування та моделювання політичних процесів дозволяють оцінювати потенційні наслідки інформаційних загроз для стабільності держави, суспільної довіри та легітимності політичних інститутів, а також формувати стратегічні сценарії розвитку інформаційної безпеки.

Зокрема, метод комп’ютерного моделювання загалом дає змогу формалізувати складні соціальні процеси та відтворювати їхню динаміку в умовах змінних параметрів [24, с.49]. Цей метод дозволив досліджувати соціальні мережі як складні нелінійні системи, у яких навіть незначні інформаційні імпульси можуть спричиняти масштабні наслідки через ефект «ланцюгового поширення». Крім того, моделювання забезпечило можливість виявлення найбільш вразливих елементів інформаційного простору та оцінки ефективності заходів протидії інформаційним загрозам.

Метод комп’ютерного моделювання виступив допоміжним аналітичним інструментом, який доповнив традиційні якісні та кількісні методи дослідження і підсилив розуміння механізмів функціонування інформаційних загроз у соціальних мережах в умовах Війни за Незалежність України.

У наукових дослідженнях, присвячених аналізу загроз інформаційній безпеці, широко застосовується розвинений математичний інструментарій, основу якого становлять методи теорії ймовірностей та теорії ігор [369, с. 35–48]. Використання цих підходів дає змогу формалізувати невизначеність, оцінювати рівень ризиків і прогнозувати можливі сценарії реалізації загроз. Зокрема, для вивчення процесів здійснення атак на інформаційні ресурси у залучаються положення теорії диференціальних ігор і диференціальних перетворень [365]. Зазначені методи забезпечують формування ґрунтовних теоретико-математичних моделей, які відображають динаміку протиборства та слугують основою для комплексного аналізу й прогнозування розвитку відповідних процесів.

До структури методологічного забезпечення дослідження входять, насамперед, загальні принципи організації наукової роботи, які формують її теоретико-методологічний фундамент. Серед них ключове значення мають принципи системності, об’єктивного підходу, історичної обумовленості, комплексності та використання міждисциплінарних зв’язків, що дозволяють розглядати досліджувані явища у взаємозв’язку та розвитку. При дослідженні сучасних загроз інформаційній безпеці важливо дотримуватися принципів об’єктивності та історизму, які передбачають неупереджене оцінювання фактів і подій та врахування їх розвитку в історичному контексті, що дозволяє коректно інтерпретувати еволюцію загроз, ролі інформації як стратегічного ресурсу та трансформацію інформаційних систем. Так, зокрема, принцип історизму дає змогу простежити її розвиток у суспільстві та зміну значущості цього феномена. Зокрема, він показує, як інформаційна безпека набула критичного значення в процесі переходу від індустріального до постіндустріального

суспільства, коли інформація стає стратегічним ресурсом, а складність потоків даних і пов’язаних із ними загроз істотно зростає.

Отже, таким чином, методологія дослідження сучасних загроз інформаційній безпеці в соціальних мережах в умовах Війни за Незалежність України має комплексний та міждисциплінарний характер. Її основу становить поєднання загальнонаукових принципів (системності, об’єктивності, історизму, комплексності) та різних методологічних підходів, що забезпечують цілісне осмислення досліджуваного явища. Використання системного, функціонального та структурно-функціонального підходів дозволяє розглядати інформаційну безпеку як складну багатокомпонентну систему, що перебуває у постійній взаємодії з соціальним і технологічним середовищем. Синергетичний підхід акцентує увагу на нелінійному характері інформаційних процесів і їхній здатності до швидких трансформацій. Додатково компаративістський, герменевтичний, соціологічний та моделювальний інструментарій забезпечує як порівняльний аналіз практик протидії загрозам, так і поглиблене розуміння змісту інформаційних впливів та їхньої динаміки.

1.3. Нормативно-правова база дослідження інформаційної безпеки

Нормативно-правова база інформаційної безпеки є не лише сукупністю юридичних норм, а й важливим інструментом реалізації державної інформаційної політики та відображенням політичних пріоритетів держави. У політологічному вимірі правове регулювання інформаційної безпеки розглядається як складова механізму влади, що визначає правила взаємодії між державою, суспільством та суб’єктами інформаційного простору. Саме через нормативно-правові акти держава інституціоналізує своє бачення загроз, формує стратегічні цілі та закріплює моделі реагування на інформаційні виклики.

Особливого значення набуває аналіз поєднання міжнародних і національних правових норм, адже інформаційна безпека дедалі більше

виходить за межі внутрішньої політики та стає елементом глобальних політичних процесів. Міжнародні правові документи, стандарти й рекомендації впливають на формування національних підходів, водночас адаптація цих норм до внутрішнього законодавства відображає специфіку політичного режиму, рівень демократичності та особливості державного управління.

Політична стабільність у контексті Війни за Незалежність України проявляється через прозорі та демократичні механізми формування органів влади, що забезпечують легітимність державних рішень і довіру громадян. Важливим є демократичний транзит влади, тобто передбачувана і мирна зміна керівництва, що мінімізує внутрішні конфлікти та потенційну експлуатацію вразливостей противником (Додаток Л).

Ефективна протидія вимагає, в першу чергу, створення відповідної законодавчої бази та регуляторних механізмів, які б дозволяли швидко реагувати на інформаційні загрози та притягати до відповідальності винних у поширенні дезінформації.

Розвиток міжнародної правової бази для протидії ІПсО формує правові рамки для ефективного реагування на інформаційні загрози, забезпечуючи узгодженість дій на глобальному рівні.

Для прикладу, «Countering Foreign Propaganda and Disinformation Act» (2016) («Про протидію іноземній пропаганді та дезінформації») – закон США, ухвалений у грудні 2016 р. в межах пакету Національного закону про оборону (NDAA), спрямований на посилення державної спроможності протидіяти іноземній пропаганді та дезінформації, насамперед з боку росії, Китаю та інших авторитарних режимів. Документ передбачив створення Глобального центру взаємодії (Global Engagement Center, GEC) при Державному департаменті США для координації інформаційних зусиль урядових структур, громадських організацій та міжнародних партнерів. Серед ключових завдань закону - моніторинг та аналіз інформаційних кампаній, що становлять загрозу національним інтересам США; організація міжвідомчої взаємодії для ефективної протидії маніпуляціям; надання фінансової й технічної підтримки

незалежним медіа в державах із обмеженою свободою слова; а також розробка стратегічних комунікацій та контрнаративів для спростування пропагандистських повідомлень. Ухвалення цього закону стало важливим кроком до формування системної політики США у сфері інформаційної безпеки, вплинуло на розвиток аналогічних механізмів у державах ЄС та НАТО й заклало підґрунтя для міжнародної співпраці у протидії дезінформаційним загрозам [357].

6 серпня 2020 р. президент Д. Трамп видав виконавчий наказ відповідно до Закону про міжнародні надзвичайні економічні повноваження (IEEPA), який забороняв усі взаємодії громадян США з китайською компанією ByteDance Ltd, фактично забороняючи використання популярного додатка TikTok на території США. Хоча адміністрація Дж.Байдена скасувала наказ Трампа, сам президент Байден видав власний указ щодо технологій іноземного походження, що свідчить про те, що проблеми кібербезпеки й надалі залишатимуться актуальними [354].

У Сінгапурі у 2019 р. ухвалено “Закон про захист від онлайн-фальсифікацій та маніпуляцій” (“Protection from Online Falsehoods and Manipulation Act”, POFMA), спрямований на боротьбу з поширенням неправдивої інформації та фейкових новин. Закон надає уряду розширені повноваження щодо нагляду за онлайн-платформами, веб-сайтами та навіть приватними груповими чатами. Зокрема, міністри можуть вимагати від інтернет-платформ видалення або редагування матеріалів, які вважаються неправдивими та шкідливими для суспільних інтересів, а у разі необхідності блокувати доступ до веб-ресурсів. За невиконання вимог закону передбачено значні штрафи (до 733–735 тис. доларів США) та ув’язнення до 10 років. Прем’єр-міністр Лі Сянь Лун зазначив, що нові норми дозволяють швидко реагувати на дезінформацію та захищати країну від ворожих інформаційних кампаній, водночас уряд обіцяє, що санкції будуть більше спрямовані на компанії, ніж на окремих громадян. Саме цей Закон став одним із найбільш суворих законів світу щодо онлайн-дезінформації, поєднуючи адміністративні,

цивільні та кримінальні механізми впливу, а його ухвалення відображає тенденцію країн Південно-Східної Азії посилювати контроль над цифровим інформаційним простором [311; 312; 276; 277].

У березні 2016 р. Євразійський центр Атлантичної ради (Atlantic Council) опублікував рекомендації щодо захисту демократичних суспільств від дезінформації. Документ створено за участю понад 100 експертів із різних країн, включно з науковцями, журналістами, урядовцями та представниками IT-компаній. Основна мета – запропонувати заходи для урядів і приватного сектору та створення Коаліції протидії дезінформації. Потреба у протидії дезінформації зросла через втручання росії у вибори 2016 р. у США та аналогічні випадки в Європі [71].

Ключовим інструментом ЄС у боротьбі з інформаційними маніпуляціями, який створив підґрунтя для правового регулювання цифрових платформ і заклав основу для інтеграції механізмів саморегулювання у загальноєвропейське законодавство став «Code of Practice on Disinformation» («Кодекс практики з дезінформації») – добровільний саморегулятивний інструмент ЄС, спрямований на протидію поширенню дезінформації в цифровому середовищі. «Кодекс практики з дезінформації» став першим інструментом, за допомогою якого ключові гравці цифрової індустрії домовилися про стандарти саморегулювання для боротьби з дезінформацією ще у 2018 р. Він встановив стандарти для онлайн-платформ щодо контролю політичної реклами, маркування фейкових акаунтів і ботів, співпраці з фактчекінговими організаціями та моніторингу поширення неправдивого контенту. У 2022 р. відбулося оновлення документа, яке включало чіткіші показники ефективності, розширення кола учасників і інтеграцію з правовими механізмами Digital Services Act, що посилило прозорість та підзвітність цифрових платформ у боротьбі з дезінформацією [355].

Регламентом Європейського Союзу, спрямованим на створення сучасної правової бази для цифрових платформ та онлайн-послуг є «Digital Services Act» (DSA) («Про єдиний ринок цифрових послуг» 2022 р.). Він встановлює правила

щодо відповідальності платформ за поширення незаконного контенту, дезінформації та шкоди користувачам, а також забезпечує прозорість алгоритмів, модерації контенту та реклами. DSA регулює діяльність великих онлайн-платформ, встановлюючи спеціальний контроль над ризиками, пов'язаними з дезінформацією та маніпуляціями та вводить обов'язки прозорості, включно з публікацією інформації про рекламні кампанії та рекомендації алгоритмів. Особливу увагу приділено дуже великим онлайн-платформам, які мають значний вплив на суспільну думку [360].

Стратегія «ProtectEU», представлена Європейською Комісією 1 квітня 2025 р., є комплексним підходом до внутрішньої безпеки ЄС, спрямованим на підвищення стійкості держав-членів до гібридних загроз та забезпечення безпеки громадян. Стратегія базується на інтегрованому підході, який охоплює державні інституції, громадянське суспільство, бізнес і наукову спільноту. Основними напрямами реалізації є посилення повноважень Europol, розширення складу Frontex до 30 000 осіб до 2027 р., створення Європейської системи критичних комунікацій, а також удосконалення цифрових посвідчень особи для забезпечення безпеки та стійкості громадян і критичної інфраструктури [379]. Стратегія підкреслює необхідність комплексного реагування на гібридні кампанії, що включають кібератаки, дезінформацію, втручання у вибори та інші форми асиметричного впливу, і спрямована на створення системи постійного моніторингу, адаптації та взаємодії між цивільними та державними інституціями для протидії сучасним і майбутнім загрозам [380].

Стратегія впроваджує інтегрований «whole-of-society» підхід, залучаючи громадян, бізнес і громадські організації, та передбачає гармонізацію з іншими документами безпекового блоку ЄС, такими як «Preparedness Union Strategy», «European Defence White Paper», «European Democracy Shield».

У межах ЄС сформовано комплексну багаторівневу систему нормативно-правового регулювання у сфері кібербезпеки. Ця система спрямована на забезпечення належного рівня захисту цифрового простору, запобігання,

виявлення та нейтралізацію сучасних кіберзагроз, а також на створення єдиних стандартів реагування на інциденти безпеки для всіх держав-членів ЄС. Вона має безпосереднє значення для трансформації українських систем правового та інституційного забезпечення. До ключових актів відносяться: Директива NIS (2016 р.), яка визначає основи безпеки мереж та інформаційних систем; Директива NIS2 (2022 р.), що розширює рамки кіберзахисту та вводить суворіші вимоги до суб'єктів критичної інфраструктури; Регламент «Cybersecurity Act» (2019 р.), який встановлює мандат і структуру сертифікації ENISA; Регламент GDPR (2016 р.), спрямований на захист персональних даних та обов'язок повідомляти про порушення їх безпеки; Регламент Digital Operational Resilience Act (DORA), що регламентує цифрову стійкість фінансового сектору; Регламент Digital Services Act (DSA), орієнтований на забезпечення безпеки та підзвітності цифрових платформ; Регламент Digital Markets Act (DMA), який забезпечує ринкову конкуренцію та враховує кібербезпековий вимір; а також Cyber Resilience Act, що встановлює стандарти кіберзахисту на рівні цифрових продуктів [256, с.11].

Одним із перших європейських лідерів, який зайняв активну позицію щодо боротьби з дезінформацією, став президент Франції Е. Макрон. Навесні 2018 р. уряд Франції подав до Національних зборів законопроект, спрямований на обмеження поширення фейкових новин, який згодом було ухвалено [148].

20 листопада 2018 р. Франція ухвалила закон про боротьбу з маніпулюванням інформацією ("Lutte contre la désinformation"), який передбачає низку заходів для забезпечення прозорості та достовірності інформації під час виборчих кампаній, розширення повноважень Вищої аудіовізуальної ради, яка отримала право припиняти трансляцію телеканалів, контрольованих іноземними державами. Окрему увагу законодавці приділили запобіганню втручанню іноземних держав і засобів масової інформації у вибори. Також закон передбачає спеціальне регулювання соціальних мереж, зокрема Facebook і Twitter, які зобов'язані надавати інформацію про замовний

контент та політичну рекламу, що сприяє підвищенню прозорості інформаційного простору та ефективнішому протидії дезінформації [315; 164].

У Великій Британії “Закон про телерадіомовлення” (1990 р.) зобов’язує медіа дотримуватися неупередженості та точності в новинах, а регулятор Ofcom накладає штрафи на порушників. Хоча фінансові санкції застосовуються рідко, репутаційні наслідки для медіа, визнаних винними, ефективно стримують поширення дезінформації. Подібна практика виявилася успішнішою за повну заборону медіа; аналогічні заходи застосовують Литва та Латвія, штрафуючи російські державні ЗМІ [71].

У Німеччині центральним нормативним актом у сфері протидії дезінформації є закон “NetzDG” (2017), який зобов’язує соціальні платформи видаляти незаконний контент протягом 24 годин після його виявлення та регулярно звітувати про порушення. Закон спрямований на запобігання поширенню дезінформації та маніпуляцій, а його ефективність забезпечується системою штрафів і контролю. Додатково реалізуються урядові програми з медіаграмотності, що навчають громадян розпізнавати фейки та критично оцінювати інформаційні повідомлення [350].

Сукупність нормативних документів задає орієнтири для України у питаннях модернізації законодавства, вдосконалення інституційної архітектури, створення системи звітування, а також розробки програм підготовки й перепідготовки фахівців у сфері протидії кіберзлочинності та забезпечення кіберстійкості.

Україна активно розвиває законодавчу базу та створює спеціальні інституції для протидії інформаційним маніпуляціям та інформаційно-психологічним операціям

Основними законодавчими актами є: Конституція України, Закон України «Про інформацію», Закон України «Про основні засади забезпечення кібербезпеки України», Закон України «Про національну безпеку України» та Закон України «Про медіа», «Доктрина інформаційної безпеки України» та інші документи.

Конституція України закладає правові засади захисту інформаційного простору держави та громадян від деструктивного інформаційного впливу. Відповідно до Конституції України, «Захист суверенітету і територіальної цілісності України, забезпечення її економічної та інформаційної безпеки є найважливішими функціями держави, справою всього Українського народу» (Стаття 17). Стаття 34 Конституції гарантує право на свободу думки, слова та поширення інформації, одночасно передбачаючи, що це право не може використовуватися для заподіяння шкоди національній безпеці, державному суверенітету, територіальній цілісності, конституційному ладу та правам інших осіб. Саме Конституція України виступає основою для формування нормативно-правової та інституційної системи захисту від інформаційних загроз, забезпечуючи баланс між свободою слова та національною безпекою. [378].

Швидке впровадження інформаційних технологій і глобалізація інформаційних відносин спричинили зростання занепокоєння щодо стану кібербезпеки об’єктів критичної інфраструктури. В Україні актуальність цієї проблеми відображалася ще у рішенні РНБО від 17 листопада 2010 р. «Про виклики та загрози національній безпеці України у 2011 році», де одним із пріоритетів було створення єдиної системи протидії кіберзлочинності для захисту критичної інфраструктури. Однак, на той час законодавство охоплювало лише окремі об’єкти, тоді як єдиного порядку їх класифікації та визначення ключових термінів не було [208, с. 101].

Указом Президента України від 25 лютого 2017 р. затверджено «Доктрину інформаційної безпеки України», яка визначає національні інтереси в інформаційній сфері та напрями державної політики щодо захисту інформаційного простору. Мета доктрини - протидія деструктивному впливу рф, зокрема через пропаганду війни, розпалювання національної і релігійної ворожнечі, зміну конституційного ладу або порушення суверенітету та територіальної цілісності України. Пріоритети державної політики в інформаційній сфері передбачають удосконалення нормативно-правового регулювання механізмів виявлення, фіксації, оперативного реагування,

обмеження доступу та видалення з інформаційного простору держави, зокрема з українського сегмента мережі Інтернет, інформаційних матеріалів, що становлять загрозу життю і здоров'ю громадян України, містять заклики до війни, розпалюють національну або релігійну ворожнечу, пропагують насильницьку зміну конституційного ладу чи посягання на територіальну цілісність держави, а також можуть підривати державний суверенітет [81].

Доктрина є важливою в для кібербезпеки, оскільки останню, відповідно до поглядів І. Діордіци доцільно розглядати як підсистему інформаційної безпеки], яка охоплює лише ту частину інформаційної сфери, де для обробки інформації використовуються інформаційно-телекомунікаційні системи [336, с.299; 78, с. 201].

Закон України «Про національну безпеку України» встановлює правові, організаційні та методологічні засади забезпечення комплексної безпеки держави, включно з протидією інформаційним загрозам. Він визначає інформаційну безпеку як ключовий компонент національної безпеки, що охоплює захист державних інтересів у сфері інформаційного простору, системи комунікацій, медіа та критичної інформаційної інфраструктури від деструктивного впливу, дезінформації, пропаганди та інших видів інформаційних атак.

Закон закріплює обов'язок держави забезпечувати превентивне виявлення загроз, своєчасне реагування на інформаційні атаки, а також підвищення стійкості суспільства до дезінформаційних кампаній. Законом також передбачено створення інституційної та нормативної бази для координації дій органів державної влади, силових структур та громадських організацій, спрямованих на нейтралізацію інформаційних загроз [97].

Закон України «Про інформацію» визначає принципи державної інформаційної політики та заборону поширення недостовірної інформації. Відповідно до Статті 3 (Розділ 1), "Основними напрямами державної інформаційної політики є:… забезпечення інформаційної безпеки України" [95].

Правові та організаційні основи забезпечення кібербезпеки в Україні визначаються Законом України «Про основні засади забезпечення кібербезпеки України» від 5 жовтня 2017 р. № 2163-VIII та Стратегією кібербезпеки України, затвердженою Указом Президента України від 26 серпня 2021 р. № 447/2021. [205].

Закон України «Про основні засади забезпечення кібербезпеки України» встановлює правові та організаційні рамки для захисту національної інформаційної інфраструктури та протидії інформаційним загрозам. Основними засадничими принципами закону є визначення державних пріоритетів у сфері кібербезпеки, забезпечення інтегрованого підходу до захисту критично важливих об’єктів інформаційної та комунікаційної інфраструктури, а також координація дій усіх суб’єктів у кіберпросторі. Закон закріплює обов’язок державних органів здійснювати моніторинг загроз, аналізувати потенційні ризики та оперативно реагувати на кібератаки, у тому числі на ті, що мають інформаційний характер. Особлива увага приділяється протидії дезінформаційним кампаніям, маніпуляціям у медіа та спробам втручання у роботу державних інформаційних систем. Ключовим завданням закону є створення системи превентивного та реагуючого характеру: вона передбачає не лише виявлення та блокування шкідливих впливів у кіберпросторі, а й підвищення обізнаності користувачів, розвиток медіаграмотності. В Законі подається чітке визначення поняття “система активної протидії агресії у кіберпросторі”, яке визначається як комплекс організаційних, правових, наукових і технічних заходів, спрямованих на підвищення рівня кіберзахисту держави.

Активна протидія агресії у кіберпросторі включає конкретні дії, спрямовані на нейтралізацію кібератак держави-агресора, його систем і мереж, а також усіх джерел походження кіберзагроз.

Система активної протидії у кіберпросторі виступає інтегрованим механізмом національної безпеки, який поєднує превентивні та заходи

реагування для ефективного протидії кіберзагрозам і збереження суверенітету держави у цифровому середовищі [98].

Одним із основних завдання державної політики у сфері медіа (Стаття 5 Закону України «Про медіа») є «забезпечення ефективного нагляду (контролю) за дотриманням на території України вимог і обмежень у сфері медіа, передбачених цим Законом, з метою захисту національного медіа-простору України та побудови інформаційного середовища, здатного протистояти актуальним загрозам інформаційній безпеці» [96].

Стратегія національної безпеки України, затверджена Указом Президента України від 14 вересня 2020 року № 392/2020 [289], визначає пріоритети та шляхи зміцнення безпеки держави в умовах війни та з урахуванням особливостей кіберпростору.

Постанова Кабінету Міністрів України від 23.12.2020 №1295 «Деякі питання забезпечення функціонування системи виявлення вразливостей і реагування на кіберінциденти та кібератаки» визначає основні засади функціонування системи виявлення вразливостей та реагування на кіберінциденти й кібератаки, яка здійснюється щодо об’єктів кіберзахисту, зазначених у частині другій статті 4 Закону України «Про основні засади забезпечення кібербезпеки України» [65].

Відповідно до Статті 107 Конституції України та Закону України «Про національну безпеку України», Указом Президента України «Про рішення Ради національної безпеки і оборони України від 15 жовтня 2021 року «Про Стратегію інформаційної безпеки» було введено в дію та затверджено рішення Ради національної безпеки і оборони України від 15 жовтня 2021 року «Про Стратегію інформаційної безпеки» [306]. Досягнення цієї мети здійснюється через заходи стримування та протидії загрозам інформаційній безпеці, нейтралізацію інформаційної агресії, зокрема спеціальних інформаційних операцій держави-агресора, розвиток системи взаємодії між органами влади, місцевого самоврядування та суспільством, а також зміцнення міжнародної співпраці на засадах партнерства і взаємної підтримки.

Першочергова стратегічна ціль полягає у протидії дезінформації та інформаційним операціям, насамперед з боку держави-агресора, які загрожують незалежності України, конституційному ладу, суверенітету та територіальній цілісності держави, пропагують війну та насильство, розпалюють ворожнечу й ненависть, здійснюють терористичні акти та порушують права людини. Для цього передбачено створення системи раннього виявлення, прогнозування та запобігання гібридним загрозам, включно з медіа-моніторингом національних і іноземних медіа, аналізом інформаційного простору, добуванням та опрацюванням розвідувальної інформації, запуском систем електронного моніторингу та підготовкою звітів за результатами моніторингу. Стратегія передбачає налагодження ефективної взаємодії між державними органами, місцевим самоврядуванням та інститутами громадянського суспільства, інституційне посилення роботи Центру стратегічних комунікацій, забезпечення наукового супроводу, реалізацію проєктів для захисту національного інформаційного простору та протидії втягуванню громадян у незаконні збройні формування. Важливим стратегічним напрямком також визначається підвищення рівня медіакультури та медіаграмотності суспільства з метою захисту від дезінформації та маніпулятивної інформації (проведення просвітницьких кампаній, запровадження курсу медіаграмотності у школах, навчання державних службовців і місцевих посадових осіб, організація тренінгів, конференцій, семінарів та інших заходів для розвитку критичного мислення та навичок роботи з інформацією) [306].

Для забезпечення безпечного функціонування кіберпростору та його ефективного використання в інтересах людини, суспільства і держави розроблена та затверджена «Стратегія кібербезпеки України» [292], затверджена Указом Президента України від 26 серпня 2021 року № 447/2021. Стратегія визначає основні напрямки забезпечення кібербезпеки, зокрема: захист критичної інфраструктури, включно з енергетичними, транспортними та фінансовими системами; розвиток сучасних технологій для моніторингу, виявлення та нейтралізації кіберзагроз, а також удосконалення

криптографічного захисту даних; підвищення обізнаності населення та формування культури кібергігієни; формування постійно діючого міжвідомчого координаційного механізму взаємодії з провідними ІТ-компаніями, глобальними провайдерами цифрових послуг та адміністраціями соціальних мереж [303, с.664].

Сучасна нормативна база у сфері протидії інформаційним загрозам визначає функції та повноваження ключових інституцій, формуючи цілісну систему захисту інформаційного простору, що корелює з підходами, застосовуваними у світовій практиці.

Отже, нормативно-правова база інформаційної безпеки в політологічному контексті постає як інструмент державної влади та засіб політичного управління інформаційними процесами. Міжнародні правові акти закладають загальні рамки та принципи забезпечення інформаційної безпеки, формуючи спільний дискурс реагування на глобальні інформаційні загрози, тоді як національне законодавство конкретизує ці підходи відповідно до внутрішніх політичних умов і стратегічних інтересів держави. Українська нормативно-правова база у сфері інформаційної безпеки відображає процеси інституціоналізації державної інформаційної політики та трансформації уявлень про інформаційну безпеку як складову національної безпеки. Вона фіксує роль ключових політичних акторів, визначає межі державного втручання в інформаційний простір та окреслює баланс між безпековими пріоритетами і демократичними цінностями.

Інформаційна безпека виступає багатокомпонентним феноменом, що інтегрує технічні, соціальні, інституційні та правові аспекти захисту інформаційного простору і виконує ключову роль у забезпеченні стабільності політичної системи та захисту національних інтересів у сучасному інформаційному середовищі. Вона охоплює низку структурних компонентів: технічну складову, що передбачає захист інформаційних систем, мереж і каналів передачі даних; інституційну складову, яка забезпечує нормативно-

правове регулювання, координацію діяльності державних органів та управління інформаційними потоками; а також соціальну складову, що включає підвищення медіаграмотності, формування критичного мислення та протидію дезінформації. Ключові функції інформаційної безпеки зосереджені на захисті інформаційних ресурсів, моніторингу загроз, протидії маніпулятивним, дезінформаційним та психологічним операціям, а також на підтримці стратегічних цілей держави в сфері національної та міжнародної безпеки.

У сучасних умовах Війни за Незалежність України інформаційна сфера стає одним із ключових театрів протиборства, де інформаційні впливи поєднуються з політичним, економічним, дипломатичним та воєнним тиском. Це підвищує значущість інформаційної безпеки як інструменту захисту державного суверенітету і стримування зовнішніх загроз. Особливості інформаційної безпеки проявляються у високій динамічності, багаторівневості та тісному взаємозв'язку технічних, соціальних і політичних чинників, що зумовлює необхідність застосування системного та комплексного підходів, інтегруючих технологічні, правові та освітні заходи, здатних адаптуватися до трансформації загроз у сучасних інформаційних конфліктах.

Дослідження теоретичних підходів демонструє міждисциплінарний характер інформаційної безпеки. Політологічний підхід підкреслює її роль у підтримці стабільності держави, легітимності політичних інститутів та формуванні суспільних настроїв. Соціологічно-психологічний аспект дозволяє оцінити вплив інформаційних потоків на громадську свідомість і поведінку користувачів, а технічні та кібернетичні методи спрямовані на створення ефективних механізмів захисту інформаційних систем і мереж. Інтеграція цих підходів дозволяє формувати цілісне наукове розуміння інформаційної безпеки як системного феномену, що включає не лише захист даних, а й соціально-політичні, правові та організаційні складові.

Теорії сучасної інформаційної безпеки дають змогу розглядати проблему з різних перспектив. Теорія інформаційної війни підкреслює стратегічне та мережеве використання інформації у конфліктних ситуаціях. Теорія мотивації

захисту пояснює механізми формування поведінки користувачів та готовності до протидії загрозам. Модернізаційна теорія фокусується на соціально-технологічних трансформаціях, що впливають на інформаційні потоки та вразливість систем, а структурно-функціональний підхід дозволяє оцінювати взаємодію елементів системи та забезпечувати її адаптивність.

Методи аналізу та синтезу забезпечують комплексну оцінку інформаційних загроз, їх взаємозв'язків та наслідків, дозволяючи формувати ефективні стратегічні та тактичні заходи захисту. При цьому дотримання принципів об'єктивності та історизму забезпечує неупереджене оцінювання процесів і подій у контексті їх розвитку, що дозволяє адекватно інтерпретувати сучасні загрози та роль інформації як стратегічного ресурсу.

Нормативно-правова база виступає інструментом державного управління та політичного регулювання інформаційних процесів.

Загалом, теоретичні підходи та методи дослідження інформаційної безпеки формують наукову основу для розробки стратегій протидії загрозам, підвищення стійкості інформаційного простору, захисту національних інтересів і забезпечення безпеки держави в умовах гібридних конфліктів та глобалізованого інформаційного середовища.

РОЗДІЛ 2. ОСОБЛИВОСТІ ТА ТЕХНОЛОГІЇ ВЕДЕННЯ ГІБРИДНОЇ ВІЙНИ В СОЦІАЛЬНИХ МЕРЕЖАХ

2.1. Соціальні мережі як інструмент стратегічного впливу

У сучасному глобалізованому світі, де інформаційні технології стали невід'ємною частиною повсякденного життя, соціальні мережі відіграють все більш значущу роль у формуванні суспільної думки, політичних процесів та національної безпеки. Вони стали не лише платформою для спілкування та обміну інформацією, але й потужним інструментом впливу на масову свідомість, що може бути використаний як для конструктивних, так і для деструктивних цілей.

Інформаційні потоки стають дедалі менш контрольованими, що ускладнює їхнє централізоване регулювання, як наслідок, управління конфліктами поступово зміщується в інформаційний простір [84]. Саме тут відбувається боротьба за інтерпретацію подій, формування наративів та вплив на громадську думку, що робить інформаційну сферу повноцінним полем протистояння, поряд із традиційними воєнними та політичними засобами. У такій ситуації дедалі більшої актуальності набуває питання забезпечення інформаційної безпеки, адже саме вона покликана гарантувати захист суспільства та держави від маніпуляцій, дезінформаційних атак і підриву довіри до демократичних інститутів. Забезпечення інформаційної безпеки в соціальних мережах стає критично важливим завданням для держави, яке вимагає комплексного підходу та постійної адаптації до нових викликів та загроз.

Соціальна мережа - структуроване середовище взаємодії, яке складається з великої кількості агентів (суб’єктів - індивідуальних або колективних, таких як особа, сім’я, група, організація) та сукупності відносин між ними, що проявляються у вигляді зв’язків, наприклад, знайомств, співпраці, або комунікацій. У цифровому середовищі соціальні мережі реалізують аналогічні

структурні принципи, проте надають можливість масштабної взаємодії та обміну інформацією в режимі онлайн, що підвищує значущість таких мереж як інструментів комунікації, формування громадської думки та потенційних ризиків кібербезпеки.

Термін «соціальна мережа» у широкому значенні був уперше введений у науковий обіг англійським соціологом Дж. Барнсом у 1954 р. у праці «Людські взаємини». За допомогою цього поняття він підкреслював, що суспільство є складною мережею взаємозв'язків між людьми. Дж. Барнс також досліджував міжособистісні відносини з використанням візуальних діаграм, на яких окремі особи зображувалися крапками, а зв'язки між ними – лініями, що дозволяло наочно відображати структуру соціальних взаємин [282, с.7-8].

Історія соціальних мереж починається ще з середини 1980-х рр. із появою перших онлайн-сервісів, таких як CompuServe, Prodigy та The Well, які, на той час, забезпечували базові можливості спілкування, участі в дискусійних групах та розміщення оголошень. Першим соціально-мережевим ресурсом у сучасному розумінні дефініції вважається Classmates.com (1995 р.), що дозволяв користувачам відновлювати контакти з однокласниками та друзями. Проте довгий час він не підтримував створення особистих профілів і додавання друзів, обмежуючи взаємодію рамками навчальних закладів [283].

Початок 2000-х ознаменувався також появою ключових соціальних та комунікаційних платформ, які не лише забезпечили нові способи взаємодії користувачів, а й сформували фундамент для сучасного цифрового суспільства, інтегруючи соціальні, професійні, освітні та медіа-функції.

Соціальна платформа визначає технічну або програмну інфраструктуру, яка забезпечує функціонування онлайн-сервісів для взаємодії користувачів. Платформа встановлює правила користування, набір функцій, алгоритми поширення контенту та взаємодії, а також механізми модерації і моніторингу. Соціальна мережа є соціальною структурою або системою, яка формується на базі взаємозв'язків користувачів, об'єднаних спільними інтересами, діяльністю, контактами чи групами. У цифровому середовищі мережа проявляється через

конкретні зв’язки між користувачами на платформі. Взаємозв’язок між цими поняттями полягає в тому, що платформа виступає технічним інструментом для створення, підтримки та розвитку соціальної мережі, а мережа існує у межах платформи, формуючи фактичну соціальну структуру користувачів.

Прикладом соціальних платформ виступили Facebook, LinkedIn, Twitter або YouTube. Соціальні мережі початку XXI ст. заклали основу сучасного цифрового комунікаційного простору. У грудні 2002 р. Рейд Хоффман заснував LinkedIn, який запущено в травні 2003 р. [258]. Платформа орієнтована на професійний нетворкінг, розвиток ділових контактів, пошук компаній і тематичних груп, а після придбання Microsoft у 2016 р. значно розширила функціональні можливості та використовується для бізнесу, освіти та наукової діяльності [140].

4 лютого 2004 р. Марк Цукерберг запустив Facebook, спочатку для студентів Гарварду, а згодом для ширшої аудиторії [327]. До 2008 р. платформа перевершила MySpace і стала глобальною мережею, доступною понад 40 мовами. Завдяки цільовій рекламі Facebook перетворився на одну з провідних платформ для передвиборчих кампаній у світі: зокрема, команда Дональда Трампа витратила понад 40 млн доларів на рекламу у Facebook за п’ять місяців до виборів президента США 2020 р. Facebook також сприяв організації місцевих політичних рухів, зокрема під час «арабської весни», коли спільно із Twitter, відіграв важливу роль у координації протестів і поширенні інформації. Водночас Facebook зазнав істотної критики у зв’язку із його роллю у поширенні мови ворожнечі, що, за даними звіту ООН 2018 р., сприяло насильству проти мусульман рохінджа в М’янмі [320].

У 2005 р. з’явився YouTube, що дозволило завантажувати, переглядати та коментувати відеоматеріали. У 2006 р. сервіс придбала компанія Google, що сприяло його швидкому розвитку. YouTube є глобальною відеоплатформою, доступною майже у всіх країнах світу, за винятком окремих держав (Іран, Туреччина, Китай, Саудівська Аравія, Судан, Пакистан, Бангладеш), які блокували його переважно з політичних та цензурних міркувань. Сервіс

перекладений 83 мовами, включно з українською (від 13 грудня 2012 р.) та пропонує контент найрізноманітніших жанрів - від навчальних відео й блогів до музики, фільмів і розважальних роликів [47].

Twitter, створений Джеком Дорсі у 2006 р., запровадив формат мікроблогів для коротких повідомлень, з можливістю додавання фото, відео та коментарів, і швидко здобув популярність у світі [181].

У червні 2011 р. Google запустила соціальну мережу Google+, інтегровану з іншими сервісами компанії, однак через низьку популярність її закрили у 2019 р. [341].

Комунікаційна платформа Skype, створена естонськими програмістами Нікласом Зеннстрьомом та Янусом Фріїсом, забезпечувала голосові та відеоконференції, а після придбання Microsoft у 2011 р. отримала ширші функціональні можливості та підтримку користувачів. На піку популярності Skype мав понад 300 млн активних користувачів на місяць і став ключовим інструментом віддаленого спілкування, навчання та роботи, особливо під час пандемії COVID-19, однак із появою сучасних конкурентів (Zoom, Teams, Google Meet) його популярність почала спадати, а Microsoft поступово в 2025 р. перенесла функції сервісу до платформи Teams [278].

Розвиток соціальних мереж від професійних платформ і мікроблогів до глобальних медіаплатформ сформував сучасний цифровий простір, що поєднує комунікацію, обмін контентом та інтерактивну взаємодію користувачів на міжнародному рівні [282, с. 7–13].

В Україні активне використання соціальних мереж розпочалося приблизно у 2006 р. з появою платформ «Однокласники» та «ВКонтакте».

Стрімкий розвиток мережевих та мобільних технологій зумовив безпрецедентну популярність масштабних соціальних платформ. Однак зростання їхньої аудиторії неминуче привертає увагу зловмисників, які використовують ці ресурси для поширення шкідливого програмного забезпечення, викрадення персональних даних та маніпулювання громадською думкою. Соціальні мережі вже давно перестали бути лише каналами

комунікації, перетворившись на проактивні середовища впливу на масову свідомість. Комерційні платформи збирають великі обсяги даних про поведінку користувачів - переваги, історію переглядів, взаємодії, час активності - і використовують їх для персоналізації контенту. Частина платформ, зокрема Facebook, LinkedIn і Google+, вимагають від користувачів зазначення достовірних особистих даних, включно з фінансовою інформацією (наприклад, даними платіжних карток), що підвищує чутливість до кіберзлочинів. Попри те, алгоритми формують стрічки новин і рекомендацій, оптимізовані для максимального залучення користувача, часто стимулюючи емоційні реакції, зокрема негативні, що підвищує ймовірність поширення контенту та тривалість перебування на платформі [50].

Соціальні мережі є зручним інструментом для поширення дезінформації, оскільки дозволяють швидко охоплювати великі аудиторії без попередньої перевірки достовірності контенту. Дезінформація - це умисне поширення неправдивої або спотвореної інформації з метою введення в оману, що спрямоване на підрив незалежності держави, конституційного ладу, суверенітету й територіальної цілісності, а також на розпалювання насильства, ворожнечі та дестабілізацію суспільства.

Поширення неправдивих відомостей може мати різні цілі – від створення панічних настроїв у суспільстві та зниження довіри до державних інституцій до спроб впливу на політичні процеси, маніпулювання громадською думкою та провокування соціальної напруженості.

Особливу загрозу становлять координовані інформаційні операції, які організовуються іноземними державами або недержавними акторами з метою цілеспрямованого впливу на внутрішньополітичні процеси. Досвід України, а також інших держав, засвідчує, що подібні операції здатні мати довгострокові наслідки для національної безпеки: вони підривають довіру до органів влади, радикалізують суспільні настрої й створюють сприятливі умови для зовнішнього втручання у внутрішні справи держави [60, с.35].

Інформаційна безпека в соціальних мережах охоплює технічні, соціальні, психологічні та правові виміри. Вона передбачає захист персональних даних, протидію дезінформації й пропаганді, запобігання використанню соціальних мереж для координації протиправних дій та підвищення стійкості суспільства до інформаційно-психологічних впливів. Держави-агресори використовують соціальні платформи як складову інформаційних операцій, що робить необхідним системний підхід до моніторингу й протидії таким загрозам. Усе це робить проблему формування ефективної системи інформаційної безпеки не лише актуальним, а й стратегічно важливим завданням для держави, адже соціальні платформи можуть бути інструментом гібридної війни та чинником дестабілізації.

Зокрема, російські спецслужби заздалегідь готувалися до використання соціальних мереж у гібридних конфліктах. Ще у 2012 р. російський пропагандистський канал RT повідомляв про виділення Службою зовнішньої розвідки рф приблизно $1 млн на створення трьох спеціалізованих систем моніторингу та впливу на соціальні мережі. Система «Диспут» призначалася для відстеження поширення інформації у блогосфері, зокрема для ідентифікації популярних авторів і дописів. Система «Монітор-3» мала на меті збір даних для OSINT-розвідки, а «Шторм-12» - активне поширення контенту та формування вигідних для росії наративів, впливаючи на суспільні настрої [382].

Соціальні мережі забезпечують можливість миттєвого поширення текстового, фото- та відеоконтенту в режимі реального часу, що створює умови для оперативного моніторингу подій та своєчасного виявлення дезінформаційних кампаній [286].

Однією з ключових небезпек соціальних мереж є надзвичайно швидке поширення будь-якої інформації, незалежно від її достовірності. Особливо вразливими є публічні особи, проте негативний ефект може торкнутися будь-кого. Серед додаткових загроз соціальних мереж слід виділити інфільтрацію контактних мереж зловмисниками через створення фейкових акаунтів або компрометацію реальних профілів. Це дозволяє накопичувати приватну

інформацію, включно з геолокацією, сімейними зв’язками та робочими контактами, і використовувати її для фішингу, шантажу або доступу до захищених ресурсів. Протидія таким діям передбачає верифікацію нових контактів, підвищення медіаграмотності користувачів, застосування двофакторної автентифікації та моніторинг підозрілої активності.

Алгоритми платформ часто сприяють поширенню сенсаційного та емоційно забарвленого контенту, що підвищує ризики масштабного розповсюдження фейків і пропагандистських повідомлень.

Умови інформаційного перевантаження та миттєвої комунікації ускладнюють своєчасне реагування на фейки: навіть якщо медіа або офіційне джерело встигає спростувати неправдиве повідомлення, воно вже охоплює значну аудиторію й продовжує поширюватися користувачами. Поширення спростувань зазвичай охоплює лише невелику частину аудиторії, а негативний емоційний ефект фейку може зберігатися, формуючи упереджене ставлення до об’єкта атаки. Це створює сприятливі умови для маніпуляцій, коли фейки використовуються для дискредитації опонентів або конкурентів, а швидкість поширення інформації робить їхні наслідки практично незворотними .

Аналітики зазначають, що прямий доступ російських спецслужб до баз даних соціальних сервісів дозволяє отримувати широкий спектр інформації, що завантажується користувачами, включно з особистими та службовими даними, що становить значну загрозу безпеці громадян і військових.

Додаткову загрозу становить використання бот-мереж і фейкових акаунтів, які штучно підсилюють певні наративи, створюючи ілюзію масової підтримки або обурення.

Важливим викликом для інформаційної безпеки в соціальних мережах є феномен так званих «інформаційних бульбашок» та посилення поляризації суспільства [228]. Алгоритми персоналізації контенту, що використовуються соціальними платформами, підбирають інформацію відповідно до попередніх уподобань і поведінки користувачів. У результаті формується замкнений інформаційний простір, у якому люди здебільшого стикаються лише з тими

поглядами, які збігаються з їхніми власними. Така ситуація сприяє поширенню екстремістських ідей, теорій змови та радикалізації окремих груп населення [374], що створює додаткові ризики для стабільності суспільства.

З огляду на це, держава має розробляти й реалізовувати комплексні стратегії забезпечення інформаційної безпеки в соціальних мережах. Такі стратегії повинні поєднувати технічні засоби (моніторинг, алгоритмічні рішення, кіберзахист) із нетехнічними заходами, серед яких особливе місце посідає розвиток медіаграмотності, критичного мислення та громадянської відповідальності. Лише системний і міждисциплінарний підхід дозволить підвищити стійкість суспільства до маніпуляцій і знизити ризики деструктивного впливу цифрового середовища.

Починаючи щонайменше з 2013 р., в російській федерації функціонувала організація, відома як «тролі з Ольгіна», яка спеціалізувалася на впливі на суспільну думку через соціальні мережі та інтернет-форуми. У 2014 р. ця структура стала активним інструментом формування громадської думки на Заході, поширюючи меседжі, вигідні кремлівському режиму [182].

російські провладні медіа та координовані групи користувачів у соціальних мережах проявили надзвичайну активність напередодні анексії Криму. Ці ресурси активно поширювали неперевірені й неправдиві матеріали, здійснювали аналітичне коментування подій, формуючи вигідний для рф інформаційний порядок денний. Значна частина контенту створювалась редакціями пропагандистських видань або поширювалась через «дружніх» інтернет-активістів. У Facebook з’являлися групи, що свідомо поширювали панічні настрої та пропаганду про «непереможність російської армії», що мало на меті деморалізувати українське суспільство. Важливо, що ці матеріали нерідко ретранслювались онлайн-ЗМІ, а подекуди - й традиційними мас-медіа [342].

У 2014 р. росія розгорнула проти України стратегію гібридної війни, яка є структурно-функціонально унікальною: вона поєднує гібридну форму дій із асиметричним змістом [57, с. 3]. Ця стратегія виявилася особливо помітною під

час анексії Криму та м. Севастополя, а також окупації частини території України терористичними організаціями «ДНР» і «ЛНР». Під час та після анексії Криму російські спецслужби неодноразово здійснювали масові блокування користувачів соціальних мереж з вираженою проукраїнською позицією. Для цього використовувались мережі ботів, які масово надсилали скарги на акаунти до модераторів платформ, маніпулюючи автоматизованими системами модерації та обмежуючи видимість критичного контенту.

У 2014–2015 рр. у всесвітній мережі діяли численні інформаційні ресурси, координацією яких займалися фахівці з інформаційних війн і спецслужб рф. Через популярні російські соціальні мережі, такі як «Вконтакте» та «Одноклассники» (діяли численні групи, зокрема «Антимайдан», «Республіка Новоросія», «Антимайдан Донбас», які поширювали проросійські та антиукраїнські нарати), а також сайти проросійських сепаратистських угруповань поширювалися сепаратистські ідеї, заклики до терористичної діяльності та консолідувалися радикально налаштовані особи. Ефективність таких впливів оцінювали за активністю користувачів («лайки», «репости», «класси») [30, с. 89–91].

Паралельно діяли сайти на кшталт «Руська весна», «КіберБеркут» та портали так званих «ЛНР» і «ДНР», що поширювали проросійську пропаганду й координували мобілізацію прихильників сепаратизму [60; 61].

Залучення платних тролів, ботнетів та створення сайтів із викривленими новинами стало системною практикою російської пропаганди. Дослідження демонструють, що ефективність інформаційного впливу зростає зі збільшенням кількості джерел, підтримки серед членів спільноти та повторюваності повідомлень [377].

Приклад координації діяльності російських інтернет-пропагандистів був виявлений завдяки операціям українських хакерських спільнот FalconsFlame, Trinity, Рух8 та КиберХунта [103].

Навіть у 2016 р., через два роки після початку Війни за Незалежність України, було виявлено широку мережу ботів, які поширювали заклики до

насильницьких дій проти української влади та провокували ідею «Третього Майдану» (Додаток Б) [258].

Служба безпеки України неодноразово фіксувала та припиняла діяльність адміністраторів груп у соціальних мережах, які займалися антиукраїнською пропагандою. Так, на початку серпня 2016 р. був затриманий мешканець Кам'янського, який, за домовленістю з кураторами з росії та тимчасово окупованих територій, створював групи для дискредитації сил антитерористичної операції та поширення закликів до зміни конституційного ладу в Україні, включно з пропагандою створення вигаданої «Дніпропетровської народної республіки» і її інтеграції до рф. Раніше, у липні того ж року, був затриманий мешканець Сєвєродонецька, завербований через соціальні мережі та залучений до кампанії інформаційного впливу проти України [251].

Соціальні мережі стали важливим джерелом інформації для OSINT-розвідки та відкрили нові можливості для відстеження пересування окремих військових і аналізу конфліктних зон. Завдяки використанню методів соціальної інженерії, зокрема збору та аналізу відкритих даних користувачів, вдалося ідентифікувати та контролювати окремі облікові записи, що дозволило викрити мережі шпигунів і бойовиків як на території України, так і за її межами.

Паралельно, на території російської федерації у 2016 р. набули чинності так звані «закони Ярової», що передбачають обов'язкову передачу Федеральній службі безпеки рф практично всіх особистих даних користувачів інтернет-ресурсів, зареєстрованих у рф, включно з логінами, електронними адресами, списками контактів та метаданими переданих повідомлень [267]. У зв'язку з цим Служба безпеки України рекомендувала українським користувачам уникати застосування російських інтернет-ресурсів, передусім соціальних мереж і поштових сервісів (Додаток В).

В цей час формувалися волонтерські та громадські ініціативи, такі як Інформнапалм, Bellingcat та інші, які за допомогою OSINT-даних із соцмереж

виявляли маніпуляції російської пропаганди та проводили розслідування, зокрема щодо збиття літака Boeing 777 рейсу MH17 біля Донецька.

Для протидії можливому втручанню в інформаційний простір України, Президент України Петро Порошенко наказом ввів у дію рішення РНБО від 28 квітня 2017 р. щодо застосування персональних та економічних санкцій, що передбачало блокування низки російських інформаційних ресурсів і соціальних мереж, серед яких «Вконтакте» та «Одноклассники» [220].

У цифровому середовищі дедалі частіше застосовується явище астротурфінгу - технологія штучного формування громадської думки або імітації суспільної підтримки через масове коментування й поширення контенту у соціальних медіа, що має безпосередній вплив на політичні процеси, зокрема на результати виборів, громадські кампанії та формування політичного порядку денного; імітація масової громадської ініціативи для створення ілюзії запиту від суспільства [339].

Астротурфінг передбачає залучення спеціально найнятих осіб, які на форумах, у блогах та соціальних мережах розміщують замовні пости й коментарі з метою створення ілюзії спонтанної масової підтримки або засудження певних явищ, продуктів, послуг, подій чи точок зору. На практиці астротурфінг проявляється через проплачені мітинги, підтасовані соціологічні дослідження, організацію масовки та створення ілюзії широкої підтримки певних ідей або організацій. У росії цей метод активно використовувався з 2014 р. під час псевдореферендумів і виборів на тимчасово окупованих територіях, коли маріонеткові ЗМІ поширювали неправдиву інформацію про «масову підтримку» рішень Кремля.

В умовах цифрового середовища астротурфінг застосовується переважно у соціальних мережах. Наприклад, дослідження BBC та Інституту стратегічного діалогу (2022 р.) показали створення численних «пропутінських» груп у Facebook, де активність часто забезпечують боти та користувачі з кількома акаунтами. Подібні штучні коментарі створюють ілюзію масової підтримки та витісняють реальні оцінки громадян. В Україні прикладом є поширення

фейкових тверджень про продаж електроенергії під час відключень, де коментарі ботів створюють відчуття широкого підтвердження неправди [201].

Для ефективного протидіяння інформаційним операціям рф у соціальних мережах доцільно застосовувати комплексний підхід. Ключовими заходами є постійний моніторинг і аналіз використання соціальних платформ рф НАТО та союзниками, залучення фахівців із глибоким знанням російської мови та культури для виявлення ключових повідомлень і координаційних структур. Важливе значення має забезпечення інформаційного плюралізму та підтримка незалежних журналістів, експертів і неурядових організацій, а також розвиток освітніх програм із медіаграмотності та кампаній із підвищення обізнаності щодо пропаганди й маніпуляцій [129; 26]. Практичні заходи включають виявлення та нейтралізацію діяльності інтернет-тролів, фактологічне спростування неправдивої інформації, активне відстеження мови ворожнечі та її блокування адміністраторами платформ відповідно до чинного законодавства. Комплексне застосування цих рекомендацій сприяє підвищенню стійкості суспільства до інформаційних атак і мінімізації ризиків дезінформації [385]. Все це особливо важливо, зважаючи на досить велику кількість користувачів соціальними мережами в Україні.

За результатами соціологічного опитування, проведеного в Україні у 2022 р., 76,6 % громадян активно користувалися соціальними мережами. Серед тих, хто обирав соціальні медіа як джерело інформації, найбільш популярним виявився месенджер Telegram (66 %), далі - YouTube (61 %) та Facebook (58 %). Варто зазначити, що респонденти могли обирати декілька варіантів відповідей одночасно. У сегменті розважального контенту лідером є YouTube, який налічує понад 28 мільйонів українських користувачів. Значна аудиторія також представлена в Instagram (понад 16,1 млн), Facebook (15,45 млн) та TikTok (понад 10,55 млн) [298].

На початок 2023 р. в Україні налічувалося 28,57 мільйона користувачів Інтернету, що відповідало рівню проникнення на рівні 79,2% населення. У січні 2023 р. кількість користувачів соціальних мереж становила 26,70 мільйона, або

74,0% від загальної кількості населення. Водночас слід зауважити, що окремі користувачі можуть мати кілька акаунтів, тому кількість акаунтів не завжди відповідає кількості унікальних осіб. Загалом, 93,5% інтернет-користувачів в Україні у січні 2023 р. використовували принаймні одну платформу соціальних мереж, що підкреслює їхню значущість для комунікацій, інформаційного обміну та соціальної взаємодії у цифровому середовищі [282 , с.23-24].

Високий рівень залученості українців до соціальних мереж зумовлює потребу дослідження не лише комунікаційних можливостей цих платформ, але й пов'язаних із ними ризиків. Науковці наголошують, що соціальні мережі у сучасних умовах виступають не лише каналами обміну інформацією, а й інструментами формування суспільних настроїв. Як підкреслює Д. Арабаджиєв, вони перетворилися на важливий засіб впливу на масову свідомість, особливо в умовах гібридної та інформаційної війни [7, с.13].

Висока швидкість циркуляції повідомлень, можливість анонімного створення та поширення контенту, а також алгоритмічні механізми, що підсилюють вірусність емоційно навантажених матеріалів, створюють сприятливий ґрунт для реалізації масштабних кампаній дезінформації та психологічного впливу. Це, своєю чергою, актуалізує необхідність критичного мислення й інформаційної грамотності як засобів протидії таким загрозам.

З початком повномасштабної війни соціальні мережі стали головним джерелом новин для більшості українців (77,9% за даними ОПОРИ), але водночас – майданчиком для поширення російської дезінформації та полем битви за інформацію. Це створює численні виклики для користувачів і медіа, які стикаються з блокуваннями, видаленням контенту, заниженням охоплень і складністю комунікації з платформами. Щоб обговорити ці проблеми та шляхи їх вирішення, Центр демократії та верховенства права (ЦЕДЕМ) 25 січня 2024 року провів експертну дискусію «Соціальні мережі під час війни», де представники медіа, НУО та Meta окреслили ключові проблеми модерації, зокрема надмірні бани за мову ворожнечі, складність оскарження блокувань, фішингові атаки й помилки алгоритмів, які зачіпають регіональні медіа.

Учасники наголосили на важливості діалогу з соцмережами, розвитку медіаграмотності користувачів та адаптації правил модерації до українських воєнних реалій. ЦЕДЕМ представив рекомендації для Meta, зокрема враховувати контекст української війни, створювати «білі списки» медіа та проводити регулярні консультації з довіреними партнерами, щоб мінімізувати негативний вплив модерації на інформування суспільства [284]. Головний медійний юрист ЦЕДЕМ Ігор Розкладай повідомив, що торік організація подала понад 800 апеляцій на видалення дописів, більшість з яких стосувалися дезінформації та зловмисної активності, значна частина якої мала «російський слід». Основними темами дезінформаційних кампаній були корупція, мобілізація та соціальні конфлікти, а також поширення фішингу й шахрайства через зламані акаунти. Розкладай відзначив покращення швидкості реагування платформ на скарги, але наголосив на необхідності подальшого захисту свободи слова, медіа [284].

Соціальні медіа, стали ключовим інструментом оперативного інформування, підтримки взаємодії з громадою та управління репутаційними ризиками [21, с. 29-32]. Однак їх амбівалентність створює додаткові загрози: помилки в тоні чи змісті публікацій можуть спричинити масштабні інформаційні кризи. Правильне використання соціальних мереж передбачає швидку адаптацію контенту, проактивне реагування на занепокоєння аудиторії, регулярні оновлення та централізовані відповіді. Прикладами успішної практики стали численні міжнародні кампанії підтримки України, благодійні ініціативи та трансформація бізнес-моделей на користь суспільних потреб, зокрема створення платформи Second Chance Bank. Соціальні мережі не лише прискорюють обмін інформацією, а й стають дієвим каналом нівелювання кризових ситуацій, забезпечуючи діалог, формування довіри та підтримку стосунків між компаніями та суспільством [334].

Аналіз соціальних мереж надає можливість як сприяти поширенню певних ідей та наративів, так і протидіяти їм. Дослідження дописів у соціальних мережах у поєднанні з метаданими дозволяє ідентифікувати лідерів громадської

думки та ключові комунікаційні вузли, через які поширюється інформація. Сучасні алгоритми обробки та класифікації зображень дають змогу визначати, які візуальні матеріали є найбільш популярними серед користувачів, а прив'язка даних до геолокації відкриває можливість відстеження змін у настроях і вподобаннях населення на певних територіях.

Комплексні технології впливу в соціальних мережах постійно уніфікуються, і їх можна використовувати як конструктивно, для розвитку демократичного діалогу, так і деструктивно, з метою маніпуляцій або дезінформації. Розпізнати характер таких технологій можна шляхом аналізу комунікацій та оцінки намірів: чи є ознаки хибного або руйнівного наміру, яка мета комунікації та які стратегічні наративи застосовано, а також чи здатна конкретна техніка завдати шкоди громадськості. До основних технологій інформаційного впливу належать соціально-когнітивний хакінг, що експлуатує соціальні відносини та психологічні вразливості користувачів, прихована реклама, орієнтована на психографічні профілі, ефект приєднання до більшості та спіраль мовчання, коли боти та фейкові акаунти підсилюють соціальне визнання або пригнічують висловлювання користувачів, а також луна-камери і інформаційні бульбашки, які обмежують контакт із протилежними ідеями. Серед інших технологій – фальшиві та підставні особи, самозванці та шахраї, що імітують офіційні джерела, підробки документів, «потьомкінські поселення» та фейкові медіа для створення видимості достовірності дезінформації. Автоматизовані інструменти, такі як боти та сокпапети, а також діпфейк і фішинг, застосовуються для масового поширення контенту, маніпуляцій або отримання конфіденційної інформації. Дезінформація та маніпуляція контентом включають фальсифікацію, зміну або неправомірне привласнення матеріалів, а сатира й пародія можуть використовуватися для легітимізації хибних точок зору. Символічні дії та публічні демонстрації використовуються для передачі меседжів і створення помилкового враження підтримки, а витік та злам інформації можуть слугувати інструментом впливу на суспільну думку [290, с.250-258].

Отже, соціальні мережі стали важливим інструментом стратегічного впливу в сучасних гібридних війнах. Вони дозволяють оперативно поширювати інформацію, формувати громадську думку, мобілізувати соціальні групи та впливати на політичні процеси всередині держави і на міжнародній арені. Соціальні мережі активно використовуються як для поширення дезінформації та пропаганди, так і для координації громадських ініціатив та протидії зовнішньому інформаційному впливу. Ефективність їх використання залежить від здатності швидко адаптувати інформаційні кампанії, використовувати різні медіа та оперативно реагувати на загрози. Соціальні мережі виступають не лише каналом комунікації, а й інструментом стратегічного впливу, який може як посилювати зовнішній тиск на державу, так і забезпечувати її інформаційну безпеку.

2.2. Інформаційно-психологічні операції в соціальних мережах: безпековий вимір для держави

Інформаційне суспільство виступає ключовим середовищем формування та еволюції нових форм конфліктності, зокрема - інформаційних конфліктів та інформаційних війн. Саме з появою інформаційного суспільства як якісно нового етапу розвитку соціуму, в межах якого інформація стає домінуючим ресурсом, відбувається трансформація природи агресії та способів її реалізації. На відміну від індустріального суспільства, яке було орієнтоване переважно на матеріальне виробництво і традиційні форми силового протистояння, постіндустріальний період характеризується зміною форм соціального напруження - від фізичного до інформаційного впливу. Таким чином, інформаційні конфлікти та інформаційні війни постають не лише як нова форма боротьби за вплив, але і як результат структурних змін у суспільстві, що демонструють залежність між рівнем його розвитку та характером конфліктогенних процесів.

У сучасних умовах трансформації суспільства в напрямку інформаційного типу, що супроводжується інтенсивними процесами глобалізації, поширенням масової культури, зростанням ролі комунікативних технологій та демократизацією соціально-політичного життя, інформаційна війна набуває особливої актуальності як комплексне соціально-політичне явище. Збільшення доступу різних соціальних груп до інформаційних ресурсів та активізація їх участі в суспільному житті зумовлюють не лише переосмислення ролі інформації як стратегічного ресурсу, але й загострення конкурентної боротьби у сфері інформаційного впливу. Інформаційна війна виступає не лише інструментом маніпуляції свідомістю, а й потужним засобом досягнення геополітичних цілей [151, с.176].

Інформаційна війна є багатокомпонентним явищем, яке охоплює різні аспекти і концептуальні підходи до її розуміння. Зокрема, її можна визначати як взаємодію між інформаційними системами або суб'єктами, спрямовану на досягнення певних матеріальних або стратегічних вигод. У більш широкому сенсі - інформаційна війна проявляється як протистояння між державами або іншими акторами в інформаційному просторі, що має на меті нанесення шкоди інформаційним системам, критично важливим ресурсам та інфраструктурі противника.

Інформаційно-психологічні війни нерідко розглядають як форму так званих «воєн культур» [352, pp. 121–132], суть яких полягає у навмисному впливі на культурну ідентичність населення з метою її трансформації або руйнування. Такий вплив, зазвичай, має на меті послаблення фундаментальних основ соціального життя, моральних орієнтирів і ціннісних систем. У результаті агресор отримує можливість здійснювати геополітичний тиск без застосування сили, використовуючи інструменти деморалізації. «Війни культур» у межах інформаційно-психологічного впливу спрямовані на глибоку зміну ідентичнісних і структурних засад суспільства, що створює умови для довготривалої дестабілізації без відкритого збройного протистояння.

Інформаційна війна є складовою гібридної війни і поєднує у собі як технологічні, так і психологічні аспекти впливу. Основними характеристиками інформаційної війни є:

1. **Безконтактний характер**. Інформаційна війна зазвичай ведеться без прямого фізичного зіткнення між сторонами конфлікту. Її основним знаряддям є інформація, що поширюється через засоби масової інформації, соціальні мережі, електронні платформи тощо.

2. **Масовий вплив на свідомість**. Однією з головних цілей є вплив на масову свідомість, громадську думку, ціннісні орієнтації та поведінкові моделі як ворожого суспільства, так і власного населення [2, с.27].

3. **Спрямованість на інформаційні та комунікаційні системи**. Інформаційна війна охоплює також технічні аспекти - зокрема, спроби дестабілізувати або зруйнувати інформаційно-комунікаційні структури супротивника, включаючи кібернапади, втручання в роботу ЗМІ, підробку цифрових джерел тощо.

4. **Використання фейків, пропаганди та дезінформації**. Центральним інструментом є поширення неправдивої або викривленої інформації з метою дискредитації, деморалізації, провокації або посилення соціальної напруги. Поширення фейкових новин полягає у навмисному створенні або викривленні інформації з метою введення аудиторії в оману щодо подій, осіб чи явищ. Для підвищення переконливості та ускладнення викриття таких повідомлень використовуються прийоми імітації офіційних джерел, емоційно забарвлена мова, а також фото- й відеоматеріали [109; 15].

5. Довготривалий і прихований вплив. Інформаційна війна часто розгортається поступово, без явного оголошення. Її наслідки можуть проявлятися через тривалий час, а самі дії можуть залишатися непоміченими для більшості учасників інформаційного простору.

6. **Гнучкість і адаптивність**. Інформаційна війна не має усталених меж - вона швидко змінює форму та засоби відповідно до ситуації. Її стратегії постійно оновлюються завдяки досягненням у сфері інформаційних технологій.

7. **Політична, економічна та ідеологічна складова**. Інформаційна війна не обмежується лише військовою сферою. Вона активно використовується у політичних кампаніях, економічному суперництві, міжнародних відносинах та ідеологічній боротьбі.

Відповідно, до узагальнених поглядів, дослідники виділяють дві особливості/риси інформаційної війни.

Першою ключовою особливістю інформаційної війни є те, що вона не ведеться на конкретній географічній території, як традиційні збройні конфлікти. Натомість її поле дії – це інформаційний простір, який формується та існує завдяки людському розуму, комунікації та взаємодії суспільства. Тут основною ареною боротьби стає свідомість людей, їхнє сприйняття, знання та уявлення про реальність, що робить інформаційну війну значно більш гнучкою та масштабною [2, с.28].

Другою визначальною рисою є те, що найпотужнішою зброєю в цьому типі війни виступає сама інформація. Вона може бути використана для впливу на поведінку, переконання та емоції людей, формування суспільних настроїв, підриву довіри до інститутів та маніпулювання масовою свідомістю. У цьому контексті домінування в інформаційному просторі стає ключовим фактором стратегічної переваги, оскільки контроль над потоками інформації та здатність визначати, що вважається правдою або фейком, визначає хід конфлікту. Таким чином, інформаційна війна характеризується не лише активним використанням даних, повідомлень та медіа, а й постійною боротьбою за панування в сфері знання, уявлень і громадської свідомості [111, с.56].

Еволюція інформаційних війн демонструє поступовий перехід від прямого технічного втручання до комплексного психологічного впливу, який поєднує технологічні та когнітивні інструменти з метою ослаблення стійкості суспільства та держави.

У процесі розвитку інформаційної війни дослідники виділяють два основні покоління методів впливу, що відображають рівень технологічного та стратегічного розвитку. Першому поколінню властиві технічні операції,

спрямовані на втручання в інформаційну інфраструктуру супротивника, включно з несанкціонованим доступом до даних, їхньою підміною чи фальсифікацією, перехопленням потоків інформації та поширенням дезінформації через канали противника чи цифрові платформи. Такі дії мали на меті вплив на управлінські рішення та функціонування державних і корпоративних структур. Друге покоління інформаційних війн фокусує увагу на психологічному та когнітивному впливі. Його ціль - маніпулювання масовою свідомістю, створення соціальної напруги та політичної нестабільності. До методів цього покоління належать дискредитація державних інституцій та культурних цінностей, провокування конфліктів між політичними суб'єктами, формування фейкових наративів і помилкових управлінських рішень. На міжнародній арені ці операції підривають авторитет держави та послаблюють партнерські відносини [180, с. 56].

Засоби ведення інформаційної війни умовно поділяються на дві основні групи, кожна з яких відображає специфіку стратегічних підходів до інформаційного протистояння. Перша група засобів зумовлена консцієнтальним (свідомісним) характером інформаційної війни та спрямована на вплив на когнітивні й соціальні процеси. Її метою є формування або трансформація громадської думки, маніпулювання механізмами ухвалення політичних та управлінських рішень, а також цілеспрямований вплив на свідомість військовослужбовців і цивільного населення з метою їх «перепрограмування» відповідно до бажаних інформаційних моделей. Друга група засобів пов'язана з технічним аспектом і орієнтована на виведення з ладу або зниження ефективності інформаційних та інформаційно-керуючих систем противника. Йдеться, зокрема, про деструктивний вплив на комунікаційні мережі, цифрову інфраструктуру, системи управління військами чи об'єктами критичної інфраструктури [180, с. 49].

Інформаційні війни здатні завдавати масштабної шкоди як на рівні окремих соціальних груп, так і на рівні державних інституцій, при цьому

використовуючи не фізичну силу, а маніпулятивний вплив на свідомість, емоції та поведінку людей.

Маніпуляція виступає ефективним засобом впливу на формування суспільної свідомості та процеси самоусвідомлення особистості в соціумі. Вона реалізується через відбір, упорядкування та подання інформації у певному ракурсі, створення емоційно забарвлених повідомлень, використання стереотипів, символів і наративів, а також через повторювані меседжі, які формують уявлення про соціальні, політичні та культурні реалії.

Такий вплив здатен направляти громадську думку, підсилювати або знижувати довіру до інституцій та окремих соціальних груп, а також моделювати поведінкові реакції індивідів у суспільстві [94, с.36]. У низці випадків результати подібного впливу можуть мати довготривалий і навіть руйнівний характер - аж до дестабілізації політичної системи, підриву національної безпеки та порушення цілісності суспільного порядку [156, с.160].

Інформаційна війна є універсальним інструментом впливу, що охоплює всі ключові сфери суспільного буття - політичну, економічну, соціальну, військову та духовно-культурну. Її універсальність полягає, з одного боку, у здатності проникати в будь-яку підсистему суспільства, завдаючи шкоди або, навпаки, формуючи вигідні інформаційні образи та наративи. З іншого боку, інформаційна війна є самодостатнім засобом досягнення стратегічних цілей: вона може ефективно функціонувати як незалежно від традиційних форм збройного протистояння, так і в поєднанні з ними, посилюючи загальний вплив на противника. Така гнучкість і багатовекторність роблять інформаційну війну однією з найнебезпечніших форм сучасної гібридної агресії [180, с.48.].

Інформаційні операції росії в контексті її війни проти України є наочним прикладом застосування принципів гібридної війни. росія системно використовує інформаційні кампанії для впливу на громадську думку як на території України, так і за її межами. Це включає поширення дезінформації, створення та підтримку фейкових наративів, маніпуляцію емоційними й когнітивними механізмами сприйняття населення, а також використання

соціальних мереж і медіа для формування вигідного для себе інформаційного поля [135].

Інформаційні війни реалізуються через впровадження дискурсивних практик, мовну інтервенцію, витіснення або дискримінацію культурних спільнот, що особливо проявляється у контексті кримськотатарського населення в окупованому Криму. До ключових проявів таких процесів належать: трансформація соціальної структури та правил мобільності, зміна системи цінностей і традицій, руйнування політичних інституцій та формування нових владних структур, переорієнтація зовнішньої політики, перебудова правової та економічної систем.

Інформаційна війна передбачає цілеспрямований вплив на всю комунікаційну систему з метою створення сприятливого інформаційного середовища на глобальному рівні та встановлення максимального контролю над інформаційними потоками в комунікативному просторі. Паралельно з цим активно застосовуються кібернетичні технології, що передбачають атакування інформаційних систем, злам серверів, поширення шкідливого програмного забезпечення, паралізацію урядових і фінансових структур.

Не менш важливим інструментом є психографічний аналіз великих даних (Big Data), що дозволяє створювати індивідуалізовані моделі впливу на різні групи населення, враховуючи їхні соціально-демографічні характеристики, уподобання та емоційний стан [340].

Інформаційна війна також включає в себе соціотехнологічні методи, які спрямовані на організацію штучних інформаційних приводів - так званих «інфовкидів» - з метою створення резонансу, ескалації конфліктів або дискредитації політичних опонентів. Часто ці технології поєднуються з реальними бойовими діями, створюючи ефект гібридного впливу, коли військові, політичні та інформаційні інструменти взаємодіють як єдина система.

Значну роль відіграють і медійні технології, передусім через соціальні мережі та цифрові платформи, де за допомогою спеціально створених акаунтів, ботів, тролів і алгоритмічного просування контенту відбувається нав'язування

потрібних смислів. Особливо небезпечною є можливість масового і швидкого поширення фейкової інформації, яка часто має високий емоційний заряд і покликана викликати страх, паніку або агресію. Організована діяльність тролів відзначається високим рівнем координації та професійної структури. Їхня робота проходить у три етапи: «підведення до теми», «підсікання» та «залучення», що демонструє явище так званого «озброєння» медіа [297, с.374; 280].

Ефективність та охоплення інформаційної війни підсилюють. інформаційно-психологічні операції (далі - ІПсО) - комплекс цілеспрямованих дій інформаційного характеру, спрямованих на вплив на свідомість, емоції, поведінку та психологічний стан цільової аудиторії з метою досягнення політичних, військових, соціальних або економічних цілей. Такі операції здійснюються шляхом поширення спеціально підібраної інформації або дезінформації, маніпулятивного контенту, а також через використання засобів масової інформації, соціальних мереж, цифрових платформ та інших каналів комунікації.

Інформаційно-психологічні операції використовуються як інструмент цілеспрямованого дестабілізаційного впливу, за допомогою якого посилюється соціально-економічна нестабільність усередині держави-противника, а також зростає психологічний і інформаційний тиск на населення та вище політичне керівництво країни - об’єкта агресії. Оскільки безпосереднім об’єктом такого впливу є свідомість людини, механізми інформаційно-психологічних операцій вибудовуються з урахуванням її когнітивних і психологічних особливостей [117].

В науковій та прикладній літературі інформаційно-психологічна операція визначається як сукупність узгоджених, цілеспрямованих і взаємопов’язаних за змістом, цілями, об’єктами впливу та часом інформаційних заходів, які реалізуються одночасно або послідовно згідно із заздалегідь розробленим планом і загальним задумом. Основною метою таких операцій є досягнення визначених результатів інформаційно-психологічного впливу на цільову

аудиторію, зокрема на військовослужбовців, цивільне населення, політичне керівництво, а також іноземну громадську думку [214, с.35].

Успішна реалізація ІПсО забезпечує досягнення стратегічних результатів - деморалізацію супротивника, зниження стійкості суспільства до зовнішнього впливу, зміщення суспільних пріоритетів тощо. Це дозволяє атакуючій стороні досягати політичних або воєнних цілей без фізичного протистояння, через контроль за інформаційним і психологічним простором.

Найбагатший досвід проведення інформаційно-психологічних операцій належить США, які застосовували їх у війнах у Кореї, В'єтнамі, Іраку, Афганістані. Під час Корейської війни (1950-1953 рр.) американці вперше реалізували стратегічні інформаційно-психологічні операції, створивши спеціалізовані підрозділи для розповсюдження листівок, радіо- та усної пропаганди з метою впливу на моральний стан ворога й легітимації своїх дій. У В'єтнамі США створили масштабну систему батальйонів психологічної війни, які взаємодіяли з артилерією та авіацією, розповсюдивши понад 50 млрд листівок і охопивши 95% населення радіомовленням [329, с.128].

Військова кампанія "Буря в пустелі" (1991 р.) стала одним із перших конфліктів, де інформаційно-психологічна компонента застосовувалася в широкому масштабі, інтегровано та з урахуванням сучасних технологій. За оцінками низки дослідників та військових аналітиків, саме ефективне використання ІПсО значною мірою сприяло швидкому досягненню стратегічних цілей коаліційних сил, а також деморалізації збройних сил Іраку, що істотно зменшило масштаби збройного спротиву [4]. Для забезпечення підтримки місцевого населення у виконанні завдань в Іраці, що стояли перед американськими військовими, було інвестовано значні ресурси у виробництво та розповсюдження політичних матеріалів, новинних випусків, розважального контенту й соціальної реклами. Такий комплекс заходів мав на меті формування сприятливого інформаційного поля, яке сприяло б легітимізації дій США та зміцненню їхнього впливу у регіоні [156, с.158].

У воєнних доктринах низки провідних країн світу, таких як США, Велика Британія, Китайська Народна Республіка, та деякі країни НАТО, ІПсО визнаються як інтегрований компонент сучасних операцій Збройних сил. З одного боку, вони розглядаються як необхідна складова підготовки та забезпечення ефективного проведення бойових дій, а з іншого - як самостійний тип бойового протиборства, здатний досягати стратегічних цілей без застосування фізичної сили [110; 321, с. 184-186; 77].

Інформаційно-психологічні операції у межах гібридної війни в соціальних мережах реалізуються через різноманітні методи та інструменти, які поєднують традиційні прийоми інформаційного впливу з новітніми цифровими технологіями. Серед найбільш поширених механізмів таких операцій слід виокремити наступні:

1. Поширення дезінформації та фейкових новин. Створення і масове розповсюдження неправдивої або маніпулятивної інформації є одним з основних методів впливу на аудиторію. Такі повідомлення часто апелюють до емоцій, викликаючи страх, гнів або зневіру, що суттєво знижує рівень критичного мислення та сприяє неконтрольованому поширенню неправди серед користувачів.

2. Використання бот-мереж і тролів. Автоматизовані акаунти (боти) та контрольовані оператори (тролі) використовуються для масштабного розповсюдження заданих наративів, нав’язування певних політичних чи ідеологічних позицій, імітації громадської підтримки або невдоволення. Їхня діяльність може формувати хибне уявлення про «суспільний консенсус» щодо певних подій чи осіб.

3. Маскування під джерела довіри. Значна частина інформаційно-психологічного впливу здійснюється через фейкові акаунти, які імітують реальні медіа, відомих осіб або активістів [113, с.55]. Така тактика дозволяє зменшити бар’єри сприйняття інформації, підвищуючи довіру до маніпулятивного контенту.

4. Психологічний тиск та маніпуляція емоціями. Контент часто орієнтований на емоційне перевантаження користувача - шляхом демонстрації шокуючих зображень, відео, трагічних історій або катастрофічних сценаріїв. Такі методи пригнічують раціональне мислення і стимулюють рефлекторну, емоційну реакцію.

5. Мікротаргетинг аудиторій. Застосування аналітики великих даних (BigData) дозволяє ідентифікувати вразливі групи населення та налаштовувати інформаційні впливи з урахуванням їхніх психологічних особливостей, інтересів і поведінкових моделей. Це забезпечує високу ефективність операцій за мінімальних витрат [340].

Науковці у своїх наукових дослідженнях визначили такі основні засоби застосування інформаційно-психологічних операцій, а саме: дезінформація; лобіювання; маніпулювання; пропагандиська діяльність; управління кризами; шантаж [294, с. 13].

У сукупності ці інструменти створюють складну екосистему інформаційно-психологічного впливу, що функціонує у реальному часі та адаптується до змін у соціальному, політичному та технологічному середовищі. Такий тип впливу важко ідентифікувати звичайними методами, що створює серйозні виклики для державних структур, громадянського суспільства та користувачів соціальних платформ.

Інформаційно-психологічні операції (ІПсО) виконують роль основного тактичного засобу впливу на цільову аудиторію. Вони є конкретними реалізаційними механізмами, які забезпечують:

- формування у масовій свідомості викривленої картини реальності;
- створення або посилення соціальної напруги;
- підрив легітимності влади та зниження рівня національної згуртованості;
- формування поведінкових моделей, вигідних ініціатору впливу.

На відміну від класичних форм впливу, ІПсО використовують не лише традиційні канали передачі інформації (ЗМІ, преса, телебачення), а й сучасні цифрові платформи, соціальні мережі, а також засоби кіберпростору. У воєнній

практиці інформаційно-психологічні операції поступово трансформуються з допоміжного інструменту ведення війни в ключовий механізм досягнення політичних та стратегічних цілей у конфліктних ситуаціях різної інтенсивності. З огляду на це, можна стверджувати, що інформаційно-психологічні операції є основою інформаційної війни, забезпечуючи її змістовне наповнення та практичну реалізацію на всіх рівнях інформаційного конфлікту. Ефективність ІПсО значно зростає, оскільки забезпечується швидкий доступ до великої кількості аудиторій, можливість гнучкої адаптації повідомлень та персоніфікації впливу [77].

У межах інформаційно-психологічних операцій широко застосовуються перевірені когнітивні механізми впливу на свідомість індивіда та масову аудиторію. Зокрема, йдеться про **ефект первинності** (преференція до першої отриманої інформації, що формує рамку сприйняття), **ефект авторитету** (покликання на джерела, яким адресати приписують високий рівень довіри), **ефект повторення** (посилення переконання через багаторазове відтворення однієї й тієї самої тези) та **механізм покладання відповідальності** (перенесення провини на конкретних осіб чи групи з метою спрямування суспільного гніву або невдоволення). Ці ефекти не лише підвищують ефективність інформаційного впливу, але й сприяють закріпленню потрібних установок у масовій свідомості

Для ефективної реалізації ІПсО широко використовуються інструменти масової комунікації, включаючи традиційні засоби масової інформації (друковані видання, телебачення, радіо), цифрові платформи (соціальні мережі, блоги, інтернет-ресурси), аудіо- та відеопродукція, а також прямі та опосередковані методи комунікації з населенням [116, с.121].

Системний і стратегічний характер інформаційно-психологічні операції носять у практиці НАТО, охоплюючи всі фази військового конфлікту - від його передумов до завершення [207, с. 110-118; 5].

Згідно з науковими підходами, інформаційно-психологічна операція реалізується у кілька взаємопов’язаних етапів, кожен з яких має власне функціональне навантаження та визначену мету [213, с. 74].

Відповідно до вимог керівних документів НАТО, які регламентують планування та проведення інформаційно-психологічних операцій, інформаційно-пропагандистська діяльність під час підготовки та ведення збройного конфлікту здійснюється у чітко визначеній послідовності. Зокрема, структура проведення таких кампаній, зафіксована в офіційних керівних настановах Альянсу, включає три основні етапи: підготовчий, інформаційний та поствоєнний.

1. Підготовчий етап. На цьому етапі реалізується комплекс заходів, спрямованих на створення сприятливого інформаційного середовища для подальших військово-силових дій. Зокрема, через медіа-канали та інші засоби комунікації формуються наративи, які підвищують рівень напруги навколо певного географічного регіону або політичного режиму, який є об’єктом потенційного впливу. У публічному дискурсі активно висуваються різноманітні звинувачення (наприклад, у порушеннях прав людини, підтримці тероризму, наявності забороненої зброї тощо), а також розповсюджується інформація про можливі терміни початку військової операції, що створює атмосферу невизначеності та страху. Окремим елементом підготовки може бути згадування про ймовірність використання новітніх або нетрадиційних видів озброєнь, що посилює психологічний тиск як на політичне керівництво противника, так і на міжнародну спільноту [207, с. 112].

2. Інформаційний етап. Цей етап передбачає формування безпосереднього інформаційного приводу, який би слугував легітимізацією початку збройної агресії. В умовах сучасної гібридної війни таким приводом може стати інсценоване порушення прав громадян, провокації або навмисно створені "фейкові" інциденти, які подаються як привід для "захисту демократії", "відновлення правопорядку" або "забезпечення стабільності". У цей період активізується діяльність на всіх рівнях інформаційного простору - від офіційних

заяв до масованого поширення повідомлень у соціальних мережах. Основна мета цього етапу - виправдати збройне втручання в очах міжнародної спільноти та нейтралізувати потенційні осередки спротиву через маніпулятивний вплив на громадську думку.

3. Поствоєнний етап (вихід з операції). Після досягнення військово-політичних цілей інформаційно-психологічна операція переходить у завершальну фазу. Її завданням є забезпечення контрольованого виходу з активної фази конфлікту із збереженням інформаційної переваги. Серед типових заходів цього етапу - формування легітимного уявлення про "перемогу", інформаційна підтримка створення тимчасових або перехідних органів управління, а також активна робота із місцевим населенням, зокрема через кампанії з "відновлення довіри", "переосмислення історії конфлікту" тощо. Особливе значення має боротьба за свідомість та лояльність населення на звільнених або окупованих територіях, адже контроль за інформаційним середовищем на цьому етапі гарантує довгострокову політичну та ідеологічну стабільність [207, с. 112].

У сучасних умовах ведення війни інформаційно-психологічні операції набули особливої ваги та стали невід’ємною складовою як інформаційного протистояння, так і безпосередніх бойових дій [301, с.69–84]. Жоден збройний конфлікт останніх десятиліть не обходиться без активної участі підрозділів ІПсО, що свідчить про системне усвідомлення ролі психологічного та інформаційного впливу на супротивника, а також на власне населення та міжнародну спільноту.

Особливої актуальності використання ІПсО набуло в умовах Війни за Незалежність України, де інформаційний фронт став не менш важливим, ніж традиційні бойові дії.

Одним із найпоширеніших прийомів було масове поширення дезінформації щодо бойових дій, зокрема фейкові повідомлення про відступи українських підрозділів або нібито значні втрати серед військових. Такі меседжі мали на

меті деморалізувати населення, створити панічні настрої та підірвати довіру до ЗСУ.

Ще одним напрямом ІПсО були фейкові повідомлення про гуманітарну кризу. Через соціальні мережі та онлайн-медіа поширювалися спотворені дані про нестачу продуктів, води чи медикаментів, нібито спричинені українською владою, що підсилювало соціальну напругу та формувало образ держави як неефективного суб'єкта.

Кампанії з дискредитації Збройних Сил України та міжнародних партнерів супроводжувалися фальшивими репортажами, відео та фотографіями, що наводили на думку про неналежне виконання бойових завдань або порушення міжнародного права. Такі операції проводилися через соціальні мережі (Facebook, Telegram, Twitter), месенджери (Viber, WhatsApp) та онлайн-медіа, використовуючи як автоматизовані акаунти (боти) [111, с. 64], так і контрольовані проросійські платформи, що створювало ілюзію широкої підтримки або суспільної паніки.

російською стороною активно використовуються різноманітні методи дезінформаційного впливу на суспільну свідомість, спрямовані на формування бажаних наративів та маніпуляцію громадською думкою. Серед них виділяють створення фальшивих новин, селективне подання фактів, емоційно заряджену пропаганду, використання автоматизованих акаунтів і бот-мереж у соціальних мережах, а також тролінг і персональні атаки. Ці інструменти дозволяють поширювати дезінформацію, підривати довіру до традиційних медіа та інститутів, а також стимулювати соціальні та політичні конфлікти. Комплексне застосування таких методів формує ефективний механізм інформаційного впливу в умовах гібридної війни [135].

Прикладами можуть бути інформаційні кампанії, спрямовані на дискредитацію Збройних Сил України, поширення фейкових «евакуацію керівництва держави» у перші дні широкомасштабного вторгнення рф. Так, зокрема, прикладом інформаційної агресії росії проти України є системне поширення дезінформації щодо нібито американських біологічних лабораторій

на території країни. Подібні кампанії активно реалізовувалися у різні періоди: вперше – на початку пандемії Covid-19 у 2020 р., коли будь-які згадки про можливе штучне походження вірусу викликали широкий міжнародний резонанс, та повторно – під час повномасштабного вторгнення росії в Україну в 2022 році.

У межах таких кампаній використовувалися методи інформаційно-психологічного впливу, зокрема поширення теорій змови, маніпуляції фактами та спотворення реальної інформації про діяльність медичних установ та наукових організацій України. Мета цих операцій полягала у створенні інформаційної загрози, формуванні негативного образу України, підриві довіри до її державних інституцій та легітимізації агресивних дій росії як протидії «зовнішнім загрозам» [61, с.35]. Застосування таких методів дозволяє одночасно впливати на міжнародну аудиторію та внутрішню громадську думку, стимулюючи соціальну напругу та поширюючи панічні настрої [106].

Інформаційна війна, що супроводжувала анексію Криму росією, продовжується й нині, охоплюючи як традиційні, так і цифрові медіа. Для росії ключові наративи залишаються стабільними: відновлення імперського статусу, у цих наративах russki mir виступає як ідеологічна відповідь ніби то на експансію Заходу, що перетворила країни Східної та Центральної Європи на «маріонетки». Інтернет став постійним фронтом інформаційного протистояння, де операції ведуться й під час військових дій.

Москва продовжує поширювати системну дезінформацію про Україну і в 2025 р, зокрема щодо нібито незаконного вилучення органів, або так званої «чорної трансплантології». російські офіційні особи (М.Захарова) та державні медіа пов’язують ці твердження з діяльністю США, стверджуючи, що Україна нібито слугує полігоном для експериментів із біозброєю та незаконними медичними практиками. Такі заяви регулярно озвучуються високопоставленими представниками Кремля та поширюються на платформах державних ЗМІ, зокрема у соціальних мережах, без надання будь-яких документальних доказів або перевірених джерел [3].

У червні 2025 р. російські пропагандистські ресурси поширили сфальсифікований лист нібито від імені Прем’єр-міністра України щодо нібито «підготовки до евакуації центральних органів влади на захід країни» (Додаток Г). Документ містив неправдиві відомості про скорочення штатів, передислокацію міністерств і надання списків мобілізаційного персоналу, що не відповідало дійсності та було повністю вигадане. Центр протидії дезінформації при Раді національної безпеки і оборони України підтвердив, що офіційного документа не існує, а його зміст супроводжувався численними орфографічними помилками та порушеннями процедур діловодства [18; 222].

російські спецслужби продовжують використовувати інформаційно-психологічні операції для дискредитації України. За даними Центру протидії дезінформації при Раді національної безпеки і оборони України, ворог здійснює масові дзвінки та надсилає повідомлення, використовуючи шантаж, щоб примусити родичів поширювати сфабриковані листи зі звинуваченнями української влади у нібито відмові від обмінів. Ці повідомлення направляються також до міжнародних організацій і державних інституцій, включно з ООН та адміністрацією США [244].

російські пропагандистські кампанії системно спрямовані на дискредитацію Збройних Сил України через поширення фейкової інформації та маніпулятивних наративів. До основних методів належать поширення відео та фотографій, змонтованих або створених за допомогою штучного інтелекту, сфабриковані повідомлення про нібито масові дезертирства, випадки мародерства або насильства серед військових, а також маніпуляції з чисельністю та успішністю операцій ЗСУ.

Такі інформаційно-психологічні операції мають на меті деморалізацію особового складу, підрив довіри суспільства до армії, створення атмосфери хаосу та сумнівів щодо ефективності оборонних структур. Вони також використовуються для легітимізації військових агресій росії, формування негативного образу України на міжнародній арені та посилення впливу на зовнішню громадську думку. При цьому сучасні технології, зокрема

генеративний контент і соціальні мережі, значно підвищують масштабність і швидкість розповсюдження подібних фейків.

російські телеграм-канали поширюють відеоконтент, що нібито демонструє невдоволення українських військових та їхнє нібито самовільне залишення частин. Однак перевірка джерел показала, що першоджерело відео відсутнє, а записи, найімовірніше, були створені або змодифіковані із застосуванням технологій штучного інтелекту. Аналіз ролика свідчить про численні аномалії: невідповідність звуку і міміки, обмежену рухливість обличчя під час мовлення, неприродний вигляд очей і відсутність окремих деталей, що характерно для генеративного контенту. Використання інструменту Sensity AI підтвердило ймовірне застосування ШІ у більш ніж 71% випадків на записі [35].

російськими спецслужбами у мережі було поширено змінений скриншот заголовка новини українського видання, нібито свідчить про напад військового 92-ї ОШБр на працівника територіального центру комплектування (ТЦК) у Харкові. Аналіз показав, що це фотофейк: пропагандисти відредагували оригінальний заголовок, замінивши слово «чоловік» на «військовий», створивши хибне враження щодо участі бійців ЗСУ. Оригінальна стаття стосувалася нападу місцевого жителя у місті Зміїв Харківської області, який не мав жодного стосунку до ЗСУ. Поліція підтвердила, що нападник не є військовослужбовцем, і наразі перебуває під цілодобовим домашнім арештом. Цей випадок ілюструє типову методику російської пропаганди, спрямовану на дискредитацію українських військових через маніпуляцію новинними заголовками та фото [322].

З огляду на зростаючий вплив таких операцій на внутрішньополітичну стабільність, громадську думку, міжнародні позиції та загалом на безпекову архітектуру держави, постає нагальна потреба у формуванні ефективних механізмів протидії. У геополітичному вимірі протидія ІПсО охоплює комплекс заходів, спрямованих на виявлення, аналіз, нейтралізацію та запобігання зовнішньому інформаційному впливу. Основною метою такої діяльності є забезпечення національної безпеки, збереження суверенітету, політичної

стабільності та культурної ідентичності. При цьому характер відповідних заходів визначається політико-інституційною моделлю держави.

Моделі протидії ІПсО суттєво варіюються залежно від типу політичного режиму, а їхня ефективність значною мірою визначається балансом між захистом інформаційного простору та збереженням демократичних цінностей.

У світовій практиці умовно виокремлюють два підходи до протидії ІПсО - демократичний та авторитарний. Перший базується на пріоритеті свободи слова, відкритості та прозорості політичних інститутів. Його реалізація передбачає розбудову правової бази, яка одночасно гарантує свободу вираження поглядів та встановлює обмеження щодо поширення дезінформації й мови ворожнечі. Такі суспільства зазвичай мають незалежні медіа та регуляторні органи, які контролюють дотримання журналістських стандартів. Важливою складовою є також розвиток медіаграмотності, підтримка критичного мислення й розмаїття інформаційних джерел, що забезпечує громадянам доступ до різних точок зору. Натомість авторитарний підхід передбачає централізований контроль інформаційного простору, обмеження доступу до незалежних джерел, застосування цензури та поширення пропаганди через підконтрольні медіа. У таких умовах інформаційна політика спрямована на формування одностороннього наративу, дискредитацію альтернативних позицій, блокування цифрових платформ і посилений моніторинг цифрових комунікацій. Водночас застосовуються репресивні заходи проти опозиційних голосів - від переслідування журналістів до криміналізації публічної критики Інформаційно-психологічні операції на геополітичній арені [318].

Ідентифікація інформаційно-психологічних операцій є критично важливою складовою забезпечення інформаційної та національної безпеки загалом. У сучасному геополітичному контексті, коли держави активно використовують інформаційні ресурси для впливу на внутрішньополітичні процеси інших країн, розуміння механізмів ІПсО набуває стратегічного значення. Для виявлення таких операцій застосовуються низка методик, серед яких - лассуелівський метод, моделі Сміта, пропагандистська модель Хермана і Чомскі, підхід

Джовета й О'Доннелл та SCAME-метод. Ці інструменти дозволяють аналізувати джерела, зміст, канали, аудиторію та наслідки інформаційного впливу, розкриваючи структуру та цілі ІПсО. Їх використання сприяє формуванню ефективних стратегій протидії пропаганді, дезінформації й маніпуляції громадською думкою, а також зміцненню стійкості демократичних інститутів перед зовнішнім інформаційним тиском [318, с.81-84].

Ключовим інструментом протидії інформаційно-психологічним операціям виступає контрпропаганда, оскільки її завданням є нейтралізація зовнішнього інформаційного впливу та захист національного інформаційного простору. Вона передбачає комплекс заходів, що поєднують реактивні та проактивні дії: не лише спростування дезінформації, а й формування позитивного іміджу держави на міжнародній арені. Ефективність контрпропаганди базується на стратегічному плануванні, аналізі ворожих кампаній, визначенні цільових аудиторій, створенні релевантного контенту, його поширенні через різні медіа та постійному моніторингу результатів.

Серед ключових принципів контрпропаганди виділяють наступальність, оперативність, гнучкість і комплексність. Основні методи включають пряме спростування дезінформації, переключення уваги та контратаку, а типові тактичні прийоми - «парасольку», «лійку», «колесо» та «заміщення» - спрямовані на зниження ефективності ворожих інформаційних впливів [318, с. 86–87]. У сукупності ці підходи формують системний механізм інформаційного захисту держави в умовах гібридної війни.

Українська сторона застосовує комплекс контрпропагандистських заходів. Це включає оперативне спростування фейкових повідомлень через офіційні канали, інформаційні кампанії у соціальних мережах з донесенням правдивої інформації, верифікацію даних, а також активну міжнародну комунікацію з метою формування достовірного образу України в світі. Прикладами таких заходів були публікації від Міноборони та Генштабу ЗСУ, роз'яснювальні ролики у Telegram-каналах, спростування фейків через

міжнародні медіаплатформи та інформування партнерів про реальний стан справ на фронті.

Контрпропаганда в умовах російсько-української війни довела свою ефективність як елемент національної системи інформаційного захисту. Вона здатна мінімізувати негативний вплив ІПсО, зменшити ризики деморалізації населення та посилити стійкість суспільства до зовнішніх інформаційних загроз, одночасно забезпечуючи формування позитивного міжнародного іміджу держави.

Поряд із контрпропагандою, яка виконує функцію оперативного реагування на деструктивні інформаційні впливи, сучасна система протидії інформаційно-психологічним операціям ґрунтується на комплексному застосуванні взаємопов'язаних інструментів, спрямованих як на нейтралізацію загроз, так і на формування стійкості суспільства. У цьому контексті вагому роль відіграють стратегічні комунікації, що забезпечують послідовне та узгоджене донесення офіційних позицій і сприяють підвищенню рівня довіри до державних інституцій. Важливим елементом є також розвиток механізмів перевірки достовірності інформації, які дозволяють своєчасно виявляти та спростовувати маніпулятивні або неправдиві повідомлення. Поряд із цим особливого значення набуває підвищення рівня медіаграмотності населення, що формує здатність громадян критично оцінювати інформаційні потоки та знижує їхню вразливість до психологічного впливу. Не менш важливими є заходи із забезпечення кіберзахисту інформаційної інфраструктури, удосконалення нормативно-правового регулювання інформаційної сфери, а також налагодження ефективної взаємодії з міжнародними партнерами та цифровими платформами. Системний моніторинг інформаційного простору із застосуванням сучасних аналітичних інструментів забезпечує можливість раннього виявлення загроз і формування превентивних заходів.

Отже, у сучасних умовах ведення війни інформаційно-психологічні операції становлять одну з найбільш ефективних форм впливу на суспільну свідомість та поведінку населення. Завдяки інтерактивності, високій швидкості

поширення контенту та широкому охопленню аудиторій, цифрові платформи стали ідеальним середовищем для реалізації маніпулятивних інформаційних стратегій. Застосування таких технологій, як бот-мережі, фейкові акаунти, мікротаргетинг та емоційно забарвлений контент, дозволяє суб'єктам гібридного впливу здійснювати системну та приховану дестабілізацію суспільства. Це не лише ускладнює процес ідентифікації джерела загрози, а й створює умови для довготривалого порушення інформаційної безпеки держави. У цьому контексті актуальним залишається завдання формування комплексної системи протидії інформаційно-психологічному впливу, яка має поєднувати державні, технологічні та освітні підходи, зокрема шляхом розвитку критичного мислення, медіаграмотності населення та вдосконалення національної політики у сфері інформаційної безпеки.

2.3. Кіберзагрози та технічні інструменти гібридної війни за допомогою соціальних мереж

Кіберпростір сьогодні є ключовим елементом функціонування сучасного суспільства, оскільки цифрові технології та мережеві ресурси інтегруються у всі сфери життя людини. Використання цих технологій має критичне значення для державної політики та національної безпеки. У той час як стратегічний баланс у сфері традиційної зброї ще зберігається, у кіберпросторі паритет фактично порушено, що підтверджується активністю державних кіберпідрозділів, а також громадських і терористичних організацій, які використовують цифровий простір для досягнення соціально-політичних, економічних, інформаційних та військових цілей [174, с.93]. Для України кіберпростір створює підвищену уразливість критичної інфраструктури та інформаційних систем, що вимагає ефективних заходів захисту, превентивного моніторингу загроз і своєчасного реагування на кібератаки.

рф використовує сучасні інформаційні технології для впливу на свідомість громадян, поширення пропаганди агресивної війни, розпалювання національної

та релігійної ворожнечі, а також для спроб зміни конституційного ладу або порушення суверенітету та територіальної цілісності України. Важливим компонентом сучасної гібридної війни виступають кіберзагрози, оскільки, власне, вони поєднують технічні та організаційні засоби впливу на критичну інфраструктуру та інформаційні ресурси держави. Застосування російською федерацією технологій гібридної війни проти України зробило інформаційну сферу ключовою ареною протиборства. Кібербезпека держави спрямована на захист комп'ютерних систем і мереж від кіберзагроз, таких як хакерські атаки, віруси та інше шкідливе програмне забезпечення.

Законодавством передбачено використання сучасних технологічних засобів кіберзахисту, таких як шифрування, системи аутентифікації та контролю доступу, резервне копіювання та відновлення критично важливої інформації. Окремо визначено пріоритет міжнародної співпраці, яка передбачає обмін інформацією про загрози та інциденти, участь у спільних навчаннях і тренінгах, а також взаємодію з міжнародними організаціями та державами для підвищення ефективності національної системи кібербезпеки.

Кібербезпека, відповідно до чинного законодавства, визначається як захищеність життєво важливих інтересів людини, громадянина, суспільства та держави під час використання кіберпростору [226]. Вона передбачає забезпечення сталого розвитку інформаційного суспільства та цифрового комунікативного середовища, своєчасне виявлення, запобігання та нейтралізацію реальних і потенційних загроз національній безпеці України у кіберпросторі.

Під кібербезпекою розуміють підсистему інформаційної безпеки, що зосереджується на захисті комп'ютерних систем, мереж і програмного забезпечення від цифрових загроз. Вона передбачає впровадження технічних та організаційних заходів для запобігання кіберзагрозам, зокрема хакерським атакам, вірусам, шкідливому ПЗ та фішингу, а також здійснення дій для оперативного реагування і відновлення після інцидентів. [53, с.466].

М. Сулмейєр визначав кібербезпеку як комплекс дій із запобігання і реагування на загрози, спрямовані на критичну інфраструктуру держави, підкреслюючи необхідність міжнародного співробітництва та розробки політик для протидії кіберконфліктам [53, с. 467].

Віктор Цимбалюк визначав кібербезпеку як стан захищеності інформаційних систем та мереж від кіберзагроз, що досягається через впровадження спеціальних технологій, управлінських процесів та практик оцінки і мінімізації ризиків у цифровому середовищі [331].

У сфері кібербезпеки особливо важливим є: захист критичної інфраструктури, включно з енергетикою, транспортом, зв'язком та фінансовим сектором; розвиток технологій для моніторингу, виявлення та нейтралізації кіберзагроз, а також удосконалення криптографічного захисту даних; підвищення кібергігієни шляхом формування обізнаності населення щодо основ кіберзахисту; інтеграцію з міжнародними стандартами через співпрацю з країнами-партнерами, обмін досвідом і технологіями та впровадження стандартів, таких як ISO/IEC 27001.

Серед ключових принципів забезпечення кібербезпеки, відповідно до нормативно-правової бази закладено комплексний підхід до захисту всіх компонентів кіберінфраструктури, превентивні дії та оцінку загроз, системну взаємодію між державними органами, приватним сектором і міжнародними партнерами, а також відповідальність суб'єктів за виконання встановлених обов'язків. Для реалізації цих принципів створено національну систему кібербезпеки, яка об'єднує державні органи, силові структури та критичну інфраструктуру, формуються центри моніторингу та реагування на кіберінциденти, а також визначаються суб'єкти критичної інфраструктури, які підлягають обов'язковому захисту та аудиту [226].

Кіберзагроза трактується як наявні або потенційно можливі явища та фактори, які створюють небезпеку життєво важливим національним інтересам України у кіберпросторі та можуть негативно впливати на стан кібербезпеки

держави, ефективність кіберзахисту її об’єктів і безпеку інформаційної інфраструктури [226]

За визначенням В. Ліпкана у першому словнику зі Стратегічних комунікацій, кіберзагроза розглядалась як дестабілізуючий чинник, що негативно впливає на об’єкти інформаційної безпеки шляхом використання технологічних можливостей кіберпростору. Вона спрямовувалася на порушення конфіденційності, цілісності, авторства, доступності та спостережності інформації, а також включала загрозу застосування деструктивних інформаційно-психологічних впливів на свідомість і психічний стан населення [291, с. 190].

Згідно з визначенням Діордіц І.В., кіберзагроза являла собою протиправні, карані дії суб’єктів інформаційних правовідносин, які створювали небезпеку життєво важливим інтересам людини, суспільства та держави. Їх реалізація залежала від належного функціонування інформаційних, телекомунікаційних та інформаційно-телекомунікаційних систем, а також від процесів створення, збору, отримання, зберігання, використання, поширення, охорони та захисту інформації [80, с.101].

Дослідники виокремлюють такі види кіберзагроз:

- Аргетовані атаки (APT) передбачають прицільне або масове втручання для компрометації конкретних систем або користувачів, зокрема посадових осіб і осіб з доступом до цінної інформації.
- Кібертероризм полягає у використанні мереж для впливу на системи керування об’єктами, координації дій терористичних угруповань та здійсненні інформаційно-психологічного впливу на населення.
- Кібервійни включають застосування спеціалізованого шкідливого ПЗ, наприклад Stuxnet, для диверсій та порушення роботи критичних і військових систем.
- Хактивізм полягає у викритті таємної інформації та незаконних дій урядів або політичних сил через публікацію даних у відкритому доступі [27, с. 107].

•Атаки на банківські системи здійснюються з метою викрадення коштів через фішинг, крадіжку даних платіжних карток та втручання у системи «клієнт-банк».

•Атаки на електронний уряд - спрямовані на порушення функціонування інформаційно-комунікаційних систем державних органів і органів місцевого самоврядування, що могло підривати довіру до державних послуг.

•Апаратні закладки передбачають шкідливі модифікації мікросхем і прошивок комп'ютерного та мережного обладнання для несанкціонованого доступу [58, с. 17; 79, с.206].

До таких загроз дослідник І. Діордіца відносить і гібридну війну. [336, с. 299-309; 78, с. 201].

У "Стратегічному оборонному бюлетені України" подано офіційні дефініції ключових понять, що стосуються кібербезпеки у воєнний час, зокрема, "воєнна агресія в кіберпросторі" та "кібероборотьба". "Воєнна агресія в кіберпросторі" трактується як систематичне та масштабне застосування деструктивних дій проти держави в інформаційно-комунікаційних мережах, що здійснюються іноземними державами або їх коаліціями. До таких дій відносять використання кіберпідрозділів збройних сил, розвідувальних та спеціальних служб, застосування кіберозброєння й інших спеціальних засобів впливу, зокрема із приховуванням джерел атаки та каналів її реалізації. "Кібероборотьба" розглядається, як комплекс скоординованих дій у кіберпросторі, що включає як наступальні (кібератаки, кібероперації, радіоелектронне подавлення), так і оборонні заходи (захист власної інфраструктури), спрямованих на досягнення стратегічної, оперативної чи тактичної переваги над противником [289; 350].

Стосовно терміну "кібератака", то вона визначається, як "спрямовані (навмисні) дії в кіберпросторі, які здійснюються за допомогою засобів електронних комунікацій (включаючи інформаційно-комунікаційні технології, програмні, програмно-апаратні засоби, інші технічні та технологічні засоби і обладнання) та спрямовані на досягнення однієї або сукупності таких цілей: порушення конфіденційності, цілісності, доступності електронних

інформаційних ресурсів, що обробляються (передаються, зберігаються) в комунікаційних та/або технологічних системах, отримання несанкціонованого доступу до таких ресурсів; порушення безпеки, сталого, надійного та штатного режиму функціонування комунікаційних та/або технологічних систем; використання комунікаційної системи, її ресурсів та засобів електронних комунікацій для здійснення кібератак на інші об'єкти кіберзахисту" [229].

Основні види кібератак, що застосовуються зловмисниками проти держав, включають деструктивні атаки, підривні атаки, озброєння даними та дезінформацію. Деструктивні атаки спрямовані на фізичне або логічне пошкодження інформаційних і технологічних систем, що може призвести до зупинки роботи критично важливих об'єктів та втрати даних. Підривні атаки мають на меті приховане порушення нормальної роботи систем, підрив довіри до інфраструктури або створення передумов для майбутніх деструктивних дій, часто через проникнення у внутрішні процеси та маніпуляції даними. Озброєння даними передбачає використання викрадених або зібраних даних як інструменту тиску чи впливу, наприклад, для шантажу, економічних маніпуляцій або втручання у політичні процеси. Дезінформація полягає у цілеспрямованому поширенні неправдивої або спотвореної інформації через цифрові канали, соціальні мережі та медіа з метою маніпулювання громадською думкою, посилення соціальної напруженості або підриву легітимності державних інституцій [256, с.86; 371]. Кібератаки можуть мати технічний, програмний або соціоінженерний характер, бути одиничними або здійснюватися серіями, мати як локальні, так і глобальні наслідки для об'єкта атаки.

Кіберборотьба - це комплексна діяльність у кіберпросторі, яка включає як наступальні, так і оборонні дії, а також інформаційну розвідку. Її метою є досягнення кіберпереваги, захист власних ресурсів і дестабілізація супротивника. Кібератака - це лише один із інструментів кіберборотьби, конкретна наступальна операція, спрямована на виведення з ладу, знищення або несанкціоновану зміну інформаційних систем противника (таблиця 1.1).

Таблиця 1.1

Порівняльна таблиця “Кіберборотьба - Кібератака”

Ознака	Кіберборотьба	Кібератака
Сутність	Сукупність дій у кіберпросторі, що включає наступальні, оборонні та розвідувальні операції.	Конкретна наступальна дія, спрямована на завдання шкоди інформаційним системам чи даним.
Масштаб	Широкий, стратегічний — охоплює усі аспекти кібероперацій.	Обмежений, тактичний — один інцидент або операція.
Мета	Досягнення переваги у кіберпросторі, забезпечення кібербезпеки, вплив на супротивника.	Порушення роботи систем, крадіжка даних, шантаж, дестабілізація.
Інструменти	Оборонні технології (фаєрволи, SOC), наступальні дії (DDoS, шкідливе ПЗ), кіберрозвідка.	DDoS-атаки, віруси, фішинг, експлойти, шкідливі скрипти.
Суб’єкти	Держави, військові структури, спецслужби, приватні компанії, хактивісти.	Ті ж самі суб’єкти, але діють точково і цілеспрямовано.
Тривалість	Може бути довгостроковою та постійною.	Переважно короткочасна, досягнення швидкого ефекту.
Приклади	Створення Кіберкомандування ЗСУ, діяльність ІТ-Армії України, кампанії з протидії російським хакерам.	Атаки 14, 15, 16 та 23 лютого 2022 року на урядові сайти України, NotPetya (2017), атаки на енергомережі України (2015, 2016).

Джерело: укладено автором [292], [371]

Головними напрямами забезпечення кібербезпеки України є системна протидія кіберзлочинності, кібертероризму та кібершпигунству, що передбачає запобігання, виявлення та нейтралізацію загроз критичним об’єктам національної інформаційної інфраструктури [292].

Кіберзлочин (комп’ютерний злочин) - це суспільно небезпечне винне діяння, вчинене в кіберпросторі або із його використанням, за яке передбачена кримінальна відповідальність згідно з законодавством України [90; 98].

До основних видів кіберзлочинності належать розповсюдження шкідливого програмного забезпечення, злам паролів, викрадення реквізитів банківських карток, а також розповсюдження незаконної інформації в Інтернеті [79, с.211; 230, с. 33].

До найпоширеніших видів кіберзлочинів також відносять кардинг, фішинг, вішинг, онлайн-шахрайство, піратство, кард-шарінг, соціальну інженерію, молвери, поширення протиправного контенту, рефайлінг та інші [52].

Соціальні мережі стають потужним інструментом кібершпигунства. Метою кібершпигунства у соціальних мережах є виявлення політичних та соціальних настроїв користувачів, моніторинг потенційної екстремістської, терористичної або антиурядової діяльності, отримання даних про організаційні зв'язки, участь у заходах та мітингах, а також формування соціально-психологічних профілів для проведення інформаційних операцій і маніпуляцій. Методи збору інформації включають аналіз відкритих даних, фішинг та соціальну інженерію для отримання доступу до приватної інформації, моніторинг поведінкових патернів користувачів для виявлення схильності до певних дій або груп, а також використання шкідливого програмного забезпечення, зокрема троянських програм та кейлогерів, для отримання інформації, яка не доступна публічно.

Кібершпигунствоу соціальних мережах, в свою чергу, є формою комп'ютерного шпигунства, що передбачає систематичний збір інформації про користувачів через їхню активність у цифровому середовищі. До таких даних належать профільні відомості, включно з іменем, віком, місцем проживання, професійною діяльністю та контактами; активність у мережі, зокрема публікації, коментарі, лайки, перепости та участь у групах; мультимедійні матеріали, такі як фотографії, відео та геолокаційні дані; а також соціальні зв'язки, включно з друзями, підписниками та характером взаємодій [212].

Кібератероризм - це комплексна модель дій, що проявляється у навмисних, політично мотивованих атаках на інформацію, оброблювану комп'ютерами та комп'ютерними системами, які створюють небезпеку для життя чи здоров'я людей, або можуть призвести до інших тяжких наслідків. Такі дії здійснюються

з метою порушення громадської безпеки, залякування населення або провокації військового конфлікту [59].

Джерелами кіберзагроз можуть виступати міжнародні хакерські угруповання, окремі кваліфіковані злочинці у сфері інформаційних технологій, іноземні державні органи, терористичні та екстремістські формування, а також транснаціональні корпорації та фінансово-промислові групи.

Серйозну загрозу національній безпеці України становлять кібератаки на критично важливі сектори державного управління та інфраструктури – зокрема енергетичний комплекс, системи зв'язку, охорону здоров'я, транспортно-логістичні мережі та банківсько-фінансову сферу.

Перші зафіксовані кібератаки на інформаційні системи державних установ і приватних підприємств України датуються 2013 р., під час масових протестів [361].

Російсько-українська кібервійна стала першим конфліктом у кіберпросторі, під час якого відбулася успішна атака на енергетичну систему з виведенням її з ладу. Крім того, зафіксовано численні кібератаки на державні інформаційні системи, зокрема систему «Вибори» під час президентських виборів, а також атаки на відмову обслуговування (DDoS), діфейси, кібершпигунство та інші прояви кіберзагроз [359].

Показовим прикладом є кібератака на енергетичний сектор України 23 грудня 2015 р. у результаті якої за допомогою фішингової кампанії та шкідливого програмного забезпечення зловмисники отримали доступ до диспетчерських систем енергокомпаній, що призвело до масштабних відключень електропостачання для значної кількості споживачів [326].

Схожий інцидент зафіксовано 19-20 лютого 2016 р., коли було здійснено цілеспрямовану розсилку шкідливих електронних листів на адреси близько ста енергетичних підприємств України. Ця атака мала характер точкової кампанії, спрямованої на проникнення в інформаційні системи через заражені документи, надіслані співробітникам компаній [373]. Ці випадки підтвердив тенденцію до

системного використання фішингових технологій як ключового інструмента гібридних операцій проти критичної інфраструктури.

Кіберзагрози в Україні проявляються на рівні державних інформаційних систем. Так, 6 грудня 2016 р. відбулася хакерська атака на урядові сайти, зокрема, Державну казначейську службу України та інші державні органи, а також на їхні внутрішні мережі, що спричинило затримки у проведенні бюджетних виплат [194]. Уже 7 грудня 2016 р. уряд оперативно виділив 80 млн гривень на посилення кіберзахисту державних систем та протидію подібним інцидентам .

Подібні загрози фіксувалися і в соціальних мережах: наприклад, 19 грудня 2017 р. у Facebook поширювався вірус, який маскувався під файл із назвою video_123. Відкриття такого файлу запускало шкідливу програму, що дозволяла зловмисникам отримати контроль над акаунтами користувачів, викрасти конфіденційну інформацію та порушити роботу систем**.**

Кіберзагрози, як показує сучасний досвід, стали невід’ємною складовою сучасних конфліктів, поєднуючи інформаційні, психологічні та технологічні аспекти впливу. Проте для ефективної реалізації політичних та військових цілей країни-агресори використовують не лише кібератаки, а й широкий спектр технічних інструментів гібридної війни. До них належать засоби електронного та радіотехнічного впливу, системи розвідки та спостереження, автоматизовані платформи для збору й аналізу даних, а також технології масового поширення дезінформації. Таким чином, дослідження кіберзагроз логічно доповнюється аналізом технічних засобів, що забезпечують комплексний характер сучасних гібридних атак.

До технічних інструментів гібридної війни належать спеціалізовані шкідливі програми (зокрема BlackEnergy, Industroyer, NotPetya), засоби для несанкціонованого збору даних і віддаленого керування зараженими мережами, технології соціальної інженерії та фішингових атак, а також інструменти втручання у роботу промислових систем управління (SCADA). Використання цих методів у комплексі дає змогу здійснювати скоординовані кібератаки з

реальними фізичними наслідками, що підтверджує перетворення кіберпростору на важливий театр сучасних воєнних дій.

У червні 2017 р. Україна стала мішенню однієї з наймасштабніших і найруйнівніших кібератак, що отримала назву NotPetya [186]. Атаку було організовано угрупованням Sandworm, яке отримало контроль над серверами компанії Linkos Group - розробника програмного забезпечення для електронного документообігу M.E.Doc. Цей продукт активно використовувався підприємствами, банками та державними установами для податкової звітності та фінансових операцій, що робило його зручним каналом для поширення шкідливого коду. Механізм атаки полягав у модифікації офіційного оновлення програми: вірус вбудовувався безпосередньо у дистрибутив і поширювався серед користувачів через легітимні канали. Після інсталяції зараженого оновлення шкідливе програмне забезпечення отримувало можливість швидко поширюватися всередині корпоративних мереж, використовуючи вразливості операційних систем та протоколів обміну даними. Уже 27 червня, у день початку зараження, шкідливе програмне забезпечення паралізувало роботу близько двох тисяч організацій, причому приблизно 75% жертв були українськими. Серед найбільше постраждалих – державні установи, поліція, банківські системи, аеропорт «Бориспіль», київський метрополітен, засоби масової інформації, мобільні оператори та медичні заклади. За даними Кіберполіції України, вірус шифрував або знищував критично важливі дані, блокував доступ до комп’ютерних систем, зупиняв бізнес-процеси та завдавав суттєвих економічних збитків. Хоча формально шкідливий код імітував роботу програм-вимагачів, його справжньою метою було не отримання викупу, а деструктивне виведення з ладу інформаційних ресурсів. NotPetya став показовим прикладом того, як кібератаки перетворюються на складові гібридної війни: застосування легітимних каналів розповсюдження програмного забезпечення, використання складних технічних експлойтів і поєднання шкідливого коду з елементами дезорганізації управління створили умови для масового ураження критичної інфраструктури та підриву стабільності держави.

Українські офіційні органи заявляли, що до атаки на критичну інфраструктуру країни причетні 16-й та 18-й центри ФСБ росії, які спеціалізуються на питаннях інформаційної безпеки, криптографії та захисту каналів зв'язку. У США атаку вірусу NotPetya розцінили як елемент гібридної стратегії Кремля, спрямованої на дестабілізацію ситуації в Україні та підтвердження його причетності до триваючого конфлікту [295].

У травні 2021 р. ГО «Детектор медіа» провела дослідження споживання дезінформації в Україні, показавши, що проросійські наративи активно проникають у медіапростір південно-східного регіону через телебачення, місцеві ЗМІ та соціальні мережі. Вразливими до таких маніпуляцій є переважно російськомовні громадяни віком понад 45 років із Донбасу, Харкова та Запорізької області, що живуть у соціально-економічно неблагополучних умовах та мають низький рівень медіаграмотності. Антиукраїнські наративи спиралися на ностальгію за радянським минулим, ідеологізацію історичної пам'яті, політизацію мовних і релігійних питань та соціально-економічну нестабільність, досягаючи ефекту завдяки одночасному поширенню різними каналами [291, с.237-240].

Початок повномасштабної збройної агресії російської федерації проти України у 2022 р. супроводжувався суттєвим зростанням масштабів, частоти та складності кібератак, спрямованих як проти державних органів, так і проти критичної інфраструктури та приватного сектору. Це засвідчило інтеграцію кібероперацій у комплекс гібридних воєнних дій.

Атаки на державні установи, енергетичний сектор, медіа та банківську систему стали регулярною складовою гібридної війни, доповнюючи фізичні військові дії.

У 2022 р., порівняно з 2021 р., спостерігалося значне зростання кількості подій інформаційної безпеки. Зокрема, у категорії «Шкідливий програмний код» зафіксовано збільшення у 18,3 рази, а в категорії «Збір інформації зловмисником» – у 2,2 рази. Загалом протягом 2022 року було зареєстровано у 2,8 разів більше кіберінцидентів, ніж у попередньому році, що свідчить про

активізацію кіберзагроз та підвищення їхньої різноманітності [206; 66]. Українські державні та фінансові сайти зазнали серії масштабних кібератак, спрямованих на паралізацію роботи критичної інфраструктури та поширення деструктивних повідомлень [325].

Перша атака 14 січня 2022 р. торкнулася десятків державних ресурсів на платформі CMS October, друга - 15–16 лютого - банків та урядових сайтів, а третя 23 лютого, перед повномасштабним вторгненням, - вивела з ладу ключові державні портали та супроводжувалася поширенням шкідливого програмного забезпечення HermeticWiper, призначеного для знищення даних. Вразливості у програмному забезпеченні та заздалегідь підготовлені шкідливі коди свідчать про системний і цілеспрямований характер цих кібератак.

В квітні 2022 р. російські хакери використали сім інтернет-доменів для проведення кібератак, які Microsoft взяла під контроль, що дозволило запобігти їх реалізації. За оцінкою компанії, угруповання Strontium намагалося отримати доступ до комп'ютерних мереж з метою забезпечення тактичної підтримки фізичного вторгнення та викрадення конфіденційної інформації. Інформацію про атаку та заходи реагування компанія повідомила уряду України [335].

CERT-UA (урядова команда реагування на комп'ютерні надзвичайні події при Держспецзв'язку), зафіксувала розповсюдження електронних листів з темою «№1275 від 07.04.2022». Листи містили HTML-файл, відкриття якого створювало архів із шкідливим файлом, що надавало зловмисникам повний контроль над комп'ютером, загрожуючи крадіжкою інформації та пошкодженням даних. Активність пов'язана з угрупованням UAC-0010 (Armageddon), яке раніше здійснювало кібератаки проти державних органів України та країн ЄС [304; 122].

Протягом 2023 р. у межах функціонування Системи виявлення вразливостей та реагування на кіберінциденти було здійснено аналіз близько 18 мільярдів подій, що надходили в результаті моніторингу, збору, передачі та обробки телеметричних даних про кіберінциденти та кібератаки. Первинний аналіз дозволив ідентифікувати 133 мільйони подій з ознаками потенційних

загроз інформаційної безпеки. Подальший вторинний аналіз та застосування фільтраційних механізмів дозволили класифікувати та опрацювати близько 148 тисяч критичних подій, які становили реальну загрозу кіберпростору. У доповнення до автоматизованого аналізу, фахівцями з інформаційної безпеки було зафіксовано та опрацьовано 1105 підтверджених кіберінцидентів, що свідчить про зростання на 62,5% у порівнянні з показниками 2022 р. Така динаміка підкреслює актуальність посилення заходів кіберзахисту та вдосконалення систем моніторингу і реагування на інциденти [91; 67; 288; 68; 197].

За даними 2023 р., в Україні зафіксовано понад 2,5 млн кібератаки, що на 15,9% перевищує показник 2022 р.. За інформацією урядової організації CERT-UA, яка відповідає за запобігання, виявлення та реагування на кібератаки, протягом року зареєстровано понад 347 атак на центральні органи влади, близько 276 - на органи місцевого самоврядування, 175 - на організації сектору безпеки та оборони, а також 127 атак - на приватні компанії [75].

Хактивісти застосовують різні методи для реалізації своїх цілей. Найпоширенішими з них є дефейсинг веб-сайтів, під час якого змінюється зовнішній вигляд, контент або функціональність сайту для передачі повідомлення або демонстрації власних поглядів; DDoS-атаки (атаки відмови в обслуговуванні), коли велика кількість систем або пристроїв створює перевантаження цільового ресурсу, блокуючи його роботу та привертаючи увагу до певного питання; і витік даних, що передбачає несанкціонований доступ до баз даних або систем для розкриття конфіденційної чи секретної інформації з метою викриття неправомірних дій та привернення уваги до ігнорованих проблем, що може також призводити до розкриття особистих або державних даних [11].

Найактивнішими проросійськими угрупованнями хактивістів, які здійснювали атаки на інформаційні ресурси України у 2023 р., були: «Народная CyberАрмия», «BLUENET», «NoName057(16)», «PHOENIX» та «Lira».

Кількість кібератак, проведених цими угрупованнями, становила 9% від загальної кількості атак, організованих аналогічними групами [119].

У 2023 р. Департамент кіберполіції Національної поліції України суттєво посилив свою діяльність у сфері протидії кіберзлочинності, виявивши понад 3600 кіберзлочинів, провівши 18 міжнародних спецоперацій у співпраці з іноземними правоохоронними органами (Грузії, Швейцарії, Чехії, Ізраїлю, Норвегії, Нідерландів, Франції, Німеччини та Сполучених Штатів.), оголосивши підозру понад 1700 особам, передавши до суду понад 4000 обвинувальних актів, заблокувавши близько 13 тисяч ворожих вебресурсів та забезпечивши відшкодування збитків на суму майже 144 млн грн. [177].

Звіт за 2024 р. ґрунтувався на статистичних даних Оперативного центру реагування на кіберінциденти (далі - ОЦРК) у межах функціонування Системи виявлення вразливостей і реагування на кіберінциденти та кібератаки. За цей рік було опрацьовано сотні мільярдів подій телеметрії та зафіксовано майже 3 мільйони подій інформаційної безпеки. Досягнення таких результатів стало можливим завдяки постійному моніторингу активності в інформаційно-комунікаційних системах, використанню засобів виявлення загроз у мережі, аналізу даних із систем захисту кінцевих точок, а також інтеграції даних розвідки загроз для своєчасного виявлення потенційних кіберінцидентів та кібератак на об’єкти кіберзахисту. Особлива увага під час обробки даних була зосереджена на 28 тисячах критичних подій інформаційної безпеки, які вимагали негайного втручання аналітиків ОЦРК. У результаті комплексного аналізу цих подій було виявлено та опрацьовано 1042 підтверджені кіберінциденти. Переважна більшість інцидентів була пов’язана з поширенням шкідливого програмного забезпечення, основною метою якого було отримання віддаленого доступу до інформаційних систем з метою кібершпигунства або викрадення грошових коштів. Понад 90% опрацьованих кіберінцидентів у 2024 р. стосувалися організацій урядового сектору. Найактивнішими кластерами кіберзагроз, виявленими ОЦРК у 2024 р., стали UAC-0010, UAC-0006 та UAC-0050 відповідно до класифікації CERT-UA. Основним початковим вектором

кібератак було поширення шкідливого програмного забезпечення за допомогою електронної пошти, зокрема методи T1566.001 Phishing: Spearphishing Attachment за класифікацією MITRE ATT&CK [69].

19 грудня 2024 р. здійснено кібератаку на державні реєстри України, що призвело до тимчасової недоступності численних інформаційних систем, у тому числі Державного реєстру актів цивільного стану громадян, Єдиного державного реєстру юридичних осіб та ФОП, Державного реєстру прав на нерухоме майно та порталу державних сервісів «Дія» [242; 144].

У відповідь на загрозу Європейський Союз, НАТО та міжнародні технологічні компанії активізували співпрацю з Україною, посиливши обмін даними про кіберінциденти, надання технічної допомоги й підтримку у зміцненні національної кіберстійкості.

Щодня на українські об’єкти здійснюється понад десять кібератак, що завдає значної шкоди економіці та особливо критично впливає на об’єкти інфраструктури.

Сучасні кібератаки характеризуються високою складністю та потенційною небезпекою, що створює серйозні загрози для критично важливої інфраструктури. Зловмисники зосереджують увагу на виявленні вразливостей у системах управління та застосовують різноманітні інноваційні методи, зокрема багатофункціональне шкідливе програмне забезпечення, віруси-шифрувальники, ботнети для розподілених атак (DDoS), а також втручання у хмарні сервіси та виробничі системи через ланцюги постачання. У контексті швидкого розвитку штучного інтелекту масштаби та наслідки таких загроз у найближчі 5–10 років можуть істотно зрости, створюючи нові виклики для глобальної кібербезпеки та потребуючи вдосконалення стратегій захисту і управління ризиками.

Кібератаки не лише ускладнюють функціонування державних інституцій, але й створюють додаткові ризики для цивільного населення, провокуючи соціальну напругу та дестабілізуючи суспільство. Сукупність таких атак може

спричинити суттєве послаблення економічного потенціалу країни та завдати прямої шкоди її стратегічним інтересам [174].

Отже, аналіз кіберзагроз та технічних інструментів гібридної війни засвідчив, що кіберпростір перетворився на один із ключових театрів сучасного конфлікту, де змикаються військові, політичні та інформаційні чинники. Використання кібератак, зокрема таких як вірусні кампанії на кшталт NotPetya, атаки на енергетичну інфраструктуру та державні інформаційні системи, доводить їхню здатність паралізувати критично важливі функції держави, спричиняти економічні втрати та створювати атмосферу паніки. Технічні інструменти гібридної війни - шкідливе програмне забезпечення, DDoS-атаки, фішингові кампанії, засоби інформаційно-психологічного впливу - є складовою ширшої стратегії ведення війни, спрямованої на підрив національної безпеки. Кіберзагрози слід розглядати не лише як технічні інциденти, а як елемент цілеспрямованої політико-військової діяльності супротивника. Це вимагає формування цілісної системи кібероборони, інтеграції державних, приватних та міжнародних зусиль, розвитку нормативно-правової бази та підвищення кіберстійкості критичної інфраструктури України.

Соціальні мережі сьогодні виступають не лише як канали комунікації, а й як повноцінні інструменти стратегічного впливу, що активно використовуються у гібридних конфліктах. Користувачі отримують лише ті повідомлення, що підтверджують їхні наявні погляди. Це сприяє формуванню однорідних інформаційних середовищ, де критичне мислення знижується, а поляризація суспільства зростає. Використання соціальних мереж у гібридних війнах виходить за рамки традиційної пропаганди: вони дозволяють у режимі реального часу проводити кампанії впливу, спрямовані на делегітимізацію політичних інститутів, підрив довіри до медіа та органів державної влади, створення атмосфери соціальної напруги. За допомогою таргетованої реклами, автоматизованих бот-мереж та штучно створених акаунтів (тролів) відбувається

поширення фейкових повідомлень і конспірологічних наративів, що впливають на емоції, а не на раціональну оцінку подій.

Соціальні платформи дедалі частіше використовуються для організації протестних рухів і мобілізації масових акцій. Завдяки високій швидкості обміну інформацією вони дозволяють координувати дії великої кількості людей, що робить їх ефективним інструментом як громадянської активності, так і деструктивного втручання зовнішніх акторів. У гібридній війні цей потенціал часто використовується для провокування внутрішніх криз, дестабілізації політичної ситуації та створення ілюзії масової підтримки певних радикальних ідей.

Для держави така ситуація становить серйозний виклик. Система моніторингу та реагування на інформаційні атаки у соціальних мережах у більшості випадків не встигає за темпом їхнього поширення. Це призводить до того, що дезінформаційні кампанії досягають значного охоплення ще до того, як державні інституції надають спростування або офіційну позицію. Крім того, правові механізми протидії інформаційним загрозам у соціальних мережах залишаються обмеженими, оскільки вони повинні балансувати між забезпеченням національної безпеки та дотриманням свободи слова й прав людини.

Соціальні мережі є не лише майданчиком для комунікації, а й ареною боротьби за свідомість громадян, де протистоять один одному наративи, цінності й політичні інтереси.

Ключове місце серед інструментів гібридної війни у соціальних мережах посідають інформаційно-психологічні операції, адже їхній вплив спрямований безпосередньо на когнітивну сферу людини – її емоції, світогляд, систему цінностей та соціальну поведінку. Вони поєднують традиційні методи психологічного тиску, такі як пропаганда, дезінформація та нав’язування стереотипів, із новітніми цифровими технологіями, що забезпечують швидке та масштабне охоплення цільової аудиторії.

Сучасні ІПсО використовують бот-мережі для масового тиражування однакових повідомлень, створення штучного ефекту «суспільного консенсусу» та посилення впливу певних наративів. Таргетована реклама дозволяє персоналізувати інформаційні вкиди та впливати на вразливі групи населення, сегментовані за соціально-демографічними, політичними чи психологічними ознаками. Застосування deepfake-технологій створює додаткові ризики, адже сфальсифіковані відео та аудіо можуть дискредитувати політичних лідерів або провокувати суспільні конфлікти, перш ніж буде доведена їхня недостовірність.

Використання штучного інтелекту дозволяє автоматизувати поширення меседжів і в режимі реального часу підлаштовувати інформаційні кампанії під реакцію аудиторії. Це робить ІПсО гнучкими, динамічними та складними для нейтралізації. Їхня стратегічна мета виходить за межі простої дезінформації: вони спрямовані на довгострокову зміну суспільних настроїв, формування вигідних агресору моделей поведінки, створення атмосфери безсилля та недовіри до інституцій влади. Це особливо небезпечно в умовах війни, коли підтримка єдності та стійкості суспільства є вирішальним чинником національної безпеки. Саме тому протидія ІПсО має бути одним із пріоритетів державної політики у сфері кібербезпеки та стратегічних комунікацій, поєднуючи технологічні рішення (моніторинг, алгоритми виявлення бот-мереж) з просвітницькими заходами та розвитком критичного мислення громадян.

Кіберзагрози та технічні інструменти гібридної війни стали критично важливим фактором національної безпеки, оскільки їхнє використання здатне впливати одночасно на різні рівні функціонування держави та суспільства. Кібератаки різного типу - від масових DDoS-операцій до масштабних вірусних кампаній на зразок NotPetya - можуть паралізувати роботу урядових установ, комунальних служб, фінансових установ та підприємств приватного сектору. Вони не лише зупиняють обробку та передачу даних, але й порушують логістику, призводять до фінансових збитків і дестабілізують повсякденне функціонування критичної інфраструктури.

Особливо небезпечними є кібероперації, які поєднуються з інформаційними кампаніями. Таке поєднання посилює психологічний ефект на населення, формує відчуття хаосу та невизначеності, стимулює панічні настрої і підриває довіру до державних інституцій. У цьому контексті кібератака перестає бути виключно технічним інцидентом і стає елементом комплексної гібридної стратегії, спрямованої на контроль над інформаційним простором і вплив на політичні процеси.

Слід також відзначити, що сучасні кібероперації дедалі частіше набувають комплексного характеру, охоплюючи одночасно різні сектори життєдіяльності держави. Зокрема, вони можуть впливати на енергетичну інфраструктуру, фінансовий сектор, канали комунікацій, транспортні мережі та державні сервіси. Такий широкий спектр цілей ускладнює їх виявлення та нейтралізацію і вимагає від держави системного підходу до кіберзахисту, інтеграції технічних, організаційних та правових заходів.

РОЗДІЛ 3. МЕХАНІЗМИ ЗАХИСТУ ТА ПІДВИЩЕННЯ СТІЙКОСТІ ІНФОРМАЦІЙНОГО ПРОСТОРУ В УМОВАХ ГІБРИДНОЇ ВІЙНИ

3.1. Протидія інформаційним загрозам в соціальних мережах: український та світовий досвід

Сучасна міжнародна система характеризується зростанням непередбачуваності, загостренням конфліктів і деструктивних процесів глобального масштабу. У таких умовах гібридні та проксі-війни набувають статусу провідних інструментів геополітичного протистояння. Вони поєднують військові та невійськові методи впливу - дипломатичні, політичні, економічні, інформаційно-психологічні та кіберзасоби. Це створює потребу у виробленні комплексних підходів до протидії гібридним загрозам і забезпечення національної безпеки. Ефективна протидія вимагає інтегрованого використання дипломатичних, політичних, економічних і військових важелів для захисту національних інтересів, підтримання стабільності та зміцнення обороноздатності держав [101].

Гібридна агресія російської федерації проти України стала каталізатором значних змін у сфері стратегічних комунікацій та національної стійкості. За оцінкою експертів, досвід протидії гібридним загрозам, який Україна накопичила з 2014 р., виступив тригером для модернізації інституцій, удосконалення політик і вироблення нових процедур реагування на внутрішні та зовнішні виклики.

В умовах воєнного стану забезпечення інформаційної безпеки потребує комплексного підходу, що поєднує кілька взаємопов’язаних методів. Правові методи встановлюють нормативну основу захисту інформації, визначають права, обов’язки та порядок реагування на кіберзагрози. Організаційні методи передбачають створення структур і процедур управління безпекою, розробку політик, навчання персоналу та аудит інформаційних систем. Технічні методи

включають застосування апаратних і програмних засобів, криптографічного захисту, контролю доступу, резервного копіювання та сучасних технологій, зокрема штучного інтелекту, для виявлення та нейтралізації загроз. Інформаційні та комунікаційні методи спрямовані на протидію дезінформації, моніторинг інформаційного простору та підвищення кібергігієнічної культури населення. Соціально-психологічні методи враховують людський фактор, формують навички цифрової безпеки та проводять профілактику внутрішніх загроз. Застосування цих методів у комплексі забезпечує стійкість інформаційного середовища, захист державних і приватних систем та підвищення ефективності реагування на сучасні кіберзагрози [150, с 70-73.].

Фахівці пропонують комплекс політичних і стратегічних заходів, спрямованих на виявлення, стримування та нейтралізацію гібридних загроз. Однак спроможність та дієвість таких рішень значною мірою залежить від формування довіри та впевненості у суспільстві, адже інформаційна, когнітивна та соціальна сфери є центральними елементами сучасної гібридної конфронтації [14].

Необхідність забезпечення інформаційної безпеки обумовлюється низкою важливих факторів. По-перше, вона є невід’ємною складовою загальної національної безпеки України, оскільки будь-які порушення в інформаційній сфері можуть безпосередньо впливати на політичну, економічну та соціальну стабільність держави. По-друге, існують реальні та потенційні загрози інформаційній сфері, здатні завдавати значної шкоди національним інтересам, включно з економічними, оборонними та культурними аспектами. Ці загрози можуть проявлятися у вигляді кібератак, дезінформації, несанкціонованого доступу до критичних даних або маніпулювання суспільною думкою. По-третє, інформація сама по собі є потужним засобом впливу на свідомість і поведінку людей, що підвищує значення її захисту для запобігання маніпуляціям, соціальній дезорієнтації та загрозам демократії. Гарантування інформаційної безпеки є не лише технічним завданням, а й соціально-політичним пріоритетом, який вимагає комплексного підходу, що включає правові, організаційні,

технологічні та освітні заходи. Без належного рівня захищеності інформаційного середовища держави неможливе ефективне функціонування органів влади, економічних структур і громадянського суспільства [20, с.68].

Стратегія національної оборони в умовах гібридної війни повинна базуватися на комплексному підході, що поєднує безпекові, інституційні та соціально-економічні заходи.

Г. П. Мідттун (колишній військовим аташе норвезького посольства в Україні) визначає 4 фактори ефективної стратегічної оборони. Передусім важливим є відновлення довіри між населенням та ключовими державними інститутами – урядом, парламентом, судовою владою, а також засобами масової інформації. Це передбачає підвищення рівня прозорості ухвалення рішень, активне залучення громадянського суспільства до процесів контролю та формування політики, а також гарантії безпеки журналістської діяльності. Водночас критично необхідним є зниження протестного потенціалу суспільства шляхом глибинного реформування судової та законодавчої системи, системної боротьби з корупцією, залучення іноземних інвестицій і зміцнення макроекономічної стабільності, що сприяє підвищенню соціальної згуртованості**.** З огляду на це, стратегія протидії гібридній агресії повинна спиратися на поєднання внутрішніх реформ, інституційного зміцнення та зовнішньої координації, що уможливлює створення стійкої системи національної безпеки, здатної ефективно реагувати на багатовимірні виклики сучасного безпекового середовища [178].

Базовою основою протидії в умовах гібридної війни виступає сильна держава з розвиненими та стабільними інститутами, здатними витримувати зовнішній тиск, зберігати авторитет і забезпечувати безперервне функціонування суспільства навіть у кризових умовах. Інституційна стійкість проявляється у здатності державних органів ефективно реагувати на інформаційні, економічні, політичні та безпекові виклики, що виникають у результаті активних дій противника, включаючи кібератаки, пропаганду та соціально-політичні маніпуляції.

Інформаційна політика під час війни виконує подвійне завдання: захищає державну таємницю та національні інтереси, водночас забезпечуючи прозорість, інформування громадян і підвищення стійкості суспільства [139, с. 18-24].

Оцінка інформаційної безпеки здійснюється через ключові показники, що відображають технологічний рівень захисту, стан інформаційного розвитку суспільства та здатність системи протидіяти загрозам, що дає змогу визначити стійкість, ефективність і потенціал розвитку національної інформаційної системи [105, с.50-52].

Протидія дезінформації в умовах надзвичайних правових режимів є пріоритетом державної політики у сфері національної безпеки. Вона включає комплекс заходів - від кримінального та адміністративного реагування до інституційних механізмів, міжнародної співпраці та просвітницької роботи серед населення. Забезпечення інформаційної безпеки вимагає балансу між захистом національних інтересів і дотриманням фундаментальних прав людини, таких як свобода слова та доступ до достовірної інформації, а ефективна політика протидії фейкам ґрунтується на принципах правової держави, відкритості та відповідальності [345, с 177-179].

Ефективне управління інформаційною безпекою потребує координації між державними органами, правоохоронними структурами, громадськими організаціями та приватним сектором для обміну інформацією, узгодження заходів реагування на загрози та вдосконалення практик безпеки [141, с.53-56].

Ключовими елементами національної системи безпеки, що інтегрують правоохоронні, контррозвідувальні та превентивні функції, зокрема у протидії інформаційним загрозам та кібернетичним атакам, які можуть негативно впливати на суверенітет та стабільність держави виступають: Служба безпеки України (СБУ), Державна служба спеціального зв’язку та захисту інформації України (ДССЗІ), Рада національної безпеки і оборони України (РНБО), Центр стратегічних комунікацій та інформаційної безпеки при Міністерстві культури

та інформаційної політики (ЦСКІБ), Національна рада з питань телебачення і радіомовлення.

Служба безпеки України є державним органом спеціального призначення з правоохоронними функціями, який забезпечує комплексну державну безпеку, дотримуючись прав і свобод людини та громадянина. Основними напрямами діяльності СБУ є протидія розвідувально-підривній діяльності, боротьба з тероризмом, а також забезпечення контррозвідувального захисту державного суверенітету, конституційного ладу та територіальної цілісності. Крім того, СБУ відповідає за охорону оборонного і науково-технічного потенціалу країни, реалізацію заходів у сфері кібербезпеки та інформаційної безпеки держави, а також захист об’єктів критичної інфраструктури [97].

Протягом 2023 року Служба безпеки України системно викривала мережі проросійських інтернет-агітаторів та блогерів, які публічно виправдовували збройну агресію рф, поширювали дезінформацію та брали участь у інформаційно-психологічних операціях ворога. У квітні–травні цього року СБУ повідомила про підозру блогеру Юрію Подоляці, який перебуваючи в росії виступав на пропагандистських телеканалах і поширював фейки через власні канали в YouTube, RuTube та Telegram, а також проросійському блогеру-священнику Андрію Ткачову. Крім того, були ліквідовані ботоферми та міжрегіональні мережі інтернет-агітаторів, які намагалися дискредитувати Збройні Сили України та розпалювати антиукраїнські настрої у різних регіонах країни, зокрема в Києві, Івано-Франківську, Закарпатті, Запоріжжі, Миколаївщині, Одесі, Харкові, Дніпропетровщині та Кіровоградщині.

У червні–листопаді 2023 р. СБУ викрила ще одну мережу з 11 проросійських інтернет-агітаторів у п’яти областях. Серед них були жителі Києва, Миколаєва, Дніпропетровщини, Кіровоградщини, Вінниці, Запоріжжя, Івано-Франківщини та Хмельниччини, а також клірики місцевих храмів та співробітники підприємств критичної інфраструктури. Вони створювали та адміністрували групи у соцмережах, поширювали кремлівську пропаганду, героїзували дії російських військ і закликали до співпраці з окупантами. Всі

підозрювані фігурували у кримінальних провадженнях за статтями Кримінального кодексу України, що стосуються колабораційної діяльності, виправдовування та глорифікації збройної агресії рф, а також порушення територіальної цілісності держави [39; 191; 192; 193; 218; 261; 262; 263; 264; 265; 266; 310].

Діяльність проросійських інтернет-агітаторів та блогерів залишалася однією з ключових загроз інформаційній безпеці України й у наступні роки війни, включно з 2024-2025 роками, і потребувала постійного реагування з боку СБУ та інших державних органів для протидії дезінформації, захисту громадян та підтримки стабільності в умовах триваючої агресії.

Важливим інституційним механізмом протидії інформаційним загрозам виступає Рада національної безпеки і оборони України. У контексті інформаційної безпеки РНБО здійснює функції формування державної політики щодо протидії інформаційним загрозам, моніторингу інформаційного простору та розробки заходів для захисту критично важливої інформаційної інфраструктури. Рада також відповідає за координацію дій у сфері кібербезпеки, протидії дезінформаційним кампаніям, а також за визначення пріоритетів у сфері стратегічних комунікацій та захисту державних інформаційних ресурсів [231].

Відповідно до Статті 22 Закону України «Про національну безпеку України», Державна служба спеціального зв’язку та захисту інформації (ДССЗІ) України є державним органом, відповідальним за функціонування та розвиток державної системи урядового зв’язку та Національної системи конфіденційного зв’язку. Інституція забезпечує формування та реалізацію державної політики у сферах кіберзахисту критичної інформаційної інфраструктури, державних інформаційних ресурсів і конфіденційної інформації, для якої законом встановлено спеціальний режим захисту. До сфери повноважень ДССЗІ належать також криптографічний та технічний захист інформації, регулювання телекомунікацій, використання радіочастотного ресурсу, організація поштового

зв’язку спеціального призначення, а також виконання інших завдань, передбачених законодавством [97].

Національна рада з питань телебачення і радіомовлення України є конституційно визначеним незалежним регуляторним органом, який забезпечує реалізацію державної політики у сфері медіа та аудіовізуальних комунікацій. Діяльність ради спрямована на протидію дезінформаційним та маніпулятивним впливам у медіа-просторі. Орган здійснює моніторинг контенту, оцінює його відповідність державним стандартам, сприяє розвитку професійної етики журналістики і підвищенню медіаграмотності населення [188].

Державний центр кіберзахисту Державної служби спеціального зв’язку та захисту інформації України є державною установою, створеною у 2007 р. в структурі Держспецзв’язку, з часом набув статусу окремої юридичної особи, сформував CERT-UA, інтегрувався у міжнародні мережі кіберзахисту та з 2018 р. має законодавчо закріплені повноваження у сфері кібербезпеки України [112]. Основними завданнями центру є впровадження організаційно-технічної моделі кібербезпеки як складової національної системи кібербезпеки, а також створення та забезпечення функціонування ключових компонентів захисту інформаційних ресурсів. До таких компонентів належать система захищеного доступу державних органів до мережі Інтернет, система антивірусного захисту національних інформаційних ресурсів, механізми аудиту інформаційної безпеки та оцінки стану кіберзахисту об’єктів критичної інформаційної інфраструктури, система виявлення вразливостей і реагування на кіберінциденти та кібератаки щодо об’єктів кіберзахисту, а також система взаємодії команд реагування на комп’ютерні надзвичайні події. Крім того, ДЦКЗ Держспецзв’язку займається розробкою сценаріїв реагування на кіберзагрози, заходів щодо протидії таким загрозам, а також програм і методик проведення кібернавчань у координації з іншими суб’єктами забезпечення національної кібербезпеки [76].

31 березня 2021 р. в інституційній структурі Міністерства культури та інформаційної політики України було сформовано Центр стратегічних комунікацій та інформаційної безпеки як елемент державної інформаційно-

комунікаційної архітектури, спрямований на зміцнення національної стійкості та протидію зовнішнім і внутрішнім інформаційним загрозам. Організаційно-структурною основою Центру є головна редакція, що функціонує як спеціалізований підрозділ у межах Українського національного інформаційного агентства «Укрінформ» та забезпечує вироблення й поширення стратегічно релевантного контенту. Його діяльність охоплює системний аналіз інформаційного середовища, моніторинг ворожих наративів, вивчення вразливих аудиторій і розроблення методів їх захисту. Важливе місце у функціонуванні Центру займає підвищення суспільної обізнаності про інформаційні загрози шляхом створення аналітичних матеріалів, проведення роз'яснювальних заходів та зміцнення комунікаційних спроможностей органів влади. Серед ключових напрямів діяльності ЦСКІБ – формування ефективних контрнаративів, інтеграція українських комунікаційних меседжів у щоденну діяльність урядових інституцій, розвиток міжнародного партнерства у сфері стратегічних комунікацій та спільне напрацювання інструментів протидії гібридній агресії. Значна увага приділяється оперативному інформуванню суспільства через соціальні мережі та цифрові платформи, а також розробці доступних довідкових матеріалів для населення, зокрема щодо алгоритмів дій у кризових ситуаціях [328].

Показовим прикладом такої роботи є проєкт Dovidka.info, який стартував у 2021 р. у вигляді брошури та згодом трансформувався в інтерактивний онлайн-ресурс із матеріалами та чат-ботами у месенджерах Telegram і Viber. Проєкт забезпечує швидке поширення перевіреної інформації, необхідної для захисту життя та безпеки громадян, особливо у прифронтових регіонах і в умовах воєнного стану.

У грудні 2021 р. Центр стратегічних комунікацій та інформаційної безпеки ініціював проведення першого в Україні Kyiv Stratcom Forum, присвяченого питанням стратегічних комунікацій. У заході взяли участь 32 українських та міжнародних експерти, які в ході панельних дискусій обговорювали шляхи посилення співпраці між державними інституціями та громадянським

суспільством з метою підвищення стійкості національного інформаційного середовища та протидії дезінформаційним кампаніям [22].

Після початку повномасштабної агресії російської федерації у лютому 2022 р. ЦСКІБ трансформувався у ключовий елемент державної системи стратегічних комунікацій, який виконує функцію інституційного хабу офіційної інформації про перебіг війни.

Центр стратегічних комунікацій та інформаційної безпеки при МКІП запустив чат-бот @SpravdiBot для виявлення та знешкодження російських фейків. Користувачі можуть надсилати підозрілу інформацію, маніпуляції та ворожі повідомлення [41].

Важливим чинником безпеки також є створення ефективної системи гібридної оборони, що забезпечує одночасну протидію військовим і невійськовим загрозам шляхом синхронізації дій різних секторів державного управління. Для цього доцільним є формування крос-секторальних платформ, які координують зусилля урядових структур, силових органів, приватного сектору та громадських інституцій.

Економічний розвиток держави передбачає її здатність підтримувати належний рівень життя населення, що безпосередньо впливає на соціальну згуртованість та довіру громадян до інституцій. Економічно стабільна держава може забезпечувати регулярні доходи, соціальні гарантії, розвиток інфраструктури та підтримку бізнесу, що зменшує вразливість населення до зовнішніх маніпуляцій. Розвинена економіка також створює сприятливі умови для розвитку промисловості та підприємництва, підвищує інвестиційну привабливість країни та забезпечує ресурсну базу для фінансування оборонних і безпекових потреб. У контексті гібридної війни економічна безпека держави дозволяє протистояти економічним тискам, санкціям та саботажу, а також знижує ризик соціальної дестабілізації, що може бути використана противником для підриву національної безпеки[70].

Одним із фундаментальних завдань сучасної економічної стратегії України є підвищення рівня її стійкості в умовах зростання зовнішніх та внутрішніх

викликів. Це потребує створення комплексу взаємопов’язаних передумов, які умовно поділяються на внутрішні та зовнішні. Внутрішній вимір передбачає скорочення критичної імпортозалежності стратегічно важливих секторів національної економіки, запровадження постійного моніторингу іноземних інвестицій з урахуванням ризиків для економічної та національної безпеки, а також забезпечення фінансової та енергетичної автономії ключових галузей, без яких неможливе стабільне функціонування держави. У зовнішньому вимірі важливими завданнями виступають розширення співпраці з міжнародними партнерами у сфері вироблення та реалізації санкційних механізмів, протидія зовнішньому енергетичному тиску, а також посилення ефективності інтеграційних інструментів у межах міжнародних союзів і організацій, відповідальних за підтримання безпеки .

У перші місяці повномасштабної війни економічна безпека України значною мірою забезпечувалася за рахунок довоєнних фінансово-економічних резервів та наявного ресурсу стійкості, що були доповнені оперативною консолідацією зусиль на національному, регіональному та місцевому рівнях, високим рівнем самоорганізації й соціальної згуртованості громадян перед загрозою російської агресії, а також масштабною та безпрецедентною міжнародною підтримкою [216].

Цілком закономірно, що війна суттєво підриває економічну безпеку України, спричиняючи зниження виробництва, руйнування інфраструктури, погіршення фінансової стійкості та зростання соціально-економічних проблем. Забезпечення стабільності вимагає стратегічного управління ресурсами, стимулювання інвестицій і реалізації реформ, спрямованих на відновлення та підвищення стійкості економіки у післявоєнний період [128; 138; 27].

Підтримка економічної безпеки у період воєнного стану потребує системного й комплексного підходу, що передбачає розробку та реалізацію цілісного комплексу заходів, спрямованих на збереження економічної стабільності та безперервності функціонування господарських процесів. До ключових методів, які доцільно застосовувати, належать: диверсифікацію

економіки, розвиток резервних ринків і джерел енергії, захист критичної інфраструктури, мобілізацію внутрішніх і зовнішніх ресурсів, а також збереження людського капіталу для підтримки стійкості та відновлення економіки [281].

Важливою умовою дієвого протистояння гібридним формам агресії є формування цілісної системи інституційного забезпечення санкційної політики, що поєднує механізми розроблення, узгодження та імплементації економічних обмежень у тісній взаємодії з міжнародними партнерами. Дослідження цього напряму охоплює три аспекти, які доповнюють один одного: по-перше, теоретичний аналіз природи та масштабів загроз економічній безпеці, які виникають унаслідок гібридної агресії; по-друге, узагальнення практичного досвіду застосування санкцій у світовій політиці та оцінку їхньої ефективності для України; по-третє, розроблення науково обґрунтованих рекомендацій щодо вдосконалення національної санкційної стратегії з метою підвищення рівня економічної стійкості держави [86].

У сучасних дослідженнях гібридних конфліктів підкреслюється, що ключова боротьба розгортається у когнітивній сфері, яка охоплює не лише громадян власної держави, але й населення інших країн та територій, де ведуться операції. Основним об’єктом впливу виступає свідомість суспільних груп і політичних еліт, здатних ухвалювати стратегічні рішення. Зміна їхніх уявлень, мотивацій і моделей поведінки розглядається як визначальний чинник досягнення політичних та військових цілей агресора. У цьому контексті традиційні військові ресурси виконують допоміжну функцію, тоді як центральне місце займають інформаційно-психологічні засоби впливу на масову свідомість. [178].

Стратегія і тактика, застосовані рф в Україні, реалізовували ідеї, викладені російськими військовими аналітиками генералом Валерієм Герасимовим, начальником Генерального штабу рф. Він визначив елементи сучасної війни XXI ст., де межі між війною і миром, військовими та підпільними агентами

розмиваються, а головний театр бойових дій переміщується у «серця і уми» населення.

Відповідно до його ідей, основною мішенню стають громадяни, що піддаються впливу пропаганди, які можуть несвідомо або свідомо співпрацювати з противником і використовувати надані ресурси для реалізації його цілей. Такі процеси спостерігалися на Донбасі та сприяли окупації Криму. І хоча фінансові та економічні інтереси держави-агресора у гібридній агресії відіграють значну роль, проте ключовим об'єктом залишається суспільна свідомість. Саме тому ефективна протидія гібридним загрозам передбачає не лише військові заходи, а й розвиток інформаційних кампаній, що не є пропагандою, а спрямовані на донесення реальних результатів реформ і досягнень держави, що може служити надійним механізмом захисту від інформаційних маніпуляцій [227].

Психологічна складова гібридної війни передбачає формування в суспільстві уявлення про необхідність певного політичного вибору та адаптацію громадської думки до зовнішнього впливу.

Ідеологічна стабільність виступає фундаментом духовної та ціннісної єдності держави, знижуючи вразливість населення до психологічних, пропагандистських та інформаційних впливів. Вона ґрунтується на наявності зрозумілої національної ідеї, загальноприйнятих цінностей та конкурентоспроможних ідеологічних концепцій, які відповідають сучасним викликам і можуть бути інтегровані у регіональні та глобальні контексти, наприклад, у цінності демократії та прав людини. До механізмів забезпечення ідеологічної стабільності належать державні комунікаційні кампанії, освітні програми з історії та національної ідентичності, а також публічні дискусії, що сприяють формуванню громадянської свідомості та зміцненню національної солідарності.

Досвід України показує, що громадська стійкість є визначальним чинником протидії такій стратегії. Наприклад, за даними опитувань 2018–2019 рр.,

переважна більшість населення нашої держави зберігала проєвропейські та демократичні орієнтири, попри тривалу агресію з боку рф.

Окрему увагу слід приділити використанню соціальних мереж для збору розвідувальної інформації та проведення кібератак. Як зазначає Ю. Гулак, інформаційна складова гібридної війни передбачає активне застосування соцмереж для збору даних про потенційні цілі та здійснення таргетованих атак [62, с.62]. Це ставить перед державою завдання розвитку ефективних систем кіберзахисту, а також підвищення обізнаності користувачів щодо правил безпечної поведінки в цифровому середовищі, щоб мінімізувати ризики витоку інформації та впливу шкідливого контенту.

Не менш важливим є забезпечення прозорості політичної реклами, що дозволяє контролювати джерела фінансування та цілі поширення політичного контенту, зменшуючи ризики прихованого впливу на громадську думку. Крім того, створення механізмів оперативного видалення шкідливого контенту та блокування акаунтів, які поширюють дезінформацію, є необхідною умовою для підтримання безпечного та надійного інформаційного середовища. Такий підхід дозволяє зменшити вплив інформаційних загроз, підвищити стійкість суспільства до маніпулятивних кампаній і забезпечити ефективне функціонування цифрового інформаційного простору держави.

Важливим напрямком забезпечення інформаційної безпеки є вдосконалення законодавчої бази щодо діяльності соціальних мереж. Це передбачає розробку норм, які визначають відповідальність платформ за поширення дезінформації, гарантують захист персональних даних користувачів та передбачають механізми протидії використанню соціальних мереж для координації протиправних дій [28, с. 30]. При цьому ключовим завданням залишається збереження балансу між безпекою, свободою слова та правом на приватність користувачів, щоб законодавче регулювання не перетворювалося на надмірну цензуру. В цьому контексті, в 2023 р. Кабінет Міністрів України доручив Міністерству культури та інформаційної політики розробити зміни до законодавства, спрямовані на посилення відповідальності за поширення

недостовірної інформації, що формує позитивний образ держави-агресора - російської федерації [132]. Ця ініціатива уряду України передбачає створення чітких правових механізмів для запобігання поширенню дезінформації.

Законодавчі заходи тісно переплітаються із потребою аналізувати та протидіяти психологічному впливу інформаційних кампаній, що особливо актуально у контексті соціальних мереж. У цьому контексті окремої уваги заслуговує проблема психологічного впливу соціальних мереж на користувачів та суспільство в цілому. Як зазначає О. Саєнко, механізми інформаційно-психологічного впливу в умовах гібридної війни активно використовують особливості сприйняття інформації в соціальних мережах [257]. Це включає експлуатацію когнітивних упереджень, застосування емоційно заряджених повідомлень для маніпулювання громадською думкою, а також створення ефекту «інформаційного перевантаження», що знижує критичне мислення користувачів.

Особливу роль відіграє розвиток технологій аналізу емоційного стану користувачів та суспільних настроїв. Вони дозволяють виявляти зародження негативних тенденцій, прогнозувати потенційні соціальні конфлікти та оцінювати ефективність інформаційних кампаній. Це дає змогу державним органам своєчасно реагувати на зміни суспільних настроїв і запобігати розвитку деструктивних процесів.

Особливу увагу слід приділяти проблемі використання соціальних мереж для радикалізації молоді та вербування в екстремістські й терористичні організації. Як зазначають А. Благодарний та О. Штельмах, соціальні мережі створюють сприятливе середовище для поширення радикальних ідеологій та координації дій екстремістських груп [17, с.50]. Це потребує розробки спеціальних програм профілактики радикалізації в онлайн-середовищі, а також ефективних механізмів швидкого виявлення й блокування контенту, пов’язаного з екстремізмом і тероризмом.

Критично важливим для формування стійкості суспільства до інформаційно-психологічних операцій є підвищення рівня медіаграмотності [160, с.156].

Медіаграмотність розглядається як здатність людини усвідомлено сприймати, аналізувати, оцінювати та взаємодіяти з інформацією, що надходить через різні медійні платформи, включно з телебаченням, радіо, друкованими виданнями, Інтернетом та соціальними мережами. У сучасному світі, де обсяг доступної інформації є величезним, а її точність і надійність часто сумнівні, розвиток медіаграмотності набуває особливої важливості. Ця здатність передбачає уміння розрізняти реальні події та віртуальні образи, усвідомлювати, як медіа конструюють уявлення про дійсність, а також критично оцінювати владу, поширювані міфи та засоби маніпуляції інформацією [32, с.70-72].

Як зазначає Н. Войтович, підвищення рівня медіаграмотності та формування навичок критичного сприйняття інформації є одним із найбільш ефективних способів протидії пропаганді під час інформаційної війни [37, с. 298]. Це включає впровадження програм медіаосвіти у школах і вищих навчальних закладах, проведення інформаційних кампаній для різних вікових категорій населення, а також створення онлайн-ресурсів та платформ для самоосвіти у сфері інформаційної безпеки.

Громадяни, які володіють навичками критичного сприйняття інформації, здатні вчасно розпізнавати дезінформацію, маніпуляції та пропаганду, що сприяє зміцненню демократичних інститутів і безпеки держави. Високий рівень медіаграмотності дозволяє не лише протидіяти фейкам у соціальних мережах та мас-медіа, а й сприяє формуванню активної громадянської позиції, відповідального ставлення до поширення інформації та самостійного ухвалення рішень.

Освітній онлайн-ресурс Media IQ, спрямований на підвищення рівня медіаграмотності серед широкого кола користувачів. Платформа пропонує навчальні матеріали та інтерактивні інструменти, які допомагають

користувачам розуміти, аналізувати та оцінювати інформацію з різних медіаканалів, включаючи соціальні мережі, новинні сайти, телебачення та радіо. Основна мета ресурсу полягає у формуванні критичного мислення, здатності розпізнавати дезінформацію та маніпуляції, а також у розвитку навичок безпечної та відповідальної взаємодії з медіапростором. Media IQ також пропонує практичні вправи та кейси, що дозволяють користувачам застосовувати отримані знання на практиці [373].

Систематичне навчання медіаграмотності на всіх рівнях освіти є ключовим елементом формування інформаційно стійкого суспільства. Основна мета впровадження програм з медіаосвіти в школах та вищих навчальних закладах - навчити учнів і студентів оцінювати джерела інформації, розпізнавати маніпулятивні прийоми та критично аналізувати контент у медіа.

Ефективність медіаосвіти напряму залежить від кваліфікації педагогів. Викладачі повинні володіти сучасними методиками викладання медіаграмотності та бути обізнаними щодо актуальних інформаційних загроз. В цьому контексті, на платформі Prometheus, для прикладу, запропоновано курси «Медіаграмотність для освітян» (дає змогу зрозуміти, як працюють медіа, захиститися від інформаційних загроз, але й навчити цього своїх учнів), «CS50: Вступ до кібербезпеки» (нання, отримані під час навчання , дозволять захистити свої облікові записи, дані та системи від сучасних кібернебезпек).

Курс «Цифрова безпека та комунікація в онлайні» спрямований на формування навичок безпечного використання цифрових технологій та ефективної взаємодії в мережі. У рамках курсу розглядаються основи цифрової безпеки та захисту персональних даних, ризики онлайн-комунікацій і методи їх запобігання, безпечна робота з електронною поштою, соціальними мережами та месенджерами, інструменти захисту акаунтів, створення надійних паролів і двофакторної автентифікації, а також алгоритми дій у випадку витоку чи зламу особистої інформації [332; 94].

В Україні щорічно проводиться «Тиждень медіаграмотності», що охоплює різноманітні освітні та інформаційні заходи по всій країні. Ця ініціатива

спрямована на підвищення рівня медіаграмотності населення, розвиток критичного мислення та навичок аналізу інформації, що особливо актуально в умовах масового поширення дезінформації та фейкових новин.

Соціальні мережі та онлайн-платформи відіграють ключову роль у формуванні інформаційного простору та поширенні контенту, що робить їх регулювання важливим інструментом протидії інформаційним впливам та кампаніям дезінформації.

У науковій та практичній площині регулювання таких платформ передбачає комплексний підхід, який охоплює кілька взаємопов'язаних аспектів. Перш за все, важливо встановлювати вимоги до перевірки достовірності інформації, що поширюється, з метою зменшення ризику поширення фейкових та маніпулятивних матеріалів.

Розвиток сучасних технологій відкриває нові можливості для виявлення та протидії інформаційно-психологічним операціям, забезпечуючи автоматизацію процесів моніторингу та аналізу інформаційного середовища.

Штучний інтелект має великий потенціал у сфері інформаційної безпеки, підвищуючи автоматизацію, ефективність і адаптивність захисних систем. Для його безпечного застосування необхідно: впровадити чітку нормативно-правову базу, дотримуватися етичних принципів, забезпечити прозорість алгоритмів і створити механізми зовнішнього контролю. Розвиток ШІ в Україні має базуватися на принципах безпеки, відповідальності та міжнародної співпраці, що дозволить ефективно протидіяти загрозам і підтримувати сталий розвиток цифрового суспільства [149, с. 67-69].

Завдяки застосуванню штучного інтелекту та методів машинного навчання можливо формувати високоефективні алгоритми аналізу як текстового, так і візуального контенту, формувати базу даних перевірених фактів, застосовувати технології обробки природної мови для визначення контексту та смислового навантаження повідомлень, а також інтегрувати систему виявлення фейків у соціальні мережі для оперативного реагування на поширення недостовірної інформації атак [354].

Модернізація алгоритмів стала ключовим елементом сучасних підходів до управління інформаційними потоками у глобальних соціальних мережах. Цей процес передбачає не лише вдосконалення технічних механізмів ранжування та рекомендації контенту, а й переосмислення відповідальності платформ перед суспільством. Як наголошує Sinéad McSweeney, VP of Global Public Policy у Twitter, «нашим найпершим пріоритетом є сприяння безпеці людей у нашому сервісі та за його межами, і наші команди активно працюють над цим». У своєму підході Twitter поєднує дисциплінарні заходи проти контенту, що порушує правила, із системними змінами, спрямованими на зниження видимості потенційно шкідливих матеріалів, які можуть вводити користувачів в оману без додаткового контексту.

Цей підхід демонструє відхід від бінарної логіки «залишити/вилучити» й акцентує увагу на багаторівневому управлінні інформаційним простором. Такі рішення особливо важливі в умовах кризових ситуацій, коли суспільний діалог є вразливим до маніпуляцій. Модерація контенту та алгоритмічне зниження його охоплення суттєво зменшує потенціал дезінформаційних кампаній, одночасно забезпечуючи доступ до достовірних джерел [367]. Таким чином, як бачимо, позиція S. McSweeney відображає ширшу тенденцію у глобальних технологічних компаніях - поступовий перехід від пасивного реагування на порушення до проактивного формування безпечного й інформативного цифрового середовища.

Соціальні мережі та цифрові платформи значно швидше реагують на повномасштабну війну в Україні, ніж під час попередніх криз, і в цілому демонструють кращу готовність до протидії дезінформації. За словами Тетяни Авдєєвої з Лабораторії цифрової безпеки, платформи швидко адаптувалися до нових викликів, а аналітикиня Львівського медіафоруму З. Красовська зазначає, що, попри активну співпрацю з українськими НУО, політика медіаплатформ радше реактивна, ніж проактивна. Е. Брукінґ з DFR Lab підкреслює, що реакція компаній полягає у застосуванні універсальних правил модерації контенту, які можуть працювати і в мирний час [31].

Серед основних ініціатив Meta були обмеження доступу до приватних сторінок у Facebook та Instagram, запуск програми «Data for Good» для передачі даних гуманітарним організаціям, створення Центру спеціальних операцій для модерації українською та російською мовами, маркування фейкових дописів і обмеження сторінок російських провладних медіа, включно з RT та Sputnik у ЄС і Великій Британії.

Війна в Україні має стати поштовхом для розробки системних правил, що передбачають «екстрені заходи» у випадках воєн, повстань чи конфліктів за релігійними ознаками. Twitter видаляв російську дезінформацію про бомбардування лікарні в Маріуполі (за політикою «зловживань» і «заперечення масових жертв»), а YouTube заборонив відео, що применшують вторгнення рф, посилаючись на політику щодо «ненависницького» контенту [375].

Twitter впроваджував модерацію на рівні контенту та акаунтів, зменшував охоплення дезінформації, створював тематичні добірки і тренди для достовірної інформації, маркував посилання на російські медіа, надавав безпекові ресурси кількома мовами та співпрацював із благодійними організаціями. Також були призупинені рекламні функції в Україні та росії, щоб пріоритезувати інформацію про громадську безпеку.

Google та YouTube блокували канали RT і Sputnik у всьому світі, обмежували рекомендації російських медіа, видаляли тисячі відео та надавали понад 150 українським сайтам доступ до сервісу Project Shield для захисту від DDoS-атак. Зокрема, YouTube видалив канал колишньої ведучої підсанкційного телеканалу NewsOne, пов’язаного з Віктором Медведчуком, пропагандистки Діани Панченко, яку підозрюють у державній зраді. Після закриття підсанкційного телеканалу, Панченко виїхала до росії і почала вести власний YouTube-проєкт «ПАНЧЕНКО», де поширювала російську пропаганду. Відео включали сюжети з окупованих українських міст, інтерв’ю з самопроголошеним президентом Білорусі Олександром Лукашенком, а також пропагандистський фільм про життя чеченців у складі рф [10]. З початку повномасштабного

вторгнення служба безпеки Google працює цілодобово для виявлення та блокування підозрілої активності.

В Україні реалізовані декілька прикладів використання технологій для автоматичного виявлення фейків та протидії дезінформації.

Ініціатива Google та Jigsaw в Україні спрямована на розвиток медіаграмотності та протидію поширенню дезінформації в онлайн-просторі, а також на підвищення стійкості громадян до різних форм цифрових маніпуляцій. В її основі лежить концепція prebunking (попереднє розвінчування), яка передбачає превентивне навчання аудиторії виявленню та критичній оцінці маніпулятивного контенту. Реалізація проекту здійснюється у партнерстві з Moonshot та провідними українськими організаціями й експертами у сфері медіа та фактчекінгу, серед яких Центр протидії дезінформації, Vox Ukraine, StopFake, Детектор Медіа, Суспільне та BBC Media Action. Метод prebunking виступає комунікаційною стратегією, що спрямована на формування в користувачів навичок розпізнавання дезінформації та підвищення їхньої медіаграмотності задля більш ефективного протистояння маніпуляціям у майбутньому. Проект Google Jigsaw розробив інструмент Assembler, який використовує AI для виявлення маніпуляцій із зображеннями [16].

Краудсорсинг контенту, для прикладу, передбачає залучення користувачів до створення матеріалів, таких як фото, відео, статті, переклади чи рецензії. Приклади успішного використання краудсорсингу та моніторингу соціальних мереж свідчать про їхню ефективність у гуманітарних і військово-цивільних операціях, оскільки вони забезпечують швидке отримання даних, необхідних для прийняття управлінських рішень і надання допомоги постраждалим у кризових ситуаціях [142].

На оперативну перевірку достовірності інформації та поширення спростувань спрямована розробка спеціалізованих платформ для фактчекінгу. У вітчизняному медіапросторі фактчекінг швидко здобув популярність як методика журналістських розслідувань, відповідаючи на потребу протидії антиукраїнській пропаганді. Ця техніка стала ключовим елементом

контрпропагандистської «оборони» під час інформаційної війни, спрямованої на масштабне та систематичне поширення фальсифікованих новин. До ключових напрямів належать створення централізованих баз даних перевірених фактів, розробка інструментів для краудсорсингового фактчекінгу [37, с.302], інтеграція таких платформ із соціальними мережами та месенджерами, а також створення API для включення фактчекінгу в різні інформаційні системи. Фактчекінг зосереджується на перевірці висловлювань політиків і громадських діячів на предмет їх точності та достовірності.

Інституційно в Україні фактчекінг реалізують низка спеціалізованих платформ та організацій, серед яких «StopFake», «Detector Media», «VoxCheck», «FactCheck.org.ua» та Центр протидії дезінформації при РНБО. Ці інституції систематично перевіряють інформацію, спростовують фейки, аналізують медійну активність та надають рекомендації для підвищення медіаграмотності населення. Вони використовують різні методи перевірки фактів, включно з аналізом первинних джерел, цифровою верифікацією контенту, а також порівнянням із достовірними базами даних [64, с.23].

За словами О. Гороховського, головного редактора ресурсу «FactCheck-Ukraine», фактчекінг є потужним інструментом викриття політичних маніпуляцій і фактичних спекуляцій, забезпечуючи платформу для ґрунтовних розслідувань, що базуються на даних відкритих джерел, і водночас мінімізуючи ризики звинувачень у заангажованості чи суб'єктивності [57, с. 6].

Платформа StopFake використовує як ручну перевірку фактів, так і елементи автоматизованого моніторингу для виявлення фейкових новин, аналізуючи інформацію у соціальних мережах та медіаресурсах (Додаток К) [383]. Основна мета сайту полягає у верифікації інформації, спростуванні неправдивих повідомлень, підвищенні медіаграмотності аудиторії та чіткому розмежуванні фактів журналістики від пропаганди. Проект виступає як інформаційний хаб, де аналізується кремлівська пропаганда у всіх її проявах, а команда StopFake перевіряє, редагує, публікує та поширює матеріали десятьма мовами. Ініціаторами проекту стали викладачі, випускники та студенти

Могилянської школи журналістики. Контент платформи доступний на офіційному сайті, у соціальних мережах, а також транслюється через інтернет-ресурси та місцеві телеканали України, що забезпечує широкий охоплення аудиторії та ефективне протидіяння дезінформації.

«Детектор медіа» в режимі реального часу збирає та документує хроніки кремлівської пропаганди, пов'язані з військовим наступом росії на Україну. За даними дослідження «Детектора медіа», було проаналізовано контент 700 телеграм-каналів, що функціонують у українському сегменті соціальних мереж. У результаті експерти склали перелік із 310 каналів, які визнані проросійськими або такими, що підтримують окупаційні наративи [143].

Станом на вересень 2025 р. редакція «Детектор медіа» зафіксувала значну активність проросійських та окупаційних телеграм-каналів у поширенні дезінформації та маніпуляцій. Загалом було виявлено 2732 випадки фейків, 816 випадків маніпуляцій, 775 повідомлень із пропагандистськими меседжами та 559 випадків викриття дезінформації [23]. Ці дані демонструють масштаб поширення російської пропаганди в українському сегменті телеграма та активність аналітичної роботи щодо її виявлення та документування, що є важливим елементом протидії інформаційним загрозам і формування інформаційної безпеки країни.

«Детектор медіа» повідомляв, що серед сотні найпопулярніших телеграм-каналів в Україні є 11 відверто проросійських, які поширюють маніпуляції та відкрито підтримують росію. Найбільшу аудиторію мають «Анатолий Шарий», «Легитимный», «Резидент», «Дмитрий Василец», «#МОНТЯН!» та «First Новости Войны», а менші канали, як «Шейх Тамир» і «ЗеРада», також демонструють приріст підписників. Частина каналів втратила читачів, проте загалом проросійські блоги залучають все більше росіян.

Окремо «Детектор медіа» виділяє окупаційні канали, націлені на мешканців тимчасово окупованих територій. Старі канали, створені до 24 лютого 2022 року, пов'язані з колаборантами та адміністраціями в Донецькій, Луганській, Запорізькій областях і Криму, деякі мімікрують під медіа. Після 24

лютого виникла нова хвиля каналів, що таргетують новоокуповані території, зокрема Донеччину, Луганщину та Херсонщину, часто у вигляді локальних мереж із назвами «Главное в…» або з приставками _ru/_rus, які репостять контент інших каналів та російські меседжі [143].

Впровадження блокчейн-технологій у медіа може слугувати важливим інструментом для підвищення достовірності інформації та зміцнення довіри до джерел. Ця технологія дозволяє створювати незмінні записи про походження та зміни контенту, що унеможливлює його маніпуляцію після публікації. Основні напрями застосування блокчейну в медіа включають створення децентралізованих систем верифікації новин, використання технології для захисту авторських прав на контент, розробку систем цифрових підписів для підтвердження автентичності інформації та формування блокчейн-реєстрів перевірених фактів. Такі платформи дозволяють забезпечити прозорість та достовірність публікацій, мінімізуючи ризики поширення фейкових або маніпулятивних матеріалів. Наприклад, проект Civil застосовував блокчейн для створення децентралізованої платформи журналістики, що гарантує контроль за походженням інформації та її незмінність.

До ключових аспектів оперативного виявлення та нейтралізації інформаційної атаки належить також створення спеціалізованих підрозділів, які здійснюють безперервний моніторинг інформаційного простору та виявляють потенційні загрози. Важливим є розробка протоколів реагування на різні типи інформаційних атак, що дозволяє чітко визначати алгоритм дій у кризових ситуаціях. Для забезпечення ефективності реагування необхідно налагодити швидкі комунікаційні канали між різними державними органами, що беруть участь у протидії дезінформації.

Проведення спільних навчань та тренінгів для представників різних відомств дозволяє підвищити готовність до реагування в кризових ситуаціях та вдосконалити практичні навички міжвідомчої взаємодії. Крім того, налагодження механізмів співпраці з неурядовими організаціями та медіа

сприяє оперативному поширенню достовірної інформації, що у підсумку зміцнює загальну інформаційну безпеку держави.

Окремої уваги заслуговує проблема використання соціальних мереж для підриву довіри до демократичних інститутів та процесів. Як зазначає О. Радченко, гібридна війна, що активно ведеться в онлайн-просторі, становить серйозну загрозу національному суверенітету [232]. Це потребує розробки комплексних стратегій захисту демократичних цінностей, включаючи забезпечення прозорості політичних процесів, протидію маніпуляціям з громадською думкою та підвищення довіри до державних інститутів.

Проросійські та окупаційні телеграм-канали часто використовують у своїх дописах токсичну лексику, спрямовану на приниження України, дискредитацію української влади та легітимізацію дій росії й окупаційних адміністрацій. Зокрема, у багатьох каналах слово «влада» щодо українських політиків і чиновників майже не вживається; натомість поширене використання терміну «режим» - «київський режим», «український режим», «режим Зеленського» тощо. Аналогічно, замість слова «війна» часто застосовують російський термін «спецоперація», а також поширюються формулювання на кшталт «українська криза» або «український конфлікт».

Під час аналізу контенту аналітики фіксували численні фейки та повідомлення російської пропаганди, які активно поширювали ці телеграм-канали. Такі практики підкреслюють необхідність комплексного моніторингу та аналітичної роботи, що реалізується через системи на кшталт української «Тролесфери», яка дозволяє виявляти і досліджувати активність проросійських ботів та координовані інформаційні кампанії в соціальних мережах [186].

Окремої уваги потребує модернізація Збройних Сил України, спрямована на усунення критичних вразливостей та підвищення їхньої готовності до можливого загострення збройного протистояння.

Забезпечення сил оборони сучасними матеріально-технічними ресурсами, зокрема засобами зв’язку, розвідки та логістики, є критичним для виконання завдань у кризових умовах. До ключових заходів належать оновлення озброєння

та техніки, формування резервних підрозділів і розробка мобілізаційних планів, що гарантують безперервну готовність і обороноздатність військових структур [36; 175].

Важливим аспектом забезпечення інформаційної безпеки в соціальних мережах є розвиток систем раннього попередження про інформаційні загрози, які дозволяють проактивно виявляти та нейтралізувати потенційні ризики. Це передбачає створення механізмів моніторингу та аналізу інформаційного простору для своєчасного виявлення ознак підготовки інформаційних атак, зародження деструктивних наративів або координації протиправних дій [152, с.48]. Завдяки таким системам держава може швидко реагувати на загрози, запобігаючи їхньому розвитку та мінімізуючи можливі наслідки.

Окрему увагу слід приділити використанню соціальних мереж для економічного шпигунства та промислового шпіонажу. Як підкреслює С. Северина, соціальні мережі ефективно застосовуються для збору конфіденційної інформації про компанії та їхніх співробітників [271, с.157]. Це потребує розробки спеціальних програм захисту комерційної таємниці, а також навчання працівників правилам безпечної поведінки у цифровому середовищі.

Важливим є також розвиток механізмів саморегулювання та етичних стандартів у соцмережах. До таких заходів належать створення кодексів поведінки користувачів, систем репутаційної оцінки контенту та механізмів громадського контролю за платформами. Це підвищує відповідальність користувачів і платформ за поширення інформації та створює додатковий бар’єр для дезінформації та шкідливого контенту.

Окремої уваги заслуговує проблема використання соціальних мереж для маніпулювання фінансовими ринками та проведення економічних диверсій. Цілеспрямовані інформаційні кампанії можуть спричиняти коливання фондових ринків, впливати на курси валют та формувати панічні настрої серед інвесторів [362]. Це потребує створення механізмів моніторингу фінансової інформації в соцмережах та координації дій між регуляторами ринків і органами інформаційної безпеки.

Для ефективного протистояння гібридним загрозам, за оцінками експертного середовища, Україні необхідно комплексно реформувати ключові сфери державного управління та безпеки. Серед пріоритетів виділяють викорінення корупційних практик та впливу олігархічних структур, професіоналізацію та модернізацію Збройних Сил України, покращення бізнес-клімату, зміцнення кібербезпеки, зменшення культурно-релігійного впливу російської федерації. Крім того, експерти підкреслюють важливість інтеграції зусиль урядових органів та громадянського суспільства для підвищення обізнаності населення та консолідації громадян у протидії гібридним загрозам на побутовому рівні [227].

Не менш важливим є розвиток систем виявлення та протидії інформаційним операціям, спрямованим на підрив національної ідентичності та єдності. Як зазначає Я. Калакура, у умовах окупаційно-гібридної війни соціальні мережі активно використовуються для маніпуляцій історичною пам’яттю та національними наративами [114, с.79-80]. Це вимагає створення ефективних стратегій формування та захисту національної ідентичності в цифровому просторі, зокрема через розробку позитивного контенту, цифрових платформ для вивчення історії та культури, а також протидію фальсифікаціям історичних фактів.

Особливу увагу слід приділяти відновленню цифрової інфраструктури, яке включає кілька ключових етапів. Перший етап передбачає аудит пошкоджених об’єктів, оцінку збитків і визначення пріоритетів відновлення критичних сфер, таких як енергетика, зв’язок і банківська система. Другий етап полягає у впровадженні сучасних технологій захисту, зокрема штучного інтелекту для виявлення загроз, розширеного шифрування та систем резервного зберігання даних. Третій етап охоплює підготовку кадрів і міжнародну співпрацю, включаючи створення кіберрезерву, залучення експертів, інтеграцію досвіду партнерів і навчання фахівців для протидії майбутнім загрозам [276, с.167-169].

Післявоєнна інформаційна політика має поєднувати демократичні принципи свободи слова з пріоритетами безпеки, забезпечуючи баланс між

відкритістю та стійкістю інформаційного середовища. Для цього необхідно розвивати нормативно-правову базу, забезпечувати координацію між державними органами та громадянським суспільством, підтримувати національний інформаційний продукт, підвищувати цифрову грамотність населення та інтегруватися в міжнародні системи інформаційної безпеки. Людина залишається центральним елементом політики, оскільки її знання, критичне мислення та здатність протидіяти маніпуляціям визначають ефективність захисту інформаційного простору. Усі ці заходи разом формують сталий і безпечний інформаційний простір, що поєднує свободу, відкритість і захист національних інтересів [211, с.94-98].

Глобальний характер сучасних інформаційних загроз зумовлює необхідність активної міжнародної співпраці (зокрема, участь у міжнародних ініціативах, спрямованих на протидію дезінформації) для ефективної протидії інформаційним впливам та психологічним операціям. Важливим елементом є обмін досвідом та кращими практиками з іншими країнами, що сприяє вдосконаленню національних стратегій інформаційної безпеки.

Створення міжнародних механізмів швидкого реагування на транскордонні інформаційні атаки дозволяє оперативно мінімізувати їхній вплив на суспільство та державні інституції.

США не є першою країною, яка намагалася заборонити своїм громадянам користуватися додатком, створеним та належним розробнику з іншої держави з міркувань безпеки. Китай та інші держави успішно ухвалили закони, які обмежують доступ громадян до певних іноземних додатків. Щоб оцінити наслідки реалізації таких заборон та визначити, чи вони обґрунтовані, необхідно розглянути різні заходи, які країни світу застосовували у відповідь на реальні чи уявні загрози іноземних технологій, а також витрати, пов’язані з їх впровадженням.

В США боротьбу з дезінформацією здійснюють Агентство з кібербезпеки та захисту інфраструктури (CISA) і Федеральне бюро розслідувань (FBI). CISA відповідає за захист критично важливої інфраструктури від іноземного впливу

та кіберзагроз і має спеціальну команду для протидії місінформації, дезінформації та малінформації, зокрема у соціальних мережах. ФБР зосереджується на виявленні та припиненні операцій іноземного впливу, інформує платформи соцмереж про потенційні кампанії дезінформації, зокрема діяльність російської “фабрики тролів”, та подає запити на видалення неправдивого контенту, частково реалізовані соцмережами.

У 2016 р. в США було створено Центр глобальної взаємодії Державного департаменту, спочатку для боротьби з тероризмом, а згодом – для протидії іноземній пропаганді та дезінформації, що може впливати на політику, безпеку та стабільність країни та її союзників.

У Швеції функціонує система цивільної оборони, яка передбачає оперативне реагування на інформаційні атаки, особливо в умовах кризових ситуацій, що сприяє підвищенню стійкості суспільства до дезінформації. У відповідь на загострення воєнної загрози в Європі через вторгнення рф в Україну, уряд Швеції 1 жовтня 2022 р. розпочав комплексну реформу системи цивільної готовності. Метою реформ є зміцнення стійкості держави в кризових ситуаціях мирного часу та підвищеного ризику конфліктів, зокрема шляхом налагодження ефективних вертикальних і горизонтальних організаційних зв’язків між цивільними та військовими органами управління [384].

Міжнародні організації, зокрема, ОБСЄ, також відіграють важливу роль у протидії маніпуляціям. ООН формує рекомендації для держав щодо безпечного використання інформаційних технологій та координації міжнародних зусиль у боротьбі з дезінформацією. Вагому роль у протидії інформаційним загрозам і гібридним атакам відіграє НАТО. Альянс визнає інформаційний простір як стратегічно важливу сферу безпеки та інтегрує заходи з протидії дезінформації, пропаганді та кібератакам у свою загальну концепцію колективної оборони. НАТО активно взаємодіє зі ЗМІ та підтримує публічні інформаційні канали для спростування фейків [250].

Алгоритм взаємодії з соціальними мережами за системою НАТО передбачає комплексний підхід, що включає розроблення стратегії, управління

платформами, перевірку публікацій, залучення аудиторії, політику публікацій, оцінку ефективності та позиціювання інституції. На першому етапі розробляється стратегія соцмереж, синхронізована зі стратегією стратегічних комунікацій інституції, із створенням відкритого та цікавого контенту, ключових меседжів і динамічних публікацій. Другий етап охоплює управління платформами: визначаються відповідальні співробітники, розробляється комунікаційний план із завданнями, аудиторією, типом і частотою публікацій та політикою коментарів. Третій етап передбачає перевірку матеріалів на відповідність офіційній позиції, актуальність і погодження, а також оптимізацію процесу затвердження. На четвертому етапі забезпечується залучення аудиторії через двосторонні комунікації, баланс інституційного та розважального контенту, принцип «відкритих дверей» і інноваційні методи взаємодії. П’ятий етап стосується політики публікацій: положення про використання ресурсів, аналіз аудиторії, зворотний зв’язок та актуальні контакти. Шостий етап включає оцінку ефективності кампаній за допомогою комплексних метрик залученості, участі та охоплення. Сьомий етап передбачає визначення жанрів і позиціювання інституції: офіційні сайти координуються відділом зв’язків з громадськістю, блог керівника інформує про цілі та пріоритети, Facebook і Twitter використовуються для комунікації пріоритетів, молодший персонал висвітлює успіхи, а YouTube залучає ширшу аудиторію. Додатково рекомендовано консультуватися з керівництвом перед публікаціями, обережно висловлювати особисту думку та зазначати відповідальність за комунікації [290, с.249-252].

Протидія гібридним загрозам є пріоритетом НАТО, що реалізується через розвідку, обмін інформацією між членами Альянсу та впровадження спеціальних підрозділів для моніторингу і аналізу гібридних дій. Важливим елементом є інтеграція гібридних сценаріїв у військові та політичні навчання, що дозволяє відпрацьовувати механізми реагування на різні види загроз. Підвищення стійкості цивільної інфраструктури визнається критичною умовою ефективності військових операцій, а національні уряди несуть основну відповідальність за забезпечення цього аспекту безпеки. Кіберзахист і розвиток

цифрових стратегій є ключовими напрямами протидії, включно з державно-приватним партнерством у сфері кібербезпеки.

У 2016 р. засновано платформу НАТО–Україна, яка функціонує як механізм обміну інформацією про російську гібридну тактику та сприяє розробці інструментів для зміцнення національної стійкості та захисту стратегічно важливих сфер безпеки. 21–22 листопада 2023 р. у Кишиневі (Молдова) відбулася спільна зустріч українських та молдавських експертів, присвячена обговоренню гібридних загроз, що посилилися після повномасштабного вторгнення росії в Україну, підвищенню спроможності України та Молдови запобігати гібридним атакам і реагувати на них. Консультації зосереджувалися на стратегічних комунікаціях, протидії дезінформації, розвитку міжурядового співробітництва, зміцненні енергетичної безпеки та захисті критичної інфраструктури. За словами керівника Бюро зв'язку НАТО в Молдові М. Шимакової, концентрація фахівців дала можливість виявити та проаналізувати спільні ризики для обох держав [187].

Міжнародні проєкти у сфері протидії інформаційним загрозам слугують важливим прикладом для розробки ефективних стратегій і механізмів захисту інформаційного простору. Такі ініціативи, як проєкт «Протидія іноземному втручанню» (CFI) під керівництвом Європейського інституту безпеки (EUISS) (запущений 1 січня 2023 р.) демонструють комплексний підхід до виявлення, аналізу та протидії іноземній інформаційній маніпуляції. Вони поєднують наукові дослідження, розробку методологій, створення аналітичних інструментів і міжнародне партнерство, залучаючи університети та дослідницькі центри. Зокрема, проєкт спрямований на посилення спроможностей ЄС у виявленні, аналізі, оцінці та реагуванні на загрози в інформаційному просторі [356]. Проєкт «Медіамости: Фінляндія та Україна» створений з метою адаптації найкращих міжнародних практик медіаграмотності до українських реалій, спрямований на підвищення довіри населення до медіа та формування основ для розумного суспільного діалогу, розвитку критичного мислення і свідомого сприйняття інформації. У сучасних умовах війни,

масового поширення фейкових новин та інформаційного перевантаження медіаграмотність стає не лише корисною навичкою, а й важливим інструментом безпеки, який захищає громадян від дезінформації [239].

Проєкти не лише посилюють стійкість окремих держав і регіонів до інформаційних загроз, але й сприяють формуванню глобальних стандартів реагування, обміну досвідом та кращими практиками. Вони слугують моделлю для інших країн та організацій, показуючи, як системно і координовано можна запобігати інформаційній маніпуляції, захищати демократичні цінності та підтримувати міжнародну безпеку

Медіаграмотність у світі розглядається як ключовий інструмент протидії дезінформації, фейковим новинам та інформаційним маніпуляціям. Різні країни застосовують різні підходи, поєднуючи освітні програми, державні ініціативи та міжнародну співпрацю.

У Фінляндії медіаосвіта є обов'язковою складовою шкільної програми з початкових класів. Вона спрямована на розвиток критичного мислення, інформаційної грамотності та навичок аналізу медіаконтенту. Учнів навчають розпізнавати фейкові новини, перевіряти джерела інформації та оцінювати достовірність повідомлень у різних медіа, включно з соціальними мережами [236].

Міністр освіти Фінляндії Андерс Адлеркройц підкреслив у інтерв'ю AFP, що «…медіаграмотність має важливе значення для формування стійкості суспільства, і Фінляндія усвідомила це досить рано», що відображає стратегічний підхід країни до розвитку інформаційної грамотності серед громадян [86].

Окрему увагу в Фінляндії приділено також цифровій грамотності: школярів знайомлять із принципами роботи алгоритмів, механізмами поширення інформації в інтернеті та методами захисту персональних даних. Вища освіта та програми для дорослих підтримують ці зусилля через курси з медіаосвіти, семінари та публічні кампанії [51; 87].

Фінська модель протидії дезінформації базується на профілактичному підході: замість жорсткого державного регулювання контенту держава робить акцент на формуванні у громадян умінь критично оцінювати інформацію. Завдяки цьому фінське суспільство вважається одним із найбільш стійких до дезінформації у світі, а громадяни демонструють високу здатність відокремлювати достовірні новини від маніпулятивних чи фейкових повідомлень.

Крім того, уряд Фінляндії підтримує міжнародне співробітництво у сфері боротьби з дезінформацією, обмінюючись досвідом з іншими країнами та міжнародними організаціями, що працюють над підвищенням медіаграмотності населення та стійкості суспільства до інформаційних загроз.

Аналіз практики Європейського Союзу та НАТО у сфері протидії гібридним загрозам, спричиненим діями російської федерації, дозволяє виокремити три основні напрямки реагування, що забезпечують комплексний підхід до безпеки: визнання фактів атак та їх публічне оголошення для забезпечення прозорості, консолідації союзників і внутрішньої мобілізації; підвищення стійкості національних систем через захист критичної інфраструктури, розвиток кібербезпеки, удосконалення стратегічних комунікацій і медіаграмотності населення, а також інтеграцію цивільних і військових ресурсів; формування стратегії стримування, що поєднує можливість реальної відплати з дотриманням міжнародного права і етичних норм, включає санкційні та інформаційні заходи і дипломатичний тиск, забезпечуючи баланс між демонстрацією сили і запобіганням ескалації конфлікту [280].

Згідно з доповідями ЄС і НАТО та результатами розслідування парламенту Великої Британії, ефективна протидія гібридній війні передбачає три ключові кроки:

1. Визнання фактів атак і їх публічне оголошення, що дозволяє консолідувати союзників і сформувати спільне розуміння загроз.

2. Зміцнення національної стійкості, включаючи захист критично важливої інфраструктури, кібербезпеку та підвищення медіаграмотності населення для протидії дезінформаційним кампаніям.

3. Стратегія стримування та потенційної відплати, яка передбачає адекватну реакцію на гібридні атаки без застосування незаконних або неетичних методів, що використовуються росією. До можливих заходів відноситься обмеження візового руху для російських дипломатів, інформаційні кампанії всередині рф та посилене патрулювання стратегічних об’єктів.

Водночас західні експерти відзначають високий рівень непередбачуваності російських дій і асиметричний характер атак, що ускладнює вироблення відповідної стратегії.

Досвід ЄС і НАТО підтверджує, що ефективна протидія гібридній війні можлива лише за умов багаторівневого і інтегрованого підходу. Поєднання превентивних, захисних і стримуючих заходів дозволяє створити комплексну систему реагування, де цивільні та військові інструменти взаємодіють для забезпечення стабільності. Крім того, важливим аспектом є адаптивність стратегій: гібридні загрози постійно еволюціонують, і ефективне реагування вимагає швидкого оновлення даних, аналітичної оцінки та координації дій між державами-союзниками.

Такий підхід демонструє переваги інтегрованих стратегій безпеки, зокрема:

- можливість раннього виявлення загроз;
- зниження впливу дезінформаційних кампаній;
- підвищення ефективності стримування агресора без прямої ескалації конфлікту;
- формування загальної культури безпеки серед союзників.

Отже, ефективна протидія гібридній війні потребує комплексного підходу, який інтегрує правові, оперативні та політичні інструменти. Зокрема, правова складова забезпечує нормативне регулювання дій державних органів та визначає механізми відповідальності за інформаційні та кіберзлочини.

Оперативні заходи спрямовані на своєчасне виявлення загроз, моніторинг інформаційного простору та забезпечення безпеки критично важливої інфраструктури, включно з транспортними, енергетичними та комунікаційними мережами. Політичні інструменти передбачають координацію дій між державними структурами, міжнародними організаціями та партнерами, а також ефективну комунікацію з населенням для підвищення стійкості громадян до інформаційного впливу. Міжнародне співробітництво з ЄС і партнерами, зокрема країнами з досвідом тотальної оборони, підсилює колективну здатність реагувати на гібридні загрози. Протидія гібридним викликам виступає довгостроковим стратегічним завданням, що вимагає динамічного підходу до аналізу та реагування на різні сценарії та окремі дії агресорів у сучасному безпековому середовищі. Такий комплексний підхід дозволяє мінімізувати ризики дестабілізації ключових об’єктів, забезпечити захист стратегічних ресурсів і сприяти загальній національній безпеці.

3.2. Аналіз ключових кейсів інформаційного впливу на Україну (2014–2025 рр.).

Аналіз ключових кейсів інформаційного впливу на Україну (2014–2025 рр.) неможливий без урахування політико-історичних передумов, які сформували середовище для сучасних гібридних загроз. Кінець 1990-х років став переломним етапом для росії та всієї пострадянської просторової системи. Поступове послаблення демократії, зростання авторитарних тенденцій та відродження імперських амбіцій у кремлі створили підґрунтя для ревізіоністської політики, спрямованої на обмеження суверенітету сусідніх держав і збереження їх у сфері російського впливу. Україна, яка на той час перебувала у процесі пошуку власного геополітичного курсу між Заходом і Сходом, ставала дедалі важливішим об’єктом політичного, економічного та інформаційного тиску. Саме в цей період почали формуватися механізми

пропаганди, інформаційних операцій та контрольованих медіа, які у наступні десятиліття були використані проти української державності.

Період приходу Владіміра Путіна до влади (1999 р.) позначив собою початок етапу ревізіоністської політики росії, спрямованої на відновлення статусу так званої «великої держави» та повернення впливу на пострадянському просторі.

Розпад СРСР у російському офіційному дискурсі названо «найбільшою геополітичною катастрофою XX століття», Стратегічний курс було взято на централізацію влади, зміцнення силових структур і відновлення глобальних амбіцій, що, в сою чергу, призвело до реалізації масштабних програм модернізації армії, спецслужб та медійної сфери. Паралельно відбувалося конструювання наративу «відновлення могутності Росії», який апелював до часів Петра I та культу Сталіна, інтегруючи ідеї слов'янської єдності й «цивілізаційної місії росії» [29].

В інформаційній площині росія почала системно використовувати пропаганду, мас-медіа як елемент комплексної гібридної стратегії впливу. Ця політика мала подвійний характер: з одного боку – спрямована на утримання контролю над внутрішнім простором шляхом конструювання лояльної суспільної свідомості, з іншого – на перешкоджання інтеграції сусідніх держав у західні політичні, економічні та безпекові структури (ЄС, НАТО). У такий спосіб інформаційний вплив став інструментом підтримання легітимності чинного режиму та ключовим компонентом зовнішньої політики.

російська федерація систематично аналізувала досвід військових операцій своїх союзників та інших держав з метою вдосконалення власного військового планування та адаптації його до умов сучасних конфліктів. Перед початком інформаційної кампанії проти України. росія врахувала уроки власних помилок, отримані під час Першої (1994–1996 рр.) та Другої (1999–2009 рр.) чеченських війн, аварії підводного човна «Курськ» у 2000 р., терористичного акту у Беслані 2004 р. та війни з Грузією у 2008 р. Ці події сформували у російської владної еліти розуміння організації ефективних інформаційних кампаній [351].

Ще у 2012 р. «The Guardian» повідомила, що проросійська група управляє мережею інтернет-тролів, створює план дезінформації та дискредитації опозиційних активістів і ЗМІ.

Період 2014–2015 рр. став переломним етапом в політичній історії України з точки зору інформаційного протистояння російській федерації.

На ранньому етапі акцент робився на економічній нестабільності та ризиках тісніших зв'язків з ЄС, а згодом, під час загострення Євромайдану, – на загрозах для російськомовного населення Східної України, що включало демонізацію націоналістичних радикалів, страх перед конфіскацією майна та обмеженням мовних прав, і таким чином сприяло консолідації проросійських настроїв та легітимації політики Кремля. Попри риторику про нібито «братні народи», російська зовнішня політика (в тому числі концепція євразійства О. Дугіна) та медійна практика демонстрували ієрархічне ставлення до України, де права українців на самовизначення систематично ігнорувалися, українська державність та прагнення інтегруватися з Заходом применшувалися, культурно-історичні досягнення України замовчувалися або спотворювалися.

Відмова президента Януковича підписати Угоду про асоціацію з ЄС у листопаді 2013 р. стала сигналом для Москви про можливість економічного і політичного тиску на Україну та активізувала інформаційні кампанії рф, спрямовані на легітимізацію свого впливу та формування проросійських настроїв у суспільстві [287].

російська держава здійснювала спроби контролювати соціальні мережі, блокуючи доступ до проукраїнських джерел та запитуючи інформацію про учасників Євромайдану на сайті ВКонтакте. Також були випадки звільнення редактора популярного російського інтернет-ресурсу Lenta.ru та директора ВКонтакте з наступною заміною на лояльних Кремлю осіб. Вищі кола російської влади культивують численних блогерів і тролів через адміністрацію президента, щоб поширювати наратив росії та придушувати опозиційні голоси.

Після Революції Гідності російська федерація розгорнула широкомасштабну гібридну війну, що поєднувала військові, політичні,

економічні та інформаційні компоненти. Інформаційна складова цієї війни мала особливе значення, оскільки вона була спрямована як на внутрішню аудиторію України, так і на міжнародне співтовариство.

Російський наратив включає кілька домінуючих тем. По-перше, росія протиставляє власну слов'янську православну цивілізацію «занепадаючій» Європі. По-друге, Україну позиціонують як складову євразійської концепції та важливий елемент створення Євразійського економічного союзу. По-третє, концепція «русского міра» - це ідеологічний конструкт російської державності, що від часу концепту «Москва – третій Рим» до сучасного рашизму легітимізує імперські амбіції, експансіонізм та культурну асиміляцію сусідів, заперечуючи самостійність української ідентичності й використовуючи історію, православ'я та міф про «триєдиний народ» як інструменти політичного, культурного й військового панування [49].

За словами Патріарха Кирила, спільне використання російської мови, культурна спадщина та історична пам'ять об'єднують ці країни, а Україна є ключовою для концепції «русского міра». Доктрина «русского міра» поширюється через гнучку систему стратегій, що варіюються від євразійсько-цивілізаційного дискурсу для неслов'янських народів рф, етнонаціоналістичного – для «російськомовних співвітчизників» та інтернаціонал-соціалістичного чи квазідемократичного – для західних суспільств, і головним полем її просування та протидії на теренах України є простір символічного, де боротьба точиться у площині історичної пам'яті, реальної соціальної комунікації та стратегічного моделювання українського майбутнього на власному ціннісно-онтологічному ґрунті [82].

Окрім того, українців зображують як неспроможний народ, який не здатен самостійно забезпечити державність. Значну роль відіграє апеляція до історичних подій, зокрема до великої вітчизняної війни, з метою мобілізації антинацистських настроїв та дискредитації учасників Євромайдану, яких маркують як націоналістів, нацистів і фашистів.

У процесі досягнення політичних та військових цілей росія масово використовувала дезінформацію, інформаційно-психологічні операції, активність у соціальних мережах, пропаганду через англомовні та російськомовні супутникові телеканали, а також застарілі радянські методики, такі як активні заходи та рефлексивне управління.

Особливу цінність для нас представляє Звіт Центру передового досвіду НАТО з стратегічних комунікацій (StratCom COE), підготовлений Е. Ланге-Йонатамішвілі на основі системного аналізу відкритих джерел інформації та експертних висновків, отриманих під час обговорень, що відбулися 8 травня та 17 червня 2014 р. Звіт аналізує інформаційну кампанію росії проти України, охоплюючи період від Третього саміту Східного партнерства у Вільнюсі (28–29 листопада 2013 року) до анексії Криму (16 березня 2014 року) [351]. рф відбувалося активне використання соціальних мереж як інструменту масового впливу. «Російські боти» у Facebook, Twitter та ВКонтакте поширювали фейки про «фашистську Україну», «злочини українських батальйонів» та «знищення мирного населення на Донбасі». Ця діяльність мала дві основні мети: вплив на громадську думку населення України та формування негативного іміджу країни за кордоном. За даними аналітичного центру Atlantic Council, тисячі автоматизованих акаунтів використовувалися для масового репосту проросійських матеріалів, створюючи враження широкої підтримки росії та невдоволення новою українською владою. Як відзначають у звітах НАТО та OSCE, ці інформаційні кампанії спрямовувалися на формування у міжнародної спільноти спотвореного уявлення про події в Україні та легітимізацію дій рф на південно-східному кордоні України.

У період з 15 квітня по 15 липня 2014 р. НАТО StratCom COE проаналізував понад 26 тисяч твітів російською мовою щодо ситуації в Україні, включно з Кримом, використовуючи ключові слова, пов’язані з кризою, а дані збиралися за допомогою інструменту WebRadar. Результати дослідження показали високу поляризацію між користувачами, які підтримували Україну, та проросійськими акаунтами, при цьому 12,2% твітів мали агресивний характер, а

провокаційні коментарі зростали під час загострення конфлікту, переважно з проросійською позицією. Проросійські акаунти мали більший вплив завдяки активному використанню акаунтів ЗМІ для поширення інформації про кризу, домінуванню однорідних думок, що підтримували політику Путіна, частково через контроль держави над опозиційними медіа, а також значній підтримці з боку державних інституцій, громадських організацій та відомих публічних осіб, тоді як винятком були представники Євромайдану, які мали помітний вплив через ретвіти та підписників. Проросійські користувачі виявляли більшу активність: коментували, закликали до дій, поширювали пропаганду та втручалися в дискусії, а дослідження також виявило мережі фейкових акаунтів, які координовано поширювали однакові повідомлення, створюючи видимість широкої дискусії.

Одним із ключових кейсів цього періоду стала анексія Криму та події на Донбасі. російські інформаційні ресурси активно поширювали наративи про «захист російськомовного населення», «незаконні дії Києва» та «прагнення кримчан до возз'єднання з Росією». Пропаганда супроводжувалася масовою дезінформацією, включно з фейковими новинами про «народне волевиявлення» на псевдореферендумі в Криму, що мало легітимізувати окупацію півострова на міжнародній арені.

У ході реалізації інформаційної кампанії проти України було створено єдину та скоординовану редакційну політику, яка підтримувала дії російського уряду та поширювалася через численні медіа-канали, що свідчить про централізоване управління контентом. Контрольовані проросійськими структурами медіа та телеканали, такі як «Росія 24», «НТВ» та LifeNews, активно формували громадську думку щодо ситуації в Україні з перших днів, забезпечуючи скоординоване та централізоване поширення пропагандистських меседжів, поширювали матеріали, що дискредитували Збройні Сили України, зображуючи їхні дії як «насильство над цивільними» та «злочини проти власного населення».

Журналісти державних російських ЗМІ методично маніпулювали відео- та фотоматеріалами для візуального підтвердження основного наративу, включаючи використання кадрів із конфліктів у Сирії, Косово та Чечні як ніби вони були зроблені на сході України. Ці методи виявилися особливо ефективними у соціальних мережах. Серед практик фальсифікації можна відзначити багаторазове використання однієї і тієї ж особи для демонстрації різних ролей - «кримський активіст», «мешканка Києва», «мати солдата», «мешканка Одеси», «мешканка Харкова», «учасниця Антимайдану» та «переселенка з Донецька» [348]. У всіх ролях ці люди транслювали повідомлення, які підкріплювали певну лінію наративів, наприклад, що «США та Захід є агресивними та слабкими», «Крим належить історично Росії», а «Росія - священна православна цивілізація». Такі методи значно посилювали основне завдання російських медіа - радикалізацію політичної опозиції та дискредитацію Заходу.

Строгий контроль над медіа здійснювався не лише всередині росії, а й на території Криму. Вже після появи озброєних груп у кримських містах події продемонстрували особливу роль російських телеканалів. 6 березня 2014 р., за десять днів до проведення кримського референдуму, озброєні особи увірвалися до будівлі Сімферопольської радіо- та телевежі, що призвело до припинення трансляцій українських телеканалів. Їх замінили російські канали: Inter - на NTV, 1+1 - на Перший канал. У вікно каналу «Чорне море» кинули коктейль Молотова, а вебсторінка каналу зазнала DDoS-атаки [145].

У статті Е. Рейхборна-К'єннеруда та Патріка Кулена «Що таке гібридна війна» автори підкреслюють, що ключове поле бою сучасної гібридної війни знаходиться у когнітивному просторі. Цей простір охоплює як населення власної країни, так і громадян інших держав, а також населення територій, де відбуваються операції. Унаслідок цього центром спрямування зусиль стають не військові формування та фізичні об'єкти, а саме свідомість і сприйняття ключових груп населення та політичних акторів, що приймають рішення [178]. Саме вони постають основною ціллю гібридних операцій, оскільки зміна їхніх

уявлень, мотивацій та поведінки має стратегічне значення для досягнення політичних і військових цілей агресора. Таким чином, населення перетворюється на головний фокус гібридного впливу, а традиційні військові ресурси виконують допоміжну роль у підтримці цих операцій.

За даними Центру національного спротиву, на тимчасово окупованих територіях України російські окупаційні адміністрації посилюють інформаційно-психологічний тиск на місцеве населення, примушуючи до споживання кремлівської пропаганди та нав'язуючи канали супутникового телебачення «русскій мір» під загрозою вилучення приватного обладнання [249].

Водночас у східних регіонах України активно застосовувалися механізми залякування та психологічного тиску через інтернет і місцеві медіа. Це включало публікацію «чорних списків», маніпулятивних статей та відеоматеріалів, що мали на меті дестабілізацію регіональної ситуації та посилення розколу в суспільстві.

Події в Криму та на сході України демонструють, що навіть невелика група осіб, яка отримує значну військову та інформаційну підтримку, може становити серйозну загрозу для безпеки та стабільності держави.

У ході інформаційної кампанії росія прагнула продемонструвати, що її дії були спрямовані на підтримку волі місцевого населення та самооборонних груп в Україні, при цьому активно використовувався наратив «історичної російської присутності» для легітимізації інтересів та діяльностірРосії на територіях із історичною присутністю росіян; Крим характеризувався як історично російська земля, а Севастополь - як російське місто, при цьому президент Путін наголошував, що ця переконаність у належності Криму росії існувала у свідомості людей і передавалася з покоління в покоління.

Сучасна гібридна війна, яку росія веде проти України та її союзників, характеризується комплексним застосуванням як військових, так і невійськових методів впливу.

Після окупації Криму значно зросла активність російських тролів. Основні завдання тролів: дезінформація, поширення чуток чи фальшивих фактів, активне втручання у дискусії та масове розміщення повідомлень на тематичних веб-платформах. Масовий набір тролів передбачав щоденне розміщення великої кількості коментарів, підтримку кількох акаунтів у Facebook і Twitter, залучення нових підписників та участь у дискусіях. Однією з кампаній була так звані «ввічливі люди», що просувала вторгнення з фотографіями російських військових поруч із дітьми, літніми людьми та тваринами. Війна в Криму відбувалася без офіційного оголошення. Під час формально мирного часу невеликі групи російських військ швидко окупували півострів, змушуючи українських військових або переходити на бік російських сил, або залишати свої пости.

Безіменні «ввічливі люди» у нових, непозначених формах з'явилися на аеропорту Сімферополя 28 лютого 2014 р., а до кінця наступного дня оточили ключові урядові будівлі, блокували прикордонні пости та встановили контрольні пункти по всьому Криму [33]. Вони запевняли журналістів, що перебувають там для захисту, охорони та запобігання насильству. Хоча зброя і техніка були російськими, спершу Москва заперечувала будь-який зв'язок із цими силами. Пізніше, вже після анексії, Путін визнав присутність російських військ для підтримки місцевих самооборонних груп, що демонструє ефективний психологічний тиск російських спецпідрозділів. Додатковий тиск створювали раптові навчання та перевірки боєготовності російських сил на кордоні. Соціальні мережі також використовувалися для вербування проросійських бойовиків у Східній Україні.

Основні наративи російської пропаганди включають: звинувачення України в нацизмі, нібито заборону російської мови, неправдиві повідомлення про контрабанду та неправильне використання західної зброї, маніпуляції щодо евакуації населення та гуманітарних коридорів, звинувачення українських військових у ризику для цивільного населення, а також фейки про «брудну

бомбу», зберігання боєприпасів на атомних станціях чи діяльність біолабораторій [133].

Відомі приклади показують навмисне фабрикування інформації, використання фейкових акаунтів [111, с.64]. і поширення чуток з метою створення страху або ненависті.

- **«Доктор з Одеси»**: фальшивий акаунт у Facebook нібито належав лікарю Ігорю Розовському, який, за повідомленням, намагався допомогти жертвам пожежі в Будинку профспілок в Одесі, але нібито був заблокований «проукраїнськими екстремістами». Пост швидко поширювався у Vkontakte та перекладався іншими мовами, поки журналісти не виявили, що фото лікаря взяте з рекламного буклету стоматологічної клініки на Північному Кавказі.
- **Фото вагітної жінки в Одесі**: широка циркуляція зображення вагітної, нібито задушеної проукраїнськими екстремістами, припинилася після розслідування KyivPost, що довело його фальсифікацію.

В українському інформаційному просторі сфабриковані або маніпулятивні новинні повідомлення створюють плутанину щодо надійності джерел інформації. Зокрема, дипфейки відомих політичних і військових діячів, згенеровані штучним інтелектом, спрямовані на вплив на громадську думку, закликаючи до капітуляції або зменшення підтримки військових зусиль [16].

Серед прикладів дезінформації – історії про нібито злочини проукраїнських екстремістів на Сході України: отруєння водопостачання, створення концентраційних таборів, приховані загони фашистів у лісах та циркуляри з отрутою, яку можна отримати дотиком. Одним із яскравих прикладів є сюжет російського каналу Channel One, у якому нібито описувався випадок катування і розп’яття трирічного хлопчика українською армією в центрі Слов’янська [279]. Відео активно поширювалося у соціальних мережах, але розслідування незалежних журналістів, включно з російським телеканалом Dozhd, довело його фальсифікацію: місцеві жителі Слов’янська не підтвердили фактів, описаних у сюжеті.

Успішне поєднання ідеологічної бази, традиційних медіа та розвиненої мережі користувачів Twitter стало ключовим фактором впливу в соціальних мережах.

«РИА Новости» послідовно виступало як провідний канал поширення радикальних ідеологічних установок російської влади: у травні 2021 р. на його шпальтах з'явилася стаття Тімофєя Сєргєйцева «Яка Україна нам не потрібна», яка фактично обґрунтовувала майбутню збройну агресію, а у квітні 2022 р. була опублікована його ж стаття «Що Росія має зробити з Україною», що окреслювала програму геноцидного характеру, включно з ліквідацією української державності, масовими репресіями та знищенням національної ідентичності. Ці матеріали отримали широкий резонанс, стали доказовою базою для міжнародних досліджень злочинів росії та призвели до запровадження санкцій проти автора. Особливе значення мала й дата публікації: напередодні російська влада заявила про нібито готовність до «переговорів на вищому рівні», попри триваючі ракетні удари по цивільних об'єктах України, що демонструвало подвійність російської дипломатії та узгодженість інформаційних і силових методів тиску.

З початком повномасштабного вторгнення рф тиск на свободу в інтернеті в росії та на окупованих територіях України різко посилився: у 2022 р. Роскомнагляд заблокував Facebook, Instagram, Twitter, запровадив кримінальну відповідальність за "фейки" про армію та "дискредитацію" військових, а з 2024 року почав уповільнювати роботу YouTube, що до кінця 2024-го майже повністю перестав завантажуватися. Масові відключення інтернету та мобільного зв'язку в 2025 році, зокрема у Криму та на Луганщині, ускладнили доступ до месенджерів і пошукових систем, а блокування VPN і нові закони зробили використання обходів цензури ризикованим. Паралельно впроваджується "суверенний інтернет" і нав'язується месенджер Max, який є багатофункціональним додатком із повним доступом до даних користувача та використовується як інструмент стеження, ідентифікації та політичних репресій. Правозахисники наголошують, що мешканці окупованих територій

фактично позбавлені доступу до незалежної інформації й змушені користуватися платформами, повністю контрольованими Кремлем, що створює атмосферу страху та тотального контролю [1].

Соціальні мережі відіграють роль альтернативної публічної сфери, де громадяни можуть обмінюватися інформацією, мобілізуватися й формувати критичну думку. Саме тому росія та її окупаційні адміністрації розглядають їх як загрозу й запроваджують репресії проти користувачів – від адміністративних штрафів до кримінального переслідування та викрадень.

Важливим є те, що політична комунікація в соцмережах стала ключовим інструментом опору. Публікації в Telegram, Facebook чи навіть "Одноклассниках" мають потенціал впливати на суспільні настрої й викривати пропаганду. Саме тому влада намагається застосовувати "ефект охолодження" (chilling effect): створити відчуття небезпеки й змусити громадян самоцензуруватися. З точки зору теорії інформаційної безпеки, це є прикладом гібридного контролю над інформаційним простором: поєднання правових інструментів, пропаганди й примусу.

Після початку повномасштабного вторгнення росії в Україну окупаційні адміністрації в Криму й на інших тимчасово окупованих територіях суттєво посилили інформаційний контроль і переслідування громадян.

Так, у квітні 2023 р. в окупованому Криму розпочали адміністративну справу проти блогера й громадянського журналіста Ролана Османова через його коментар у Facebook, де він написав: "Жоден цар не вартий того, щоб за нього вмирати чи вбивати". Справу відкрили за статтею 20.1 КпАП рф про "непристойні висловлювання та неповагу до суспільства й держави", а суд розглянув протокол без його участі [40].

15 травня 2023 р. підконтрольний росії Ленінський райсуд Севастополя оштрафував 40-річну мешканку міста на 30 тисяч рублів за "дискредитацію російської армії", оскільки вона розміщувала у соцмережі "Одноклассники" публікації з критикою дій рф [203].

Такі переслідування стали масовими: лише у 2022-2023 рр. в росії порушено понад 528 кримінальних справ, з них 154 – за “фейки” про російську армію [235].

Окремо варто відзначити репресії проти адміністраторів українських телеграм-каналів. У серпні 2023 р. окупанти затримали адміністраторів “РІА-Мелітополь” і “Мелітополь – це Україна”, утримували їх у секреті понад два місяці й лише 29 жовтня оприлюднили пропагандистські відео із “зізнаннями”. Серед затриманих – 19-річна дівчина та хлопець із психічним захворюванням. Усіх їх звинувачують у шпигунстві, закликах до терактів і державній зраді, що загрожує 12–20 роками позбавлення волі [204].

Цифрові платформи перетворюються на ключовий індикатор рівня політичної свободи: чим більше репресій проти користувачів соцмереж, тим більше ознак згортання публічної сфери та утвердження авторитарного режиму.

У квітні 2023 р. в окупованому Криму розпочали судове переслідування блогера та громадянського журналіста Ролана Османова через його коментар у Facebook: “Жоден цар не вартий того, щоб за нього вмирати чи вбивати”. Справу відкрили за статтею 20.1 КпАП рф про “непристойні висловлювання та неповагу до суспільства й держави”. Суд у Сімферополі розглянув протокол без участі Османова, хоча він прибув до суду. Раніше, 15 березня 2023 р., в Османова провели обшуки, допитали у ФСБ, змусили пройти поліграф і склали протокол за “зневагу до влади”, використавши цитату з його допису. Ця справа демонструє переслідування кримських активістів за будь-які прояви критики російської влади.

Після початку повномасштабного вторгнення росії в Україну в лютому 2022 року Кремль почав активно використовувати підробний «фактчекінг» - перевернення реальності під виглядом перевірки фактів. Мета такої пропаганди - поширювати дезінформацію, виправдовувати дії росії, дискредитувати справжніх фактчекерів і підірвати довіру до об’єктивних джерел інформації.

Прикладами є спроби заперечити воєнні злочини в Бучі, маніпуляції щодо теракту в «Крокус-Сіті-Гол» та створення ресурсів типу waronfakes.com, які

видають фейкові розбори подій за перевірку фактів. Такі матеріали поширюються через державні медіа рф («1 канал», «Росія 24», RT) та Telegram-канали, перекладаються кількома мовами і орієнтовані як на російську, так і на міжнародну аудиторію. Кремль цілиться на людей, які вже схильні довіряти «альтернативним медіа», і використовує фейковий фактчекінг, щоб ускладнити роботу справжніх фактчекерів, засмітити інформаційний простір та підірвати довіру до перевірених джерел. Експерти підкреслюють, що це ефективний інструмент пропаганди, який обмежує пошук правди і створює хаос у медіапросторі. За словами Мартіна Іннеса, директора Інноваційного інституту безпеки, злочинності та розвідки Кардіффського університету, росія використовувала елементи підробного «фактчекінгу» ще до 2022 р., наприклад після справи зі Скрипалем, але з початку повномасштабної війни цей метод став інституалізованим: «Війна з фейками» (War on Fakes) стала певною мірою брендом та каналом [інформації], технологія набула організованої форми, що відзначилося із початком масштабної війни в Україні». Прокремлівські медіа створюють фейкові матеріали у форматі псевдодокументів, наприклад «документальні» сюжети про нібито фейки України, щоб заплутати аудиторію та дискредитувати справжніх фактчекерів. Основна аудиторія – росіяни, але такі матеріали перекладаються й іншими мовами для міжнародного охоплення [130].

У березні 2023 р, російська пропаганда активно поширювала дезінформацію в українському та міжнародному інформаційному просторі. За даними моніторингу ГО «Платформа прав людини», експерти зафіксували 157 фейкових повідомлень на 19 тем, серед яких п’ять були новими для російської пропаганди. Традиційні наративи включали: постачання зброї Україні партнерами, дискредитацію ЗСУ та української влади, критику Президента Зеленського, спроби зобразити Україну «недодержавою», нібито вплив іноземних найманців, економічні проблеми Заходу через санкції проти рф, загрози ядерною зброєю, проблеми з біженцями, міфічні біолабораторії, нібито порушення прав населення, а також вигадані «концтабори» для тих, хто не бажає воювати з росією. Проте вже і цей час з’явилися й нові теми: нібито

програш України в битві за Бахмут, завезення радіоактивних речовин для провокацій, ордер на арешт Путіна, зустріч Путіна та Сі Цзіньпіна, а також твердження, що Україна нібито не зможе повернути Крим [274].

У першу річницю повномасштабного вторгнення росії в Україну соцмережі охопив сплеск фейків. Найпоширеніші та абсурдніші фейки російської пропаганди включають повідомлення про нібито втечу президента Володимира Зеленського за кордон або його капітуляцію, у тому числі через діпфейки, нібито погіршення стану здоров'я президента, неправдиві твердження про перепродаж України західної зброї або постачання електроенергії до Європи під час відключень, вигадані історії про «американські біолабораторії» та підготовку «брудної бомби», фейки про нібито передачу західних областей під протекторат Польщі, а також маніпуляції щодо релігійних громад, зокрема про примусове «перехрещування» парафіян УПЦ МП у Православну церкву України (Додаток Д) [302].

Деякі дописи отримали мільйони переглядів, зокрема в США ультраправі акаунти поширювали безпідставні заяви про нібито «сфальшовану» війну, організовану західними ЗМІ та урядами [38].

У Франції МЗС викрило масштабну кампанію дезінформації про війну росії в Україні. Російські спецслужби створювали підроблені сайти та фейкові URL у соцмережах, маскуючись під європейські, американські та близькосхідні медіа, щоб дискредитувати політику Заходу.

З червня 2022 до травня 2023 року діяли 355 таких вебдоменів, а у французьких медіа, як Le Monde і Figaro, виявили 58 фейкових статей. Деякі сайти імітували урядові ресурси, поширюючи неправдиву інформацію про «податки на безпеку». Також зафіксовано понад 160 сторінок у Facebook із 600 посиланнями на фейки [314].

Подібні методи пропаганди росія застосовує і в інших країнах: у США фокус роблять на критиці допомоги Україні та виборчих питаннях, у Німеччині через дипустанови та проросійські медіа поширюють меседжі про "втомленість світу від України", а у країнах ЄС та НАТО діють мережі

проросійських блогерів, які транслюють кремлівські наративи різними мовами, зокрема для українських переселенців. росія також поширює меседж про нібито “легітимність” Путіна та “нелегітимність” української влади [238].

Саме тому російська пропагандистська машина продовжує активно поширювати дезінформацію не лише в Україні, а й за її межами. Зокрема, в Ізраїлі зафіксовано випадки маніпулятивного впливу на громадську думку через підроблені новини. В ізраїльському сегменті соцмереж поширюються фейки російського походження під виглядом ізраїльських ЗМІ. За даними аналітиків Cybereason, російські спецслужби створюють підроблені статті з логотипами відомих порталів і підписами журналістів, але з неправдивим змістом. Мета – дезінформація, вплив на громадську думку та дискредитація України. Поширюються фейкові заяви про «позицію Ізраїлю щодо України», нібито цитати міністрів, а також проросійські наративи про «боротьбу з нацистами» та провокації України на Близькому Сході. Часто ці матеріали супроводжуються підробленими фото та відео [247].

Аналіз матеріалів англійською, французькою, арабською та російською мовами, оприлюднених у ЗМІ Єгипту, Нігерії та Сенегалу з серпня 2023 до січня 2024 року, виявив серію послідовних фейків: звинувачень у продажі дітей та планах України створити ядерну зброю. Часто такі публікації супроводжуються відео з вигаданими авторами та анонімними “джерелами”, а використані приміщення у відео виглядають однаково, що свідчить про постановочний характер [100].

Пропагандистські канали росії продовжують активно поширювати “репортажі” з Сирії, намагаючись сформувати у міжнародної та української аудиторії хибне уявлення про нібито причетність України до загострення безпекової ситуації в цій країні. За даними Центру протидії дезінформації, такі матеріали використовують маніпулятивні прийоми, перекручують факти та створюють фейкові наративи [244].

росія застосовує комплексні інформаційні атаки, поєднуючи різні інструменти впливу. Зокрема, створюються фейкові телеграм-канали, що

маскуються під офіційні сторінки українських бригад і батальйонів, аби поширювати пропагандистські наративи та збирати дані під виглядом “зворотного зв’язку” (Додаток Е) [245]. Паралельно використовують штучний інтелект для генерування псевдотелевізійних сюжетів, стилізованих під українські ЗМІ, у яких поширюють неправдиві повідомлення, наприклад, про нібито запроваджені графіки відключень електроенергії. Тим часом у рф тестують систему “Окулус”, здатну автоматично виявляти небажаний контент і поширювати цензуру в мережі, що свідчить про подальшу цифровізацію пропагандистських та репресивних інструментів [247].

Російська пропаганда продовжує намагатися розхитати морально-психологічний стан українців, вкидаючи в мережу нову порцію фейків, повідомляє Центр стратегічних комунікацій та інформаційної безпеки.

Найбільшим приводом для дезінформації залишається мобілізація в Україні. росія поширює панічні наративи про «п’ять варіантів мобілізації», щоб налякати людей і схилити до вимог до влади про переговори на умовах країни-агресора. Також пропагандисти розганяють фейки про «втечу західних найманців», «мільйони українських біженців у Польщі після поразки ЗСУ» та нібито «неправильне забезпечення мобілізованих». Жодне з цих повідомлень не має фактичного підтвердження. Окремо поширюються фото- та відеофейки, спрямовані на підрив українсько-польських відносин і дискредитацію української армії. Пропаганда також використовує історії про нібито «вербування» бійців Міжнародного легіону приватними структурами [184].

За даними Центру протидії дезінформації, російські ЗМІ просували нереальні історії про нібито таємні плани НАТО в Україні, «розбирання» живих бійців ЗСУ на органи, блокування банківських рахунків через неявку до ТЦК та СП, внутрішні розбірки у військових частинах, провокативні художні акції та створення фейкових сайтів із політичним контекстом. Усі ці матеріали, цілком очевидно, є частиною інформаційної війни і не відповідають дійсності [319].

Виправдання власних воєнних злочинів є одним із ключових напрямів російської пропаганди, що супроводжується поширенням фейкових матеріалів

та маніпуляцій. Російські телеграм-канали видають фото наслідків власних обстрілів за “розстріли цивільних” українськими військовими. 20 лютого 2024 р. в селі Петропавлівка Куп’янського району російський дрон-камікадзе влучив у цивільну автівку: двоє людей загинули, одна - поранена. Голова Харківської ОВА О. Синєгубов оприлюднив фото з місця атаки, але пропагандисти використали його, стверджуючи, що людей убили українські військові за відмову вітатися “націоналістичним вітанням”. Подібні фейки рф поширювала й раніше, зокрема видаючи відео з окупованого Донбасу за знущання ЗСУ з цивільних. Після блокування каналів RT Маргарита Симоньян закликала створити “народну інформаційну міліцію”, яка через бот-мережі поширює пропаганду різними мовами у соцмережах [246].

Ворожі телеграм-канали поширюють фейки про нібито підготовку ЗСУ ударів хімічною зброєю на Донецькому та Херсонському напрямках. «Не надаючи жодних доказів, російська пропаганда використовує тактику віддзеркалення, звинувачуючи Україну у злочинах власної армії (Додаток Є). Ці спроби приречені на провал», - підкреслили в ОТУ «Харків». Як раніше повідомляла АрміяInform, для ілюстрації «антивоєнного руху» російські фейкороби використовували фото з Румунії та Аргентини [204].

Інформаційна кампанія російської пропаганди висунула фейковий наратив про нібито плани України підірвати Запорізьку АЕС (Додаток Ж). Це сталося після російської провокації 4 квітня 2024 р., коли станція залишилася на одній лінії живлення. Російські ЗМІ, зокрема ТАСС та РІА Новости, поширювали фейки, посилаючись на пропагандиста та депутата Держдуми Олексія Журавльова, стверджуючи, що Україна нібито хоче звинуватити росію у підриві станції. За даними МАГАТЕ, ймовірні атаки безпілотників фіксувалися, але немає жодних доказів, що це робила саме Україна, а окупанти не допустили міжнародних експертів до місць вибухів. Для поширення наративу росія залучила міжнародні ресурси, зокрема хорватський портал Advence, який публікує фейки без перевірки фактів. Автори статей D. Marjanović та Antun Roša

фактично не існують або не ведуть журналістської діяльності, проте їхні матеріали тиражуються російськими ЗМІ для дискредитації України [239].

Російська пропаганда використовує будь-які інформприводи для інформаційно-психологічних операцій, спрямованих на посів паніки серед українців і розкол суспільства. Приводом стала заявка України до Ради Європи про часткове призупинення дії деяких пунктів Європейської конвенції з прав людини на час війни. Роспропаганда подала це як «обмеження прав українців», а соціальні мережі швидко підхопили фейкові коментарі про «тотальну диктатуру» та «втрату права на власність». Ворог намагається створити розкол між тими, хто виїхав за кордон, і тими, хто залишився в Україні, формуючи альтернативну «Україну за кордоном» і дискредитуючи легітимну владу. Поширюються фейки про нібито нелегітимність президента, примусову мобілізацію жінок і школярів, а також про «харківське підпілля» та вигадані вбивства, щоб деморалізувати населення. Головна мета цих ІПсО - переконати українців, що війна «немає сенсу» і що треба вимагати переговорів замість боротьби, посіяти недовіру до влади та підривати моральний дух суспільства [237].

Центр стратегічних комунікацій та інформаційної безпеки при Міністерстві культури та інформаційної політики оприлюднив добірку спростувань найгучніших російських фейків за період з 4 по 10 грудня 2024 р. Серед них - фейковий Telegram-бот нібито від міністра оборони Умєрова, який не має жодного стосунку до міністерства; інформація про загибель мобілізованого підлітка в Україні, яка виявилася вигадкою, насправді загинув 26-річний боєць зі Львівщини; перекручування слів генерала Муженка щодо F-16, приписавши йому порівняння України з нацистською Німеччиною; дезінформація про нібито “референдум Львівської області про приєднання до Польщі”; а також підроблений лист про збір даних студентів ЛНУ, тоді як обласна влада жодної інформації не збирає. Раніше повідомлялося, що жителі Одещини та Харківщини отримували повідомлення від ворога з пропозицією “обміняти інформацію про ЗСУ на долари” [330].

11 вересня 2024 р. канали «Sputnik Ближнее зарубежье», «NE.САХАР», «Медведь», «Петя Первый» та інші поширили відео з заявою екснардепа Ігоря Мосійчука про нібито масову реєстрацію українців у Покровську для отримання громадянства росії. Повідомлення також підхопили російські медіа («Другая Украина», «ПОЛИТИКУС», Dzen.ru) та соцмережа «ВКонтакте», що забезпечило його широке охоплення. У середині того ж місяця Telegram-канали «Укропский фреш» та «Украина.ru» поширили фейк про нібито пропозиції українським військовослужбовцям купувати місця на кладовищі ще за життя [309].

Анонімні канали «Медведь» та «UKR LEAKS» поширили фейк про нібито листівку Посольства Великої Британії в Україні, яка начебто давала громадянам країни поради, як уникати співробітників територіальних центрів комплектування та соціальної підтримки, що створювало ілюзію «загрози» з боку українських державних структур. 26 вересня російські канали «Военный обозреватель», «Кот Костян – официальный канал», «Медведь», а також російські медіа («Московский комсомолец», «Подмосковье сегодня», «Life.ru», «ОСН», «Discover 24», «TOPNews») поширили фейк про нібито загибель пілота ВПС США під час ракетного удару рф по Хмельниччині [217].

Проросійські Telegram-канали та інтернет-ресурси активно поширювали серію фейків і маніпуляцій, спрямованих на дискредитацію українських інституцій та деморалізацію населення. 3–18 вересня канали «Медведь», «Кот Костян – официальный канал», «Олеся Лосева», «СОЛОВЬЁВ», «Мир сегодня с “Юрий Подоляка”», «Colonelcassad», «Украина.ру» та інші поширили фейки про нібито примусову здачу крові неповнолітніми у Полтаві для «шведських інструкторів» та загибель іноземних військових під час ракетного удару рф. Одночасно російські медіа («Вечерняя Москва», «Аргументы и Факты», «Аргументы Недели», «ZOV Харьков») і соцмережі (X, «ВКонтакте», Facebook) активно репостили ці матеріали. Паралельно з’явилися фейки про нібито відмову священника ПЦУ у Чернівцях відспівувати загиблих через їхнє хрещення в УПЦ МП та маніпуляції щодо знайдених у Києві російських рублів

у монастирі Свято-Введенському, поширені каналами «Украина.ру», «Шкварка» та пропагандистськими акаунтами в соцмережах.

На окупованих територіях дезінформація передається через особисті розмови, робочі колективи та фейкові Telegram-канали, які видають себе за українські. Люди часто не перевіряють інформацію і передають її далі, бо бояться відкрито спілкуватися про правду. Telegram-канали під виглядом проукраїнських поширюють, для прикладу, неправдиві дані про ціни (хліб по 50 грн.), загрозу для чоловіків на вулиці від ТЦК та наслідки обстрілів. Люди на окупованих територіях часто не розповідають правду стороннім через страх бути викритими. Пропаганда змінювалась із 2014 року: спочатку ворогами називали «нацистів» чи конкретні формування, після 2022-го - всю Україну, роблячи ворогом кожного [337].

У жовтні 2024 р. Telegram-канал «Укропский фреш», а також «Шейх Тамир» і низка проросійських медіа («Другая Украина», «Вести», «News.ru», «ОТР Online», «Союз православных журналистов», «Смотрим.ru») поширили фейк про відмову у медичній допомозі парафіянам УПЦ МП після бійки у Черкасах. 27 жовтня 2024 р. аналогічні канали («Медведь», «Запорожский фронт», «На самом деле в Донецке») поширили анімаційний ролик нібито від Міністерства оборони України, в якому створювалася паралель між подіями минулого та сучасністю, із заявою, що українські військові протистоять армії КНДР. Обидва кейси активно поширювалися у соцмережах Х, «ВКонтакте» та «Одноклассники», що забезпечувало велике охоплення та повторні репости. Такі інформаційні вкиди спрямовані на підрив довіри до українських державних інституцій, дискредитацію ЗСУ та посилення образу «непрофесійності» і «маніпулятивності» української влади серед місцевої та міжнародної аудиторії [316].

ЦПДЗ зафіксував нову хвилю російських фейків про «звірства» українських військових у районі Курської операції. Пропагандисти поширюють відео з нібито військовополоненим та загиблими цивільними, стверджуючи про «десятки вбитих», хоча жодних доказів немає. «Кремль вкладає великі гроші,

щоб створити «русскую Бучу» і приховати власні злочини», - зазначають у ЦПД. За даними ГУР МО, росія у 2025 році витратить на пропаганду понад $1,4 млрд. Разом із ЦПД запущено розділ «Рупори Кремля» на порталі War & Sanctions із переліком ключових пропагандистів та медіаменеджерів [210].

У 2025 році російська пропаганда продовжує активно поширювати фейки, спрямовані на дискредитацію України та її партнерів [270]. Продовжуючи хвилю інформаційних вкидів 2025 року, російські пропагандистські ресурси систематично поширюють фейки, спрямовані на дискредитацію України, її союзників та ЗСУ, використовуючи як Telegram-канали, так і інші соцмережі. 31 січня пропагандистські канали «Медведь» та «Республика Одесса» опублікували фейк про нібито припинення фінансування міжнародного проекту Bellingcat, приписавши це коментарю головного редактора Еліота Хіггінса для The Wall Street Journal.

У лютому 2025 р. з’явився резонансний сюжет індійського каналу WION News, у якому стверджувалося, що українські військові нібито продають до половини американської зброї мексиканським наркокартелям. Джерелом цієї заяви став подкаст Такера Карлсона з відставним офіцером армії США Деніелом Девісом, який швидко набрав сотні тисяч переглядів. Цей матеріал підхопили численні проросійські Telegram-канали, поширюючи наративи про «корупцію в ЗСУ» та «послаблення європейської безпеки». Подібні інформаційні вкиди спрямовані на підрив довіри до України серед західної аудиторії, деморалізацію суспільства та створення враження неефективності міжнародної допомоги [104].

4 лютого 2025 р. в схожому руслі з’явився сюжет із підробленим логотипом Bloomberg, поширений у Telegram-каналах «Кот Костян – официальный канал», «Медведь», «Одесса Za Победу!» та інших, де стверджувалося, що з 2022 року USAID нібито втратила контроль над біолабораторіями в Україні, що призвело до втрати 20 млрд доларів інвестицій. Одночасно 5 лютого відео від нібито розважального порталу E!News повідомляло, що голлівудські зірки отримували гроші від USAID за поїздки до

України для популяризації Зеленського, поширюючись через Telegram-канали «Абу», «Не Zли русского медvедя», «Батькович», «рИдовка», «Военкор Лисицын», а також у соцмережах X і ВКонтакте. Паралельно поширювалися фейки про нібито «жорстокість» українських військових: 14 лютого відео про розстріл трьох бійців 81-ї окремої аеромобільної бригади опублікував канал «U_G_M», згодом його підхопили «Промєтєй», користувачі X (Alexander Ivanov), TikTok (olgushaa_aa) та групи ВКонтакте («Подоляка», «Палата №6»), а також численні російські відеоплатформи та YouTube [343].

Російські спецслужби продовжують фабрикувати фейки, намагаючись дискредитувати Україну на міжнародній арені, зокрема звинувативши її в підготовці терактів проти дипломатів ЄС, повідомляє ГУР МОУ.

«Безумовно, це фейки», - наголосив А. Юсов. Він додав, що «…Весь світ розуміє абсурдність цих заяв, але пропагандистські задачі вимагають певних дій, навіть якщо вони абсолютно не витримують жодної критики», - зазначив Юсов. Він також підкреслив, що це створює інформаційний шум і виправдовує агресивні дії рф: «Це примітивна спроба створити алібі для продовження майбутніх спецоперацій за кордоном» [229].

У командуванні Повітряних сил ЗСУ спростували російський фейк про нібито збитий літак F-16 над Сумською областю. За даними Центру протидії дезінформації, російські Telegram-канали поширюють неправдиву інформацію. «РАШНпропаганден знову «збили» наш літак! Цього разу F-16. Пілоти F-ок сьогодні вчергове успішно відпрацювали по рашистах. І так щодня, бойова робота триває! Пишаюсь нашими пілотами!» - написав начальник управління комунікацій Юрій Ігнат (Додаток З) [102].

Міністр оборони Данії спростував фейк російських ЗМІ про загибель данського інструктора F-16. «Ця інформація не відповідає дійсності. Жоден данський солдат не загинув в Україні. Це неправдива історія, яку поширюють російські ЗМІ, ймовірно, з метою дискредитації Данії. Я ставлюся до цього дуже серйозно», - заявив Троельс Лунд Поульсен. Він додав, що такі повідомлення - частина кампаній дезінформації у сфері безпеки [179].

У березні 2025 р. пропагандистські Telegram-канали та ресурси поширювали вигадані повідомлення про «масові втрати» українських військових на Курщині. 15 березня вони опублікували сфабриковану обкладинку «Hull Daily Mail» із цифрою 70 тисяч загиблих, а 20 березня – фейк про нібито загибель першої групи контрактників віком 18–24 роки, використавши відео з логотипом «Ґвара Медіа» для створення правдоподібності [190].

Російські та прокремлівські медіа активно поширюють дезінформацію щодо операцій ЗСУ на Курщині та Сумщині, створюючи фейки, які маніпулюють емоціями та страхом українців. Зокрема, поширювалася неправдива інформація про те, що Сумська районна рада нібито вирішила включити російське місто Суджа до складу Сумського району (Додаток І) України, а також фейкові відеоролики нібито з коментарями Валерія Залужного про затвердження Курська та Курської області в конституції України. Пропагандисти також повідомляли про термінову потребу в донорській крові для поранених у Курській області, про продаж нібито вкрадених ікон із церков та про загибель співробітниці жіночої колонії під час штурму українськими військовими. Крім того, у мережі з'являлися підроблені обкладинки німецьких видань із вигаданими заголовками про український наступ на Курщину, що є фейками [347].

Загострення на фронті та поглиблення співпраці України з ЄС спричинили нову хвилю російської дезінформації. Пропагандисти поширюють фейки, щоб дискредитувати підтримку Євросоюзу та посіяти недовіру до євроінтеграції. Найпоширеніші маніпуляції включають твердження, що відбудова України стане «непідйомним тягарем» для ЄС, що посольства України створюють фейкові Телеграм-чати для консультацій, або що українських військових нібито «розбирають на органи» у Польщі. Насправді фінансова допомога ЄС - це інвестиції у стабільність України, офіційні консультації відбуваються лише через сайти та верифіковані сторінки посольств, а фейки про трансплантації повністю вигадані. Головна мета таких атак - підірвати довіру до ЄС і створити

розкол між Україною та західними партнерами. Чим тісніші зв'язки України з ЄС, тим активніше Кремль атакує їх у медіапросторі, тому критичне мислення і перевірка джерел залишаються найнадійнішим захистом від фейків [183].

4 квітня 2025 р. росія завдала ракетного удару по Кривому Рогу. Генеральний штаб ЗСУ повідомив, що російське військове відомство намагається приховати цинічний злочин, поширюючи неправдиву інформацію про нібито «влучання в місце проведення наради командирів з'єднань ЗСУ із західними інструкторами». Насправді ракета поцілила у житловий масив та дитячий майданчик. Внаслідок обстрілу загинули щонайменше 16 мирних жителів, серед яких шестеро дітей, десятки людей отримали поранення, частина з них перебуває у важкому стані [309].

Соцмережі активно використовувалися для поширення вигаданої інформації, спрямованої на залякування населення та дискредитацію української сторони. 2 червня 2025 р. у Стамбулі Україна та росія домовилися про обмін важкопоранених і тяжкохворих військовополонених за принципом «всіх на всіх», а також про репатріацію 6000 тіл загиблих захисників, проте Москва одразу почала маніпуляції, намагаючись зірвати домовленості та дискредитувати Україну. російські спецслужби запустили масштабну інформаційно-психологічну операцію, поширюючи фейки про нібито зрив обмінів, приховування втрат, небажання влади повертати тіла загиблих і виплачувати компенсації, а також завищуючи цифри втрат ЗСУ. Пропаганда намагається посіяти паніку серед родичів полонених і загиблих, зруйнувати довіру суспільства до держави та змусити українців вимагати капітуляції [200].

30 липня 2025 р. провідне російське державне агентство «РИА Новости» опублікувало статтю під назвою «Іншого варіанту нема: живим в Україні не повинен залишитись ніхто». Автор матеріалу К. Стрєльніков, відомий як піар-фахівець та колишній співзасновник ресурсу Politrussia.com, використовував характерні прийоми російської пропаганди, зокрема дегуманізацію українських військових, яких порівнювали з «лабораторними щурами», конструювання образу «західних панів», що воюють руками українців, та маніпулятивну

дилему «капітуляція або самознищення». Стаття Стрєльнікова стала маркером посилення геноцидної риторики у російському інформаційному просторі: з 2024 р. Кремль активно поширював наратив про те, що винуватцями війни є західні партнери України, нібито перешкоджаючи «мирному врегулюванню», що слугувало елементом війни на виснаження у військовій та інформаційній площинах.

За даними Центру протидії дезінформації (ЦПД), пропагандистські матеріали включають нібито підготовку Україною “провокацій” із небезпечними речовинами на Донеччині, скидання замінованих іграшок на тимчасово окуповані території підготовку ударів по Краматорську чи провокації в пологовому будинку. Також поширюються абсурдні заяви про “крематорій для ЗСУ” у Тернопільській області (Додаток Ї), що є повною вигадкою. Ці фейки мають спільну мету: перекласти відповідальність за власні воєнні злочини на Україну, створити інформаційне “алібі” для дій російських військ та посіяти паніку й недовіру серед цивільного населення [296; 147; 46; 317].

Основною метою таких публікацій рф було моральне демобілізування українського суспільства, підірвання довіри до власних інституцій та союзників, а також підготовка підґрунтя для політичного тиску на Україну з вимогою поступок [48].

За даними Центру протидії дезінформації, основні меседжі Кремля: нібито небажання Києва досягти миру, блокування переговорного процесу, висунення нереалістичних вимог та залежність України від Москви і Вашингтона. Пропаганда поширюватиме фейки про «вибірковий підхід» у звільненні полонених, «непрозорі переговори», загрози нового вторгнення та нібито «ракетні удари». Особлива увага приділятиметься соцмережам, TikTok і міжнародній аудиторії, щоб створити паніку, дискредитувати українську державність і посіяти сумніви у західній підтримці. Кремль також використовуватиме історичні події, пам’ятні заходи та геополітичні візити, щоб демонструвати власну силу та перекладати відповідальність за втрати на

українське командування, формуючи образ України як «радикального режиму» [224].

російська федерація також послідовно використовувала міжнародні дипломатичні події як інструмент гібридної війни, розглядаючи їх не як засіб вирішення конфліктів, а як фронт інформаційно-психологічного впливу. Анонсована зустріч Дональда Трампа та Владіміра Путіна на Алясці стала для Кремля приводом активізувати пропагандистські кампанії, спрямовані на деморалізацію українського суспільства, підрив довіри до власної влади та дискредитацію міжнародних партнерів України.

Російські медіа використовували кілька основних стратегій: поширювали наратив про «втрачений шанс на мир», який нібито був на початковому етапі війни, міфологізували зустріч як «субарктичну Ялту», створювали ілюзію «останнього шансу на мир», атакували єдність України та дискредитували її міжнародні союзи. Ці інформаційно-психологічні операції мали на меті сформувати у населення відчуття марності спротиву, ізоляції держави та необхідності капітуляції. Основна стратегічна мета Кремля полягала в ерозії внутрішньої єдності України та зниженні довіри до інститутів влади, а в максимальному варіанті - у провокуванні внутрішніх заворушень або політичної кризи, що послаблює обороноздатність країни. Водночас зустріч на Алясці не створювала реальних умов для завершення війни, адже позиція росії залишалася незмінною - вимоги Кремля фактично зводилися до ультиматумів, що означали капітуляцію України. Найефективнішим протидією таким інформаційним операціям залишалося критичне мислення, опора на факти та усвідомлення, що війна ведеться за існування української державності та свободи суспільства [6].

Потрапити на російські фейки може будь-хто, навіть людина, яка добре орієнтується в темі, попереджає аналітикиня CAT UA Олена Захарченко. Росія активно створює міфи, наприклад, про нібито продаж української електроенергії за кордон, групи «повісток» або ж «жахливу поведінку»

українських солдатів на Курщині. За її словами, над цим працює не лише ФСБ, а й так звані «опозиційні» ЗМІ на кшталт телеканалу «Дождь» [195].

Ганс Петтер Мідттун (колишній військовий аташе норвезького посольства в Україні) виокремлює такі ключові ознаки гібридної політики рф:

1. Історичне та ідеологічне підґрунтя: численні згадки про «Малоросію» та висловлювання президента В. Путіна про те, що росіяни та українці «один народ», формують концептуальну легітимізацію зовнішнього втручання.

2. Заперечення державності України: під час саміту НАТО у 2008 р. президент Путін висловив думку, що «Україна навіть не є державою», що відображає прагнення підривати міжнародне визнання українського суверенітету.

3. Територіальні претензії та проєкт «Новоросія»: заяви про історичну приналежність частини українських територій до росії, а також повторне нагадування про передачу цих земель радянським урядом у 1920-х роках, слугують інструментом ідеологічного та політичного тиску.

4. Документовані плани дестабілізації: за даними Служби безпеки України (2016 р.) та витоками з пошти радника В.Путіна В.Суркова, російські спецслужби здійснюють системну роботу щодо дестабілізації внутрішньої ситуації в Україні.

5. Фокус на Причорноморському регіоні: висловлювання Путіна у 2019 р. про передачу «споконвічно російських територій» Україні підкреслюють постійний стратегічний інтерес рф до всієї південної та західної частини країни.

Гібридна війна росії проти України не обмежується лише окремими регіонами, такими як Донбас, а була спрямована на всю країну. Вона включає комплексне застосування політичних, інформаційних, економічних та історико-культурних інструментів, що створюють непередбачувану та довготривалу загрозу національній безпеці [178].

Соціальних мережі з одного боку, вони можуть слугувати інструментом поширення дезінформації та ненависті, а з іншого — засобом привернення міжнародної уваги до порушень прав людини та документування фактів. Вони також ілюструють складнощі платформ у забезпеченні ефективного контролю за контентом та необхідність розвитку медіаграмотності користувачів.

Отже, аналіз ключових кейсів інформаційного впливу на Україну у період 2014–2025 років демонструє системність та багаторівневість російських інформаційно-психологічних операцій. Кремль послідовно використовував історичні наративи, міфологізовані образи та емоційно заряджені меседжі для легітимізації власних дій, підриву морального духу українського суспільства та дискредитації українських інституцій і міжнародних союзників. Ключовим елементом таких кампаній стало поєднання військових, дипломатичних та медійних засобів впливу, що забезпечувало високий рівень контролю над інформаційним полем і дозволяло формувати бажані уявлення про конфлікт серед різних цільових аудиторій. Виявлені кейси свідчать про те, що російська інформаційна стратегія орієнтована не лише на безпосередню маніпуляцію свідомістю населення, а й на довготривале формування умов для ослаблення державної суб’єктності та суспільної єдності України.

Дослідження ключових кейсів інформаційного впливу на Україну у 2014-2025 рр. показало, що інформаційна агресія проти нашої держави носить системний і довготривалий характер, вирізняється багаторівневістю та використанням широкого спектра інструментів – від дезінформаційних кампаній і маніпуляцій у соціальних мережах до спрямованих кібератак на об’єкти критичної інфраструктури.

Загальна тенденція російських фейків демонструє систематичне використання російськими пропагандистами соціальних мереж як основного каналу поширення дезінформації.

Аналіз поширених фейкових наративів демонструє систематичне використання російськими пропагандистами соціальних мереж як основного каналу дезінформації. Серед ключових тем - нібито значні втрати українських

військових, звинувачення Збройних Сил України у «жорстокості» та порушеннях військової дисципліни, а також поширення тверджень про корупційні схеми за участю західної допомоги та США. Для підвищення правдоподібності таких повідомлень використовуються підроблені логотипи відомих медіа, цитати публічних осіб, відеоматеріали та інші елементи верифікаційного фасаду, що створюють ілюзію достовірності та авторитетності джерела.

Найактивнішими платформами для поширення таких повідомлень залишаються Telegram, X, ВКонтакте, TikTok та YouTube. Вони забезпечують не лише швидке охоплення широких аудиторій, а й активну взаємодію через репости, коментарі та лайки, що сприяє вірусному поширенню контенту серед української, російської та міжнародної спільнот. Внаслідок цього дезінформаційні кампанії здатні впливати на формування суспільних наративів, спотворювати сприйняття реальності та підривати довіру до державних інституцій, що робить інформаційний вплив ефективним інструментом у межах Війни за Незалежність України.

Аналіз українського та світового досвіду протидії інформаційним загрозам дозволяє стверджувати, що ефективний захист вимагає комплексного підходу.

Механізм протидії інформаційним загрозам доцільно розглядати як багаторівневу систему, що охоплює стратегічний, операційний і індивідуальний рівні.

На стратегічному рівні ключовим завданням є формування цілісної державної політики у сфері інформаційної безпеки, яка передбачає не лише реагування на загрози, але й їх попередження. Це включає розробку чітких комунікаційних стратегій, підтримку національного інформаційного простору. Окрім вдосконалення законодавчої бази, інституційна складова на цьому рівні передбачає розбудову сталої системи стратегічних комунікацій на рівні державних органів, посилення координації між силовими, інформаційними та дипломатичними структурами, а також інтеграцію України у міжнародні мережі протидії дезінформації (ЄС, НАТО, ОБСЄ). Важливу роль відіграє створення й

функціонування спеціалізованих структур, зокрема Центру стратегічних комунікацій та інформаційної безпеки та урядових платформ для спростування фейків.

Операційний рівень передбачає впровадження сучасних технологічних інструментів моніторингу та аналізу інформаційних потоків. Зокрема, застосування штучного інтелекту, алгоритмів машинного навчання та Big Data-аналітики дозволяє оперативно виявляти дезінформаційні кампанії, бот-мережі та скоординовану неавтентичну поведінку. Важливим елементом є також співпраця з адміністраціями соціальних платформ щодо обмеження поширення шкідливого контенту.

На соціальному та індивідуальному рівнях визначальним чинником ефективності протидії виступає інформаційна стійкість суспільства. Вона формується через розвиток медіаграмотності, критичного мислення та відповідального споживання інформації. Освітні програми, просвітницькі кампанії та включення елементів медіаосвіти в навчальні курси є необхідною умовою зменшення вразливості громадян до маніпулятивних впливів. Соціально-освітня складова передбачає й підтримку незалежних журналістських ініціатив і платформ фактчекінгу (StopFake, VoxCheck, Detector Media). Це дозволяє зменшити вразливість суспільства до психологічних операцій і сприяє формуванню культури інформаційної відповідальності.

Особливої ваги в умовах сучасних безпекових викликів набуває перехід до проактивної моделі забезпечення інформаційної безпеки, яка виходить за межі суто реактивного підходу. Така модель передбачає не лише своєчасне виявлення та нейтралізацію інформаційних загроз, але й цілеспрямоване формування власного інформаційного порядку денного. Йдеться про продукування та поширення позитивних, консолідуючих наративів, що сприяють зміцненню національної ідентичності, суспільної згуртованості та довіри до державних і демократичних інституцій.

Важливою складовою цього процесу є стратегічна комунікація, яка забезпечує узгодженість меседжів на різних рівнях державного управління та їх

адаптацію до потреб різних соціальних груп. Формування стійкого інформаційного середовища також передбачає активне залучення громадянського суспільства, медіа та експертного середовища до створення контенту, що протидіє деструктивним впливам і водночас формує позитивний образ держави як всередині країни, так і на міжнародній арені.

Загалом, на нашу думку, ефективний механізм протидії інформаційним загрозам у соціальних мережах в умовах війни має базуватися на інтеграції державного управління, інноваційних технологій і активної участі громадянського суспільства. Лише за умов їх синергії можливе не лише нейтралізувати актуальні інформаційні загрози, але й забезпечити довгострокову стійкість інформаційного простору України до зовнішніх і внутрішніх деструктивних впливів.

ВИСНОВКИ

Інформаційна безпека – це багаторівнева система правових, організаційних, технічних і соціальних заходів, спрямованих на захист інформаційного простору держави, суспільства та окремих осіб від негативного або маніпулятивного інформаційного впливу, забезпечення національної стійкості та функціональної стабільності політичної системи в умовах сучасних гібридних і кібервикликів.

Отже, інформаційна безпека є багатокомпонентним явищем, що поєднує технічні, інституційні та соціальні аспекти захисту інформаційного простору та виконує ключову функцію забезпечення стабільності політичної системи й захисту національних інтересів у сучасному інформаційному середовищі.

Інформаційна безпека виступає багатокомпонентним і багаторівневим явищем, що об’єднує технічні, інституційні та соціальні аспекти захисту інформаційного простору та виконує ключову функцію забезпечення стабільності політичної системи, захисту державних і національних інтересів, а також гарантування прав і свобод громадян у сучасних умовах інформаційного середовища. Її структурні компоненти охоплюють технічну складову, яка включає захист інформаційних систем, каналів передачі даних і інформаційної інфраструктури держави; інституційну складову, що передбачає нормативно-правове регулювання, організаційне забезпечення, координацію дій органів державної влади та формування державної політики у сфері інформаційної безпеки; а також соціальну складову, що спрямована на розвиток медіаграмотності, критичного мислення населення, протидію дезінформаційним та психологічним операціям, а також на підтримку демократичних принципів і культури відповідального споживання інформації.

Основні функції інформаційної безпеки включають не лише безпосередній захист інформаційних ресурсів і контроль за інформаційними потоками, але й моніторинг загроз, виявлення інформаційних атак і маніпуляцій, своєчасне

реагування на них, а також стратегічне формування позитивних наративів і підтримку державних цілей на національному та міжнародному рівнях. Важливим аспектом є здатність системи інформаційної безпеки забезпечувати баланс між безпековими пріоритетами та дотриманням демократичних свобод, таких як право на доступ до достовірної інформації, свобода слова і захист приватності громадян.

Особливості інформаційної безпеки проявляються у її високій динамічності, багаторівневості та взаємозв'язку між технічними, соціальними і політичними чинниками. Ці характеристики зумовлюють необхідність комплексного підходу до управління інформаційним середовищем, що поєднує технологічні засоби (системи кіберзахисту, аналітику та моніторинг інформаційних потоків), правові механізми (нормативно-правове регулювання та державну політику) та соціально-освітні заходи (формування медіаграмотності, просвітницькі кампанії, розвиток незалежної журналістики та платформ фактчекінгу). Особливу роль відіграє адаптивність системи до сучасних викликів гібридної війни та інформаційної агресії, яка проявляється у використанні дезінформації, психологічних операцій, кіберінцидентів і технологій штучного інтелекту для масового впливу на суспільну свідомість.

В умовах Війни за Незалежність України інформаційна сфера перетворюється на один із ключових театрів протиборства, де інформаційні впливи поєднуються з політичним, економічним, дипломатичним і воєнним тиском, що суттєво підвищує значущість інформаційної безпеки як інструменту стримування та захисту державного суверенітету.

Гібридна війна постає як комплексна форма сучасного конфлікту, у межах якої поєднуються воєнні та невійськові інструменти впливу, зокрема інформаційні, політичні, економічні та психологічні засоби, спрямовані на підрив інституційної стійкості держави зсередини. Вирішальну роль у таких конфліктах відіграє інформаційний вимір, оскільки саме через маніпуляцію свідомістю, дезінформацію та конструювання альтернативних інтерпретацій

реальності досягається делегітимація влади, фрагментація суспільства та ослаблення здатності держави до колективної мобілізації.

Аналіз теоретичних підходів та методів дослідження інформаційної безпеки дозволяє зробити висновок про її багатовимірний, комплексний і міждисциплінарний характер. Інформаційна безпека виступає не просто технологічним або організаційним феноменом, а соціально-політичним процесом, що взаємопов'язаний із системою державного управління, функціонуванням політичних інститутів та соціальними процесами в суспільстві. Теоретичні підходи, що поєднують політологічний, соціально-психологічний, технічний та правовий аспекти, дозволяють глибше розуміти сутність інформаційної безпеки та її функціонування у сучасному інформаційному середовищі.

Політологічний підхід у дослідженні інформаційної безпеки підкреслює її стратегічну роль у підтримці державної стабільності, легітимності політичних інститутів та консолідації суспільства. Він дозволяє оцінювати вплив інформаційних загроз на політичні процеси та ефективність державних стратегій у протидії гібридним впливам. Соціологічний та психологічний аспекти акцентують увагу на формуванні колективної свідомості, оцінюванні впливу дезінформації та маніпуляцій на поведінку громадян, що є важливим для програм медіаосвіти та розвитку критичного мислення. Технічний та кібернетичний підхід спрямований на захист інформаційних систем і мереж від кібератак та несанкціонованого втручання, використовуючи алгоритми штучного інтелекту та автоматизовані системи моніторингу для виявлення та нейтралізації загроз у реальному часі. Правовий підхід визначає межі державного втручання, забезпечує баланс між безпекою та демократичними цінностями і регламентує координацію дій між національними та міжнародними структурами. Комплексне застосування цих підходів дозволяє формувати цілісний та адаптивний механізм інформаційної безпеки, здатний протидіяти сучасним загрозам у соціальному, політичному та технологічному вимірах.

Інтеграція політологічного, соціально-психологічного, технічного та правового підходів дозволяє розглядати інформаційну безпеку як системний феномен, що одночасно є предметом наукового аналізу, об’єктом державної політики та інструментом соціального регулювання. Такий підхід забезпечує комплексне розуміння інформаційних загроз, дає можливість розробляти ефективні стратегії їхньої нейтралізації, підвищувати стійкість суспільства, забезпечувати функціонування політичних інститутів і формувати надійну систему державного управління інформаційним простором у сучасних умовах глобалізованої інформаційної взаємодії та гібридних конфліктів.

Сучасні теорії інформаційної безпеки дозволяють розглядати проблему з різних перспектив. Теорія інформаційної безпеки підкреслює роль інформації як стратегічного ресурсу та формування контрольних механізмів для забезпечення її конфіденційності, цілісності та доступності. Теорія інформаційної війни акцентує увагу на стратегічному та мережевому використанні інформації в умовах конфліктів. Теорія мотивації захисту пояснює механізми формування поведінки користувачів і їх готовність реагувати на загрози. Модернізаційна теорія фокусується на соціально-технологічних трансформаціях, що впливають на інформаційні потоки та вразливість систем.

У політологічному контексті методи дослідження інформаційної безпеки інтегрують кількісні та якісні підходи, аналітичні та експертні інструменти, забезпечуючи комплексне дослідження взаємозв’язку інформаційного середовища з політичними процесами. Використання цих методів дозволяє виявляти тенденції, оцінювати ефективність політик і стратегій, прогнозувати розвиток загроз і формувати науково обґрунтовані рекомендації щодо забезпечення національної та інформаційної безпеки.

Нормативно-правова база інформаційної безпеки в політологічному контексті постає не лише як сукупність юридичних норм, а як комплексний інструмент державної влади та засіб політичного управління інформаційними процесами. Вона визначає правила взаємодії між державою, громадянським суспільством та окремими політичними акторами, формує легітимність

державних дій у сфері інформації та окреслює межі допустимого втручання у публічний дискурс. Крім того, вона забезпечує правові механізми контролю за інформаційними потоками, що дає змогу державі регулювати процеси комунікації у суспільстві відповідно до стратегічних цілей.

Міжнародні правові акти встановлюють загальні рамки та принципи забезпечення інформаційної безпеки, формують стандарти поведінки держав у глобальному інформаційному просторі та сприяють створенню узгодженого підходу до реагування на транснаціональні загрози. Серед них – протидія кібершпигунству, дезінформаційним кампаніям та іншим формам інформаційного впливу. Міжнародне право не лише забезпечує легітимність дій держав у міжнародній спільноті, а й стимулює розвиток внутрішніх політик та стратегій, спрямованих на захист інформаційного простору.

Національне законодавство конкретизує міжнародні принципи з урахуванням внутрішніх політичних умов, стратегічних інтересів держави та соціально-культурних особливостей суспільства. В Україні нормативно-правова база у сфері інформаційної безпеки відображає процеси інституціоналізації державної інформаційної політики та трансформації концепції інформаційної безпеки як складової національної безпеки. Вона визначає повноваження ключових політичних і державних акторів, регламентує процедури моніторингу та реагування на інформаційні загрози, встановлює межі державного втручання в інформаційний простір і формує баланс між пріоритетами національної безпеки та дотриманням демократичних свобод, таких як свобода слова, право на доступ до інформації та право на приватність.

Крім того, нормативно-правова база слугує інструментом стратегічного планування інформаційної політики держави. Вона дозволяє визначати ключові напрями розвитку інформаційного середовища, інтегрувати національні інтереси в міжнародний контекст і забезпечувати координацію між різними інституційними структурами - від органів виконавчої влади до спеціалізованих центрів кібербезпеки та стратегічних комунікацій. У підсумку вона виступає як комплексний механізм, який поєднує правові, політичні та стратегічні

інструменти управління, забезпечуючи стабільність політичної системи та ефективний захист від сучасних інформаційних загроз.

У сучасних умовах соціальні мережі трансформувалися з інструментів міжособистісної комунікації у повноцінні платформи стратегічного політичного впливу, що відіграють ключову роль у реалізації гібридних стратегій. Їхня специфіка полягає у поєднанні технологічних можливостей миттєвого поширення інформації з соціально-психологічними механізмами формування громадської думки, що робить їх особливо ефективними у конфліктах немілітарного характеру. У межах гібридної війни соціальні мережі функціонують як інструмент непрямого впливу, здатний модифікувати політичну поведінку мас без застосування відкритого примусу.

Однією з ключових особливостей соціальних платформ є алгоритмічна персоналізація контенту, яка ґрунтується на аналізі попередньої активності користувачів. У результаті цього формується явище так званих «інформаційних бульбашок» або «ехо-камер», у межах яких індивід систематично отримує повідомлення, що підтверджують його вже наявні політичні погляди та ціннісні орієнтації. Така структура інформаційного споживання знижує рівень когнітивної відкритості до альтернативних позицій, послаблює критичне мислення та сприяє радикалізації суспільних груп. У політичному вимірі це призводить до зростання ідеологічної поляризації, фрагментації публічного простору та ускладнення демократичного діалогу.

У контексті гібридних війн використання соціальних мереж виходить далеко за межі класичних моделей пропаганди, які передбачали односторонню трансляцію повідомлень від суб’єкта впливу до масової аудиторії. Цифрові платформи забезпечують можливість ведення динамічних, багаторівневих кампаній впливу в режимі реального часу, що дозволяє оперативно реагувати на політичні події, коригувати наративи та адаптувати меседжі до різних цільових груп. Такі кампанії спрямовані насамперед на делегітимацію політичних інститутів, підрив довіри до традиційних медіа та органів державної влади, а також на формування відчуття соціальної нестабільності й кризи управління.

Важливу роль у цьому процесі відіграють інструменти таргетованої реклами, автоматизовані бот-мережі та штучно створені акаунти, які імітують активність реальних користувачів. Вони дозволяють масово поширювати дезінформацію, фейкові новини та наративи, водночас створюючи ілюзію широкої суспільної підтримки певних ідей або політичних позицій. Особливістю такого впливу є апеляція не до раціонального аналізу, а до емоційної сфери - страху, обурення, тривоги або недовіри, що значно підвищує ефективність маніпуляції та ускладнює її виявлення.

Соціальні платформи в сучасних політичних процесах дедалі частіше виступають як інфраструктурна основа для мобілізації колективної дії та організації протестних рухів. Їхня здатність забезпечувати миттєву комунікацію, горизонтальні зв’язки між учасниками та швидку циркуляцію мобілізаційних меседжів значно знижує бар’єри для політичної участі й сприяє активізації громадянського суспільства. У цьому контексті соціальні мережі можуть виконувати позитивну функцію, слугуючи простором реалізації свободи зібрань, самовираження та політичної самоорганізації.

Водночас у межах гібридних конфліктів цей мобілізаційний потенціал набуває амбівалентного характеру та може бути використаний як інструмент деструктивного зовнішнього впливу. Через соціальні платформи створюються штучні інформаційні імпульси, що стимулюють протестну активність, посилюють радикальні настрої або провокують загострення соціально-політичних протиріч. Застосування координованих мереж акаунтів і автоматизованих систем поширення контенту дозволяє формувати ілюзію масової підтримки певних ідей чи рухів, що спотворює реальний баланс суспільних настроїв і підриває легітимність політичних рішень.

Для держави така динаміка становить комплексний виклик у сфері національної та інформаційної безпеки. Інституційні механізми моніторингу та реагування на інформаційні загрози у соціальних мережах часто виявляються недостатньо ефективними через надзвичайно високі темпи поширення контенту та складність ідентифікації джерел впливу. Як наслідок, дезінформаційні

кампанії та маніпулятивні меседжі здатні охоплювати значні аудиторії ще до того, як державні органи формують і комунікують офіційну позицію, що посилює ефект недовіри та інформаційної дезорієнтації суспільства.

Окремою проблемою залишається обмеженість правових інструментів протидії інформаційним загрозам у соціальних мережах. Держава змушена діяти в умовах постійного балансу між потребою забезпечення національної безпеки та збереженням демократичних свобод, насамперед свободи слова й права на доступ до інформації. Надмірне регулювання може призвести до звуження громадянських прав і політичної конкуренції, тоді як недостатнє - створює сприятливе середовище для зовнішнього втручання та маніпуляції громадською думкою. Це зумовлює необхідність розроблення комплексної державної політики, яка поєднувала б правові, інституційні та комунікативні інструменти протидії гібридним загрозам у соціальних мережах без підриву демократичних засад політичної системи.

У сучасному політичному просторі соціальні мережі функціонують не лише як нейтральні канали обміну інформацією, а як повноцінна арена боротьби за формування суспільної свідомості. Саме в межах цифрового середовища відбувається конкуренція між політичними наративами, ціннісними орієнтаціями та інтересами різних акторів - держав, політичних еліт, громадських рухів і зовнішніх суб’єктів впливу. Така конкуренція має асиметричний характер, оскільки успіх у ній визначається не стільки ресурсами традиційної влади, скільки здатністю контролювати інтерпретацію подій, символічні смисли та емоційні реакції аудиторії.

Центральне місце серед інструментів гібридної війни у соціальних мережах посідають інформаційно-психологічні операції, спрямовані на безпосередній вплив на когнітивну сферу індивіда.

У політичному вимірі ІПсО виступають механізмом трансформації суспільних уявлень, що впливають на політичну ідентичність, систему цінностей і моделі соціальної поведінки. Поєднуючи класичні методи психологічного тиску - пропаганду, дезінформацію, маніпуляцію стереотипами -

з інноваційними цифровими технологіями, такі операції забезпечують високий рівень адаптивності та масштабності впливу, що суттєво ускладнює їх виявлення та нейтралізацію.

Особливістю сучасних інформаційно-психологічних операцій є активне використання автоматизованих інструментів впливу. Бот-мережі забезпечують масове тиражування ідентичних або схожих повідомлень, створюючи ілюзію домінування певної позиції в публічному дискурсі та формуючи ефект так званого «суспільного консенсусу». Така штучна видимість підтримки здатна змінювати поведінку користувачів, знижувати рівень критичного осмислення інформації та підштовхувати до конформізму в умовах інформаційного перевантаження.

Важливим інструментом ІПсО є таргетована реклама, яка дозволяє здійснювати персоналізований вплив на окремі соціальні групи. Завдяки використанню великих масивів даних аудиторія сегментується за соціально-демографічними, політичними та психологічними характеристиками, що дає змогу адаптувати меседжі до рівня емоційної вразливості конкретних груп. У результаті інформаційний вплив набуває точкового характеру та стає значно ефективнішим, водночас залишаючись малопомітним для широкого загалу.

Додаткові загрози у контексті гібридної війни створює застосування deepfake-технологій, які радикально ускладнюють розмежування між достовірною та сфальсифікованою інформацією. Маніпулятивні відео- та аудіоматеріали можуть використовуватися для дискредитації політичних лідерів, підриву довіри до інститутів влади або провокування соціальних конфліктів ще до моменту їх спростування. У політичному сенсі це посилює кризу довіри в інформаційному просторі та підриває самі основи публічної комунікації, що робить інформаційно-психологічні операції одним із найнебезпечніших інструментів сучасної гібридної війни.

Використання технологій штучного інтелекту істотно підвищує ефективність інформаційно-психологічних операцій, оскільки забезпечує високий рівень автоматизації процесів поширення меседжів та дозволяє в

режимі реального часу адаптувати інформаційні кампанії до реакцій цільової аудиторії. Алгоритми машинного навчання аналізують поведінкові патерни користувачів, їхню емоційну залученість і комунікативну активність, що дає змогу оперативно коригувати наративи, інтенсивність впливу та канали поширення контенту. У результаті ІПсО набувають гнучкого, динамічного та адаптивного характеру, що суттєво ускладнює їх своєчасне виявлення та нейтралізацію з боку державних і громадських інституцій.

Стратегічні цілі таких операцій виходять за межі короткострокової дезінформації або маніпуляції окремими подіями. У політичному вимірі вони спрямовані на довготривалу трансформацію суспільних настроїв, зміну моделей політичної поведінки та поступове формування вигідних агресору уявлень про реальність. Особливу небезпеку становить навмисне культивування відчуття безсилля, фрустрації та недовіри до інститутів державної влади, що підриває легітимність політичної системи зсередини та послаблює здатність суспільства до консолідованого спротиву зовнішнім загрозам.

В умовах збройного конфлікту або широкомасштабної гібридної війни такий вплив набуває критичного значення, оскільки єдність, соціальна стійкість і довіра до державних інституцій виступають ключовими чинниками національної безпеки. Руйнування цих чинників через інформаційно-психологічний тиск може мати не менш руйнівні наслідки, ніж прямі військові дії. Саме тому протидія ІПсО повинна розглядатися як пріоритетний напрям державної політики у сфері кібербезпеки та стратегічних комунікацій, що передбачає поєднання технологічних інструментів (систем моніторингу, алгоритмів виявлення бот-мереж і координованої неавтентичної поведінки) з інституційними та соціально-освітніми заходами, спрямованими на підвищення рівня медіаграмотності й розвитку критичного мислення громадян.

Паралельно з інформаційно-психологічними операціями дедалі більшого значення набувають кіберзагрози та технічні інструменти гібридної війни, які перетворилися на критично важливий чинник національної безпеки. Кібератаки різного типу - від масових DDoS-операцій до складних вірусних кампаній,

подібних до NotPetya, - здатні одночасно впливати на різні сфери функціонування держави та суспільства. Їхніми об’єктами стають органи державної влади, фінансові установи, комунальні служби, підприємства приватного сектору та елементи критичної інфраструктури.

Наслідки таких атак виходять далеко за межі технічних збоїв, адже вони призводять до порушення логістичних процесів, значних економічних втрат, зниження рівня довіри до державних інституцій та дестабілізації повсякденного життя громадян. У політичному контексті кіберзагрози слід розглядати як складову комплексної гібридної стратегії, спрямованої на ослаблення керованості держави, підрив її інституційної спроможності та створення відчуття системної вразливості. Це зумовлює необхідність інтегрованого підходу до забезпечення кібер- та інформаційної безпеки, що поєднує технологічний захист, ефективне державне управління та стійкість суспільства до зовнішніх впливів.

Особливо високий рівень загрози становлять кібероперації, інтегровані з інформаційними кампаніями, оскільки поєднання технічного та психологічного впливу значно посилює ефект на масову свідомість. Такі комплексні дії формують у населення відчуття хаосу, невизначеності та втрати контролю, стимулюють панічні настрої і підривають довіру до державних інституцій. У цьому контексті кібератака перестає бути виключно технічним інцидентом і перетворюється на стратегічний інструмент гібридної війни, спрямований на контроль над інформаційним простором та опосередкований вплив на політичні процеси і соціальну поведінку громадян.

Слід підкреслити, що сучасні кібероперації дедалі частіше набувають комплексного, мультисекторного характеру, охоплюючи одночасно різні сфери життєдіяльності держави та суспільства. До таких сфер належать енергетична та транспортна інфраструктури, фінансовий сектор, канали комунікації, державні сервіси та ключові соціальні інститути. Широкий спектр цілей ускладнює своєчасне виявлення та нейтралізацію загроз, підвищує ризики

системних збоїв і вимагає від держави інтегрованого підходу до забезпечення кібербезпеки.

Ефективна протидія комплексним кіберзагрозам передбачає поєднання технічних, організаційних та правових заходів, що охоплюють розробку алгоритмів виявлення атак, моніторинг критичних інформаційних потоків, правове регулювання діяльності в кіберпросторі та координацію дій різних державних і недержавних структур. Такий системний підхід дозволяє не лише зменшити прямий технічний вплив атак, а й мінімізувати їхній психологічний та політичний ефект, що критично важливо для збереження стабільності політичної системи та стійкості суспільства в умовах гібридних загроз.

Дослідження ключових кейсів інформаційного впливу на Україну в період 2014–2025 рр. показало, що інформаційна агресія проти нашої держави носить системний, багаторівневий і довготривалий характер. Вона реалізується через широке поєднання інструментів, включно з дезінформаційними кампаніями, маніпуляціями в соціальних мережах, інформаційно-психологічними операціями та спрямованими кібератаками на критичну інфраструктуру. Такий комплексний підхід свідчить про стратегічне планування інформаційного впливу, метою якого є не лише дискредитація державних інститутів, а й формування сприятливих для агресора настроїв серед населення та послаблення суспільної стійкості.

Аналіз поширених фейкових наративів демонструє систематичне використання російськими пропагандистами соціальних мереж як основного каналу дезінформації. Серед ключових тем - нібито значні втрати українських військових, звинувачення Збройних Сил України у «жорстокості» та порушеннях військової дисципліни, а також поширення тверджень про корупційні схеми за участю західної допомоги та США. Для підвищення правдоподібності таких повідомлень використовуються підроблені логотипи відомих медіа, цитати публічних осіб, відеоматеріали та інші елементи верифікаційного фасаду, що створюють ілюзію достовірності та авторитетності джерела.

Найактивнішими платформами для поширення таких повідомлень залишаються Telegram, X, ВКонтакте, TikTok та YouTube. Вони забезпечують не лише швидке охоплення широких аудиторій, а й активну взаємодію через репости, коментарі та лайки, що сприяє вірусному поширенню контенту серед української, російської та міжнародної спільнот. Внаслідок цього дезінформаційні кампанії здатні впливати на формування суспільних наративів, спотворювати сприйняття реальності та підривати довіру до державних інституцій, що робить інформаційний вплив ефективним інструментом у межах гібридної війни.

Аналіз українського та світового досвіду протидії інформаційним загрозам демонструє, що ефективний захист від дезінформації та інформаційно-психологічного впливу потребує комплексного поєднання технічних, інституційних і соціальних заходів. Технічна складова передбачає створення сучасних систем кіберзахисту та інформаційного моніторингу, впровадження безперервного аналізу інформаційних потоків, а також використання алгоритмів штучного інтелекту для оперативного виявлення та нейтралізації дезінформаційних кампаній у режимі реального часу. Такі підходи дозволяють зменшити масштаб негативного впливу на суспільну свідомість і оперативно реагувати на нові загрози.

Інституційна складова передбачає вдосконалення нормативно-правової бази у сфері інформаційної безпеки та стратегічних комунікацій, створення і розвиток сталих механізмів державного реагування на інформаційні загрози, а також посилення координації між силовими, інформаційними та дипломатичними структурами. Значну роль відіграє інтеграція України у міжнародні мережі протидії дезінформації, включно з платформами ЄС, НАТО та ОБСЄ, що забезпечує обмін досвідом, координацію операцій та доступ до сучасних технологічних рішень.

Соціальна складова включає створення й функціонування спеціалізованих державних структур, які відповідальні за стратегічні комунікації та інформаційну безпеку. До них належать, зокрема, Центр стратегічних

комунікацій та інформаційної безпеки, урядові платформи для спростування фейків, а також інші органи, що займаються медіаграмотністю та просвітницькими кампаніями серед населення. Поєднання цих трьох складових – технічної, інституційної та соціальної - створює системний механізм протидії інформаційним загрозам, здатний забезпечити стабільність політичної системи та підвищити стійкість суспільства до гібридних впливів.

Соціально-освітня складова є не менш важливою у забезпеченні інформаційної стійкості держави та передбачає формування критичного мислення серед населення, розвиток медіаграмотності, а також підтримку незалежних журналістських ініціатив і платформ фактчекінгу, таких як StopFake, VoxCheck та Detector Media. Ці заходи дозволяють зменшити вразливість громадян до маніпуляцій та інформаційно-психологічних операцій, сприяють усвідомленому сприйняттю інформації та формують культуру інформаційної відповідальності, що є невід'ємним елементом демократичного суспільства.

Підвищення стійкості інформаційного простору України можливе лише за умови комплексного, багаторівневого підходу, який інтегрує технічні, інституційні та соціально-освітні заходи. До технічних заходів належать розвиток систем кіберзахисту, аналітики та моніторингу інформаційних потоків; інституційні рішення передбачають вдосконалення законодавства, розвиток державних стратегічних комунікацій і міжнародне партнерство у сфері протидії дезінформації; соціальні ініціативи включають медіаосвіту, незалежну журналістику та фактчекінг.

Особливу значущість набуває перехід до проактивної моделі інформаційної безпеки, що передбачає не лише реагування на інформаційні загрози, а й формування власних позитивних наративів. Такі наративи спрямовані на зміцнення національної єдності, підвищення довіри до демократичних інститутів та розвиток колективної стійкості суспільства до зовнішніх впливів, навіть в умовах гібридної війни. У цьому контексті комплексний підхід забезпечує не тільки захист від дезінформації, а й стратегічне зміцнення

суспільної свідомості, що є ключовим чинником національної безпеки та стабільності держави.

За результатами дослідження наукова гіпотеза підтвердилася. Встановлено, що інституційні чинники інформаційно-безпекової політики України в умовах гібридної війни справді мають самобутній механізм функціонування, зумовлений специфікою українського політичного контексту, характером російської інформаційної агресії та особливостями середовища соціальних мереж. Аналіз кейсів 2014–2025 рр. підтвердив, що результативність протидії інформаційним загрозам визначається не лише реактивним стримуванням, а насамперед проактивною спроможністю інституційної системи формувати стійкість суспільства, підтримувати достовірний інформаційний порядок денний і мінімізувати ефекти дезінформації та маніпуляцій. Водночас підтверджено, що ефективна імплементація міжнародного досвіду потребує не механічного запозичення, а його адаптації до національних умов війни, правових рамок і суспільних запитів, що й визначає стратегічний пріоритет нарощування інституційного потенціалу у сфері інформаційної безпеки.

СПИСОК ВИКОРИСТАНИХ ДЖЕРЕЛ

1. Адамович Н. Російський Max та інші новації для тотального контролю в мережі й ізоляції окупованих територій. *Зміна.* 09 Вересня 2025. URL: https://zmina.info/articles/rosijskyj-max-ta-inshi-novacziyi-dlya-totalnogo-kontrolyu-v-merezhi-ta-izolyacziyi-okupovanyh-terytorij/ (дата звернення: 10 вересня 2025 р.)

2. Алещенко В. Психологічні аспекти інформаційної війни**.** *Вісник Київського національного університету імені Тараса Шевченка. Військово-спеціальні науки.* 2022. № 2 (50). С. 27-31.

3. «Американські біолабораторії в Україні». Як Росія продовжує ширити брехливі теорії змов для дискредитації США та України. *Голос Америки.* 30 січня 2025. URL: https://www.holosameryky.com/a/russia-weds-biolab-organ-harvesting-conspiracies-to-discredit-us-ukraine/7956938.html (дата звернення: 10 серпня 2023 р.).

4. Андрущенко Д. Інформаційно-психологічні операції. Ірак. 8 квіт. 2025. URL: https://www.psdinfo.pro/post/інформаційно-психологічні-операції-ірак (дата звернення: 10 липня 2023 р.).

5. Аніщенко О. Б. Інформаційно-психологічна протидія підрозділів Збройних сил України під час міжнародної операції з підтримання миру і безпеки в Іраку (2003-2005 рр.): організаційно-управлінський аспект аналізу. *Державне управління: удосконалення та розвиток*. 2021. № 11. URL: http://www.dy.nayka.com.ua/pdf/11_2021/32.pdf

6. «Анкоридзька лихоманка». Як російська пропаганда намагається деморалізувати українців перед зустріччю на Алясці. *Центр стратегічних комунікацій та інформаційної безпеки*. 13 серпня 2025 URL: https://ms.detector.media/propaganda-ta-vplivi/post/38312/2025-08-13-ankorydzka-lykhomanka-yak-rosiyska-propaganda-namagaietsya-demoralizuvaty-ukraintsiv-pered-zustrichchyu-na-alyastsi/ (дата звернення: 10 вересня 2025 р.).

7. Арабаджиєв Д. Ю., Сергієнко Т. І. Маніпулювання свідомістю суспільства в умовах інформаційної та гібридної війни в Україні. *Гілея: науковий вісник.* 2019. Вип.146 (3). С. 12-15.

8. Архипов О, Архипова Є. Особливості розуміння понять «інформаційна безпека» та «безпека інформації». *Інформаційні технології та безпека: основи забезпечення інформаційної безпеки* (ІТБ-2014): Матеріали XIV міжнародної науково-практичної конференції. К.: ІПРІ НАН України, 2014. С.18-30.

9. Архипова Є. О. Соціально-філософське осмислення поняття «інформаційна безпека». *Вісник НТУУ «КПІ». Філософія. Психологія. Педагогіка: збірник наукових праць*. 2011. № 3(33). С. 7–11.

10. Бабишена О. YouTube видалив канал пропагандистки Діани Панченко, підозрюваної у держзраді. URL: https://espreso.tv/suspilstvo-youtube-vidaliv-kanal-propagandistki-diani-panchenko-pidozryuvanoi-u-derzhzradi (дата звернення: 2 вересня 2025 р.).

11. Базиляк І.О. Хактивізм як феномен сучасного кіберпростору. *Інформаційна безпека суспільства в умовах дії правового режиму воєнного стану та повоєнний період* : зб. матеріалів (Київ, 29 трав. 2025 р.) / Редкол. : О. С. Тарасенко та ін. Київ : Нац. акад. внутр. справ, 2025. С.117-119.

12. Баран М. В. Адміністративно-правове забезпечення інформаційної безпеки в Україні: дис. … д-ра філософії: 081 «Право». Львів. 2022. 242 с.

13. Биков О. М. Інформаційна безпека: правовий та культурологічний виміри. *Аналітично-порівняльне правознавство*. 2024. № 2. С. 396-402.

14. Білял А. Гібридна війна – нові загрози, складність і «довіра» як антидот. URL: https://www.nato.int/docu/review/uk/articles/2021/11/30/gbridna-vjna-nov-zagrozi-skladnst-dovra-yak-antidot/index.html (дата звернення: 2 вересня 2025 р.)

15. Білодід К.С. Соціальні мережі як інструмент інформаційної війни: атаки, фейки та протидія. URL: https://elar.navs.edu.ua/items/03f59f10-8be2-4529-8f69-598d0287ffaf (дата звернення: 22 вересня 2023 р.).

16. Бішко І. Google та Jigsaw запускають в Україні ініціативу з медіаграмотності для підвищення стійкості до дезінформації. URL: https://ukraine.googleblog.com/2024/07/google-jigsaw.html (дата звернення: 10 березня 2025 р.).

17. Благодарний А. М., Штельмах О. В. Організаційні аспекти протидії інформаційній агресії як складовій гібридної війни. *Інформаційна безпека людини, суспільства, держави.* 2015. № 3. С. 48-54.

18. Богданьок О. Російська пропаганда поширює фейковий «лист Шмигаля» про евакуацію держустанов - ЦПД. URL: https://suspilne.media/1058665-rosijska-propaganda-posirue-fejkovij-list-smigala-pro-evakuaciu-derzustanov-cpd/ (дата звернення: 10 червня 2025 р.)..

19. Богуш В. Інформаційна безпека держави / В. Богуш, О. Юдін; [Гол. ред. Ю.О. Шпак]. К.: «МК-Прес», 2005. 432 с.

20. Боднар І. Р. Інформаційна безпека як основа національної безпеки *Mechanism of Economic Regulation*. 2014. №1. С. 68-75.

21. Бразалук М.Ю. Вплив інформаційно-психологічних операцій на морально-психологічний стан військовослужбовців та цивільних осіб у кіберпросторі. Інформаційна безпека суспільства в умовах дії правового режиму воєнного стану та повоєнний період : зб. матеріалів (Київ, 29 трав. 2025 р.) / Редкол. : О. С. Тарасенко та ін. Київ : Нац. акад. внутр. справ, 2025. С.29-32.

22. Брайлян Є. Як стратегічні комунікації допомагають Україні налагодити міжнародну співпрацю з протидії ворожій дезінформації. URL: https://armyinform.com.ua/2021/12/09/yak-strategichni-komunikacziyi dopomagayut-ukrayini-nalagodyty-mizhnarodnu-spivpraczyu-z-protydiyi-vorozhij-dezinformacziyi/ (дата звернення: 22 червня 2024 р.).

23. Будь на сторожі якісної інформації – ставай частиною спільноти «Детектора медіа». URL: https://disinfo.detector.media (дата звернення: 22 вересня 2025 р.).

24. Буник М. Комп'ютерне моделювання як метод дослідження соціальних систем. *Методологія політичної науки: матеріали Всеукраїнської*

наукової конференції. Перші методологічні читання /Укл. Денисенко В.М., Угрин Л.Я. Львів: ЛНУ 2010. С.49-50

25. Бутенко О. П. Комплаєнс-ризики в інноваційній діяльності підприємства. *Конкурентоспроможність та інновації: проблеми науки та практики*: Тези доповідей VIII Міжнародної науково-практич-ної інтернет-конференції, 24 листопада 2023 р. Харків : ФОП Лібуркіна Л. М., 2023. С. 144–147. URL: https://www.hneu.edu.ua/wp-content/uploads/2023/12/TEZU_2023-2.pdf.

26. Важливість інформаційної безпеки під час війни: представниця Центру стратегічних комунікацій взяла участь у форумі для молоді. Spravdi : веб-сайт. URL: https://spravdi.gov.ua/vazhlyvist-informaczijnoyi-bezpeky-pid-chas-vijny-predstavnyczya-czentru-strategichnyh-komunikaczij-vzyala-uchast-u-forumi-dlya-molodi/# (дата звернення: 12 грудня 2025 р.).

27. Варналій Є. О., Єсіна О. Г. Хакерство як соціальне явище. *Інформатика та інформаційні технології*: матер. конф. (20 квітня 2015 р.). Одеса: ОНЕУ, 2015. С. 107-109.

28. Валюшко І. О. Інформаційна безпека України: трансформація законодавства після російського вторгнення. *Історико-політичні студії*. 2017. №2 (8). С. 30–43.

29. Васильченко Б. Історія російського терору: Іван Грозний, Петро І, Сталін та Путін як продукти імперії зла. URL: https://umoloda.kyiv.ua/number/3514/196/137974/ (дата звернення: 3 вересня 2024 р.).

30. Васильчук Є. О. Російський екстремізм в Україні: [монографія]. Черкаси: Видавець Ольга Вовчок, 2015. 120 с.

31. «Ваш допис було вилучено». Вплив соціальних мереж на український інформаційний простір після початку повномасштабного вторгнення. URL: https://cedem.org.ua/wp-content/uploads/2024/01/War-Impact-Social-Media.pdf (дата звернення: 13 вересня 2025 р.).

32. Вербівський Д. С., Сікора Я. Б., Усата О. Ю. Медіаграмотність як один зі складників процесу підготовки сучасного педагога професійного навчання. *Науковий вісник Ужгородського університету.* 2021. № 1 (48). С. 69–72.

33. Веселова В. Ворота анексії: як у Криму захоплювали аеропорти й переправу. URL: https://ua.krymr.com/a/28340389.html (дата звернення: 3 вересня 2024 р.).

34. Визначення хактивізму. Веб-сайт. URL : https://www.vpnunlimited.com/ua/help/cybersecurity/hacktivism?srsltid=AfmBOoqlLPqnuffcwGOCopY74hYpgJuAilxtbEHqu0F_JSvUcw3NwIhc (дата звернення: 22 серпня 2024 р.).

35. Відеофейк: Військові 47-ї ОМБр заявили про вихід у СЗЧ - відео. URL: https://voxukraine.org/videofejk-vijskovi-47-yi-ombr-zayavyly-pro-vyhid-u-szch-video (дата звернення: 22 вересня 2025 р.).

36. Войтко О. В., Солонніков В. Г. Державна інформаційна політика - основа забезпечення інформаційної безпеки в умовах гібридної війни. *Актуальні проблеми управління інформаційною безпекою держави*. 2021. №19. URL: https://eportfolio.kubg.edu.ua/data/conference/7238/document.pdf#page=19 (дата звернення: 12 лютого 2025 р.).

37. Войтович Н. Розвиток навичок критичного мислення та медіаграмотності у населення як спосіб протидії російській пропаганді в інформаційній війні. *Журналістика майбутнього: виклики, тенденції, перспективи розвитку:* матеріали Міжнародної науково-практичної конференції (Львів, 18–19.10. 2022). Львів : Простір-М, 2022. С.297-303.

38. Вони кажуть, що війна в Україні – фейк. Хто ці люди. URL: https://www.bbc.com/ukrainian/features-64796700 (дата звернення: 22 липня 2024 р.).

39. В Одесі жінка під час стріму в TikTok заявила, що “чекає кремлівського вождя”, – Нацполіція. URL: https://imi.org.ua/news/v-odesi-zhinka-

pid-chas-strimu-u-tiktok-zayavyly-shho-chekaye-kremlivskogo-vozhdya-natspolitsiya-i52531 (дата звернення: 22 липня 2023 р.).

40. В окупованому Криму судитимуть блогера через коментар у соцмережі. URL: https://imi.org.ua/news/v-okupovanomu-krymu-sudytymut-blogera-cherez-komentar-u-sotsmerezhi-i52062 (дата звернення: 16 липня 2024 р.).

41. В Україні створили чат-бот, який допоможе боротися з російськими фейками. URL: https://zmina.info/news/v-ukrayini-stvoryly-chat-bot-yakyj-dopomozhe-borotysya-z-rosijskymy-fejkamy/ (дата звернення: 12 березня 2024 р.).

42. В Україні торік виявили 3600 кіберзлочинів. URL: https://www.ukrinform.ua/rubric-technology/3820631-v-ukraini-torik-viavili-3600-kiberzlociniv.html (дата звернення: 22 березня 2024 р.).

43. 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.

44. 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.

45. Галіпчак В. Вплив інформаційних технологій на захист національних інтересів в Україні: виклики та можливості. *X Міжнародна науково-практичніа 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

46. Ганжа К. Роспропаганда ширить фейк про нібито підготовку Україною провокації в пологовому будинку Краматорська, ЦПД. URL: https://espreso.tv/viyna-z-rosiyeyu-rospropaganda-shirit-feyk-pro-nibito-pidgotovku-ukrainoyu-provokatsii-v-pologovomu-budinku-kramatorska-tspd (дата звернення:12 вересня 2025 р.).

47. Гайдамашко О. YouTube: історія розквіту найпопулярнішого відеосервісу. URL: https://24tv.ua/tech/youtube-istoriya-rozkvitu-

naypopulyarnishogo-novini-tehnologiy_n1540446 (дата звернення: 22 грудня 2024 р.).

48. Геноцидна риторика Кремля як інструмент інформаційної війни: кейс публікацій «РИА Новости» та Кирила Стрєльнікова. «Іншого варіанту нема». Навіщо Москва знов лякає українців геноцидом. URL: https://spravdi.gov.ua/inshogo-variantu-nema-navishho-moskva-znov-lyakaye-ukrayinczіv-genoczydom/ (дата звернення: 12 липня 2025 р.)..

49. Гирич І. «Русскій мір»: від концепту «Москва – третій Рим» до рашизму. URL: https://www.prostir.ua/?blogs=russkij-mir-vid-kontseptu-moskva-tretij-rym-do-rashyzmu (дата звернення: 22 червня 2024 р.).

50. Гнатюк Р. Соціальні мережі: співвідношення позитиву і негативу? URL: https://zn.ua/ukr/family/socialni-merezhi-spivvidnoshennya-pozitivu-i-negativu.html (дата звернення: 12 червня 2023 р.).

51. Головіна О. Перемога над фейками. Як фінські учні опановують майстерність медіаграмотності. URL: https://nus.org.ua/2020/03/04/peremoga-nad-fejkamy-yak-finski-uchni-opanovuyut-majsternist-mediagramotnosti/ (дата звернення: 22 вересня 2024 р.).

52. Голуб А. Кіберзлочинність у всіх її проявах: види, наслідки та способи боротьби. *Портал Гурт.* 03 жовтня 2016. URL: http://gurt.org.ua/articles/34602/ (дата звернення: 12 червня 2023 р.).

53. Гончаренко Г. А. До проблеми визначення та розмежування дефініцій «інформаційна безпека» і «кібербезпека». *Аналітично-порівняльне правознавство.* 2024. №5. С.466-474.

54. Гончаров М. Дослідження поняття «інформаційна безпека». *Науковий вісник Ужгородського Національного Університету. Серія Право.* 2024. Випуск 82: частина 2. С.34-37.

55. Горбай Б Герменевтичний аналіз як методологічна основа дослідження політичної реальності. *Методологія політичної науки: матеріали Всеукраїнської наукової конференції. Перші методологічні читання* /Укл. Денисенко В.М., Угрин Л.Я. Львів: ЛНУ 2010. С.45-48

56. Горбулін В. «Гібридна війна» як ключовий інструмент російської геостратегії реваншу. *Дзеркало тижня – Україна*. 2015. № 2. 24 січня. С. 3.

57. Гороховський О. М. Фактчек як тренд розслідувань: можливості та перспективи : практичний посібник. Дніпро : ЛІРА, 2017. 133 с.

58. Грайворонський, М. В. Сучасні підходи до забезпечення кібернетичної безпеки. *Матеріали XIII Всеукраїнської науково-практичної конференції студентів, аспірантів та молодих вчених «Теоретичні і прикладні проблеми фізики, математики та інформатики»*, м. Київ, 21-23 травня 2015. Київ : НТУУ «КПІ». 2015. С. 10-17.

59. Гриник Р.О., Пилипенко В.М. Кібертероризм як нова форма міжнародного тероризму. Актуальні задачі та досягнення у галузі кібербезпеки. Матеріали Всеукраїнської науково-практичної конференції 34-35 листопада 2016 року м. Кропивницький. 2016. С. 61-62. URL: https://sci.ldubgd.edu.ua/bitstream/123456789/3203/1/13.pdf (дата звернення: 5 червня 2025 р.).

60. Гулай В. В. Загрози інформаційно-психологічній безпеці особи в реаліях інформаційно-психологічної війни як складової «гібридної війни» Російської Федерації проти України. *Військово-науковий вісник*. 2016. Вип. 25. С. 233-244.

61. Гулай В. Маніпулятивно-пропагандистські складові загроз інформаційній безпеці в реаліях гібридної війни Російської Федерації проти України. *Studia politologica Ucraino-Polona*. 2016. Вип. 6. С. 34-42. URL:http://jnas.nbuv.gov.ua/article/UJRN-0000586926 (дата звернення: 22 грудня 2023 р.).

62. Гулак Ю. Інформаційна складова гібридної війни Російської Федерації проти України, проблемні питання та шляхи їх вирішення. Міжвідомча науково-практична конференція: "*Уроки збройної агресії Росії проти України – воєннostратегічні аспекти"*: зб. матеріалів міжв. наук-практ. конф. (Київ, 29квітня 2021 р.). К.: Національний університет оборони України імені Івана Черняховського, 2021. С.62-65. URL:

https://nuou.org.ua/assets/documents/npc-zbr-agr-rs-pr-ukr-29-04-2021.pdf (дата звернення: 22 грудня 2023 р.).

63. Гурковський В. І. Безпека як об’єкт правовідносин в умовах глобального інформаційного суспільства. *Правова інформатика*. 2010. № 2 (26). С. 72–77.

64. Гуцуляк Д. Фактчекінг як інструмент протидії дезінформації в умовах гібридних конфліктів. *Наукові праці Міжрегіональної академії управління персоналом. Філологія.* 2024. №2 (12). С.22-26.

65. 2021. Звіт про роботу Системи виявлення вразливостей і реагування на кіберінциденти та кібератаки. URL: https://cert.gov.ua/files/pdf/SOC_Annual_Report_2022.pdf (дата звернення: 22 грудня 2023 р.).

66. 2022. Звіт про роботу Системи виявлення вразливостей і реагування на кіберінциденти та кібератаки. URL: https://nsarchive.gwu.edu/sites/default/files/documents/rr9q9n-glu5j/2023-01-00-SSCIP-Vulnerability-Detection-System-and-Response-to-Cyber-Incidents-and-Cyber-Attacks-%20via-website.pdf (дата звернення: 22 грудня 2023 р.).

67. 2023. Звіт про роботу Системи виявлення вразливостей і реагування на кіберінциденти та кібератаки. URL: https://scpc.gov.ua/api/files/9c21855d-74da-45d1-90f9-5d4f6795996a (дата звернення: 22 грудня 2023 р.).

68. 2023 року кількість зареєстрованих кіберінцидентів зросла на 62,5%: звіт оперативного центру реагування на кіберінциденти ДЦКЗ . URL: https://cip.gov.ua/ua/news/2023-roku-kilkist-zareyestrovanikh-kiberincidentiv-zrosla-na-62-5-zvit-operativnogo-centru-reaguvannya-na-kiberincidenti-dckz (дата звернення: 22 грудня 2023 р.).

69. 2024. Річний звіт Системи виявлення вразливостей і реагування на кіберінциденти та кібератаки. URL: https://scpc.gov.ua/api/files/72e13298-4d02-40bf-b436-46d927c88006 (дата звернення: 22 січня 2025 р.).

70. Даниленко С., Убийконь К. Мова ворожнечі у месенджері telegram та соціальній мережі tiktok: форми прояву під час повномасштабного вторгнення росії в Україну. *Регіональні студії*. 2024. №39. С.22-30.

71. «Демократичний захист від дезінформації»: рекомендації Atlantic Council. URL: https://ms.detector.media/mediaanalitika/post/20858/2018-03-27-demokratychnyy-zakhyst-vid-dezinformatsii-rekomendatsii-atlantic-council/ (дата звернення: 22 грудня 2023 р.).

72. 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.

73. Дерев'янко С. М. Гібридна війна: інформаційно-безпековий вимір. *Вісник Прикарпатського університету. Серія: Політологія*. 2024. Вип. 18. С. 11–18.

74. 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.

75. Державна служба спеціального зв'язку та захисту інформації України. Access Denied. URL: https://cip.gov.ua/ua/news/uryadova-komanda-cert ua-v-2023-roci-opracyuvala-2543-kiberincidenti. (дата звернення: 12 липня 2024 р.).

76. Державний центр кіберзахисту Державної служби спеціального зв'язку та захисту інформації України. URL: https://scpc.gov.ua/uk (дата звернення: 12 грудня 2024 р.).

77. Деркаченко Я. Інформаційно-психологічні операції як сучасний інструмент геополітики. *Глобальна організація союзницького лідерства*. 2016. URL: http://goal int.org/informacijno-psixologichni-operacii-yak-suchasnij-instrument-geopolitiki/ (дата звернення: 22 грудня 2024 р.).

78. Діордіца І. В. Адміністративно-правове регулювання кібербезпеки України. Дисертація на здобуття наукового ступеня доктора юридичних наук зі

спеціальності 12.00.07 – адміністративне право і процес; фінансове право; інформаційне право. Запорізький національний університет, Запоріжжя, 2018. 521 с.

79. Діордіца І. В. Класифікація кіберзагроз та їх легітимація у нормативно-правових актах України. *Підприємництво, господарство і право*. 2017. № 10. С. 206-211.

80. Діордіца І. В. Поняття та зміст кіберзагроз на сучасному етапі. *Підприємництво, господарство і право*. 2017. № 4. С. 99-107.

81. Доктрина інформаційної безпеки України. URL: https://www.president.gov.ua/documents/472017-21374 (дата звернення: 22 січня 2023 р.).

82. Доктрина «Русский мир» як інформаційна та культурна стратегія. URL: https://www.old.nas.gov.ua/UA/Messages/Pages/View.aspx?MessageID= 8592 (дата звернення: 26 листопада 2023 р.).

83. Долженко О. Гібридна війна як інноваційний концепт сучасної геополітики / В. Мироненко. *Науковий часопис Національного педагогічного університету імені М. П. Драгоманова.* Серія 22 : Політичні науки та методика викладання соціально-політичних дисциплін : зб. наук. праць. Київ : Вид-во НПУ імені М. П. Драгоманова, 2022. Вип. 31. С. 59-72.

84. Дорошкевич А. С. Гібридна війна в інформаційному суспільстві. *Вісник Національного університету «Юридична академія України імені Ярослава Мудрого»*. Серія : Філософія, філософія права, політологія, соціологія. 2015. № 2. С. 21-28.

85. Досвід Фінляндії. У школах навчають виявляти дезінформацію. URL: https://www.radiosvoboda.org/a/shkola-uchni-dezinformatsiya/33251746.html (дата звернення: 26 травня 2024 р.).

86. Економічні інструменти протидії гібридній агресії. URL: https://niss.gov.ua/publikacii/analitichni-dopovidi/ekonomichni-instrumenti-protidii-gibridniy-agresii (дата звернення: 26 листопада 2023 р.).

87. Єгорова А. Медіаграмотність змалку для всіх. Як Фінляндії вдалося стати лідеркою з розвитку критичного мислення. URL: https://ms.detector.media/mediaosvita/post/26973/2021-03-31-mediagramotnist-zmalku-dlya-vsikh-yak-finlyandii-vdalosya-staty-liderkoyu-z-rozvytku-krytychnogo-myslennya/ (дата звернення: 26 травня 2024 р.).

88. Єнін М. Соціальні технології і ідеологічна складова розпалювання війни на Донбасі. *Великі війни, великі трансформації: історична соціологія 20-го століття, 1914-2014: Матеріали міжнародної наук.- практ. конф*. (м. Київ, 27-28 листопада 2014 р.) / Укладачі А. А. Мельниченко, П. В. Кутуєв, А. О. Мігалуш. К.: Політехніка, 2014. С. 177-178

89. Єнін М., Мельниченко А., Мельник Л. Гібридна війна як різновид соціально-політичних конфліктів: сутність, технології, домінуючі дискурси. *Актуальні проблеми філософії та соціології*. 2019. № 25. С. 104–115.

90. Єрема М. Боротьба з кіберзлочинністю в умовах дії воєнного стану: Закон 2149-IX. *Юрліга.* URL: https://jurliga.ligazakon.net/analitycs/210562_borotba-z-kberzlochinnstyu-v-umovakh-d-vonnogo-stanu-zakon-2149-ix (дата звернення: 26 липня 2024 р.).

91. Жарикова А. Кількість кібератак у 2023 році зросла на 16% - Держспецзв'язку. URL: https://epravda.com.ua/news/2024/01/31/709355/ (дата звернення: 21 січня 2025 р.).

92. Жарков Я. М., Бєсєдіна Л.М. Напрямки зовнішнього інформаційно-психологічного впливу на Україну. *Збірник наукових праць Військового інституту Київського національного університету ім. Т. Шевченка*. 2009. №19. URL: http//www.nbuv.gov.u/portal/natural/znpviknu/2009-19/vip19-21.pdf (дата звернення: 21 січня 2025 р.).

93. Завгородня Л., Бардадим О., Шапошник А. Роль медіаграмотності у сучасній освіті: перспективи та виклики. Вісник науки та освіти. 2024. №4 (22). URL: https://perspectives.pp.ua/index.php/vno/article/view/11202 (дата звернення: 26 листопада 2024 р.).

94. Зайко Л. Я. Мас-медіа як чинник формування суспільної свідомості. *Актуальні проблеми філософії та соціології*. 2016. Вип. 14. С. 36-39.

95. Закон України «Про інформацію». URL: https://zakon.rada.gov.ua/laws/show/2657-12#Text (дата звернення: 16 червня 2025 р.).

96. Закон України «Про медіа». URL: https://zakon.rada.gov.ua/laws/show/2849-20#Text (дата звернення: 16 червня 2025 р.).

97. Закон України «Про національну безпеку України». URL: https://zakon.rada.gov.ua/laws/show/2469-19#Text (дата звернення: 16 червня 2025 р.).

98. Закон України «Про основні засади забезпечення кібербезпеки України». URL: https://zakon.rada.gov.ua/laws/show/2163-19#Text (дата звернення: 16 червня 2025 р.).

99. Захаренко К. В. Інституційний вимір інформаційної безпеки України: трансформаційні виклики, глобальні контексти, стратегічні орієнтири: дис. … д-ра політ. наук: 23.00.02 «Політичні інститути та процеси». Київ; Львів: Національний педагогічний університет імені М. Драгоманова, Львівський національний університет імені Івана Франка, 2021. 423 с.

100. Захарченко Ю. Вілла Зеленського, продаж дітей і закупівля урану: які фейки РФ поширює про Україну. URL: https://fakty.com.ua/ua/svit/20240308-villa-zelenskogo-prodazh-ditej-i-zakupivlya-uranu-yaki-fejky-rf-poshyryuye-pro-ukrayinu/ (дата звернення: 26 листопада 2024 р.).

101. Заходи протидії гібридним (асиметричним) проявам у міждержавному протистоянні. URL: https://sidcon.com.ua/tpost/zmczd709p1-zahodi-protid-gbridnim-asimetrichnim-pro (дата звернення: 26 квітня 2025 р.).

102. Збрехали - російські пропагандисти вигадали збиття F-16 над Сумщиною. URL: https://armyinform.com.ua/2025/03/19/zbrehaly-rosijski-propagandysty-vygadaly-zbyttya-f-16-nad-sumshhynoyu/ (дата звернення: 26 квітня 2025 р.).

103. Зламана схема координації російських пропагандистів: завдання, оплата, звіти. *Інфонапалм.* 08 липня 2016. URL: https://informnapalm.org/ua/shema-koordynatsiyi-rosijskyh-propagandystiv/ (дата звернення: 26 листопада 2023 р.).

104. ЗСУ продає американську зброю мексиканським наркокартелям, а у Німеччині мало працевлаштованих українців, бо вони не хочуть працювати. Гвара медіа 24.02 – 02.03. URL: https://gwaramedia.com/zsu-prodaye-amerikansku-zbroyu-meksikanskim-narkokartelyam-a-u-nimechchini-malo-praczevlashtovanih-ukrayincziv-bo-voni-ne-hochut-praczyuvati-fejkotnya-17-02-02-03/ (дата звернення: 16 червня 2025 р.).

105. Іванчук Н. В. Концептуальні підходи до державного забезпечення інформаційної безпеки. *Інформаційна безпека суспільства в умовах дії правового режиму воєнного стану та повоєнний період : зб. матеріалів* (Київ, 29 трав. 2025 р.) / Редкол. : О. С. Тарасенко та ін. Київ : Нац. акад. внутр. справ, 2025. С.50-52.

106. Іноземні біолабораторії в Україні: чергові витки роспропаганди. URL: https://cpd.gov.ua/articles/inozemni-biolaboratoriyi-v-ukrayiniche/ (дата звернення: 18 квітня 2024 р.).

107. Інформаційна безпека держави. Конспект лекцій для здобувачів вищої освіти освітнього ступеню «бакалавр» спеціальності 262 «Правоохоронна діяльність» / Укл.: Ю.М.Ткач, С.М.Семендяй. Чернігів: НУ «Чернігівська політехніка», 2022. 133 с.

108. Інформаційна безпека держави: навч. посіб. для студ. спец. 6.170103 «Управління інформаційною безпекою», 125 «Кібербезпека» / В. І. Гур'єв, Д. Б. Мехед, Ю. М. Ткач, І. В. Фірсова. Ніжин: ФОП Лук'яненко В. В. ТПК«Орхідея», 2018. 166 с.

109. Інформаційні атаки в соціальних мережах: дослідження впливу російської дезінформації через рекламу в Facebook. *Центр стратегічних комунікацій та інформаційної безпеки.* URL: https://cedem.org.ua/wp-content/uploads/2024/05/informaczijni-ataky-v-soczialnyh-merezhah.-doslidzhennya-

vplyvu-rosijskoyi-dezinformacziyi-cherez-reklamu-v-facebook.pdf (дата звернення: 16.05.2025 р.)

110. Інформаційно-психологічна боротьба у воєнній сфері: монографія / Г.В. Пєвцов, А.М. Гордієнко, С.В. Залкін, С.О. Сідченко, А.О. Феклістов, К.І. Хударковський. Х.: Вид. Рожко С.Г., 2017. 276 с.

111. Ісмаїлзаде Л. Медіа, маніпуляція та інформаційна війна. *Науково-теоретичний альманах Грані*. 2023. №26 (5). С. 55-65.

112. Історія Державного центру кіберзахисту Держспецзв'язку. URL: https://scpc.gov.ua/uk/history (дата звернення: 26 листопада 2023 р.).

113. Кавуненко Т. Будь медіаграмотним: ресурси для фактчекінгу. URL: https://agentyzmin.org.ua/bud-mediagramotnym-resursy-dlya-faktchekingu/ (дата звернення: 16 листопада 2023 р.).

114. Калакура Я. Методологічні засади інформаційного менеджменту в умовах окупаційно-гібридної війни Росії проти України. *Український інформаційний простір.* 2021. № 1. С. 69-84.

115. Качинський А. Структурно-функціональна модель системи забезпечення інформаційної й інформаційно-психологічної безпеки. *Доповіді Національної академії наук України*. 2023. № 1. С. 16-23.

116. Киричок А. П. Роль інформаційно-психологічних операцій під час кризово-комунікаційного реагування. *Технологія і техніка друкарства*. 2022. №4. С. 121-129.

117. Кислий В.Д., Прокопенко Д.С. Інформаційно-психологічний вплив на військовослужбовців. *Інформаційна агресія Російської Федерації проти України*: Науковий семінар ХНУ ПС ім. І.Кожедуба, 21 жовтня 2020. URL: https://hups.mil.gov.ua/assets/doc/science/stud-conf/suchasna-vijna-gumanitarnij-aspekt-21-10-2020/8.pdf (дата звернення: 6 квітня 2024 р.).

118. Кібератака групи UAC-0010 (Armageddon) на державні організації України (CERT-UA#4434). URL: https://cert.gov.ua/article/39386 дата звернення: 16 квітня 2023 р.).

119. Кількість зареєстрованих кіберінцидентів зросла на 46%: звіт оперативного центру реагування на кіберінциденти ДЦКЗ. URL: https://ukurier.gov.ua/uk/news/kilkist-zareyestrovanih-kiberincidentiv-zrosla-na-/(дата звернення: 19 квітня 2025 р.).

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

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

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

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

124. 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.

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

126. Кобець Ю. В. «Гібридна війна» як загроза національній безпеці: Основні підходи та тлумачення. *Національна і регіональна безпека в умовах гібридної війни.* Збірник матеріалів міжрегіональної науково-практичної конференції (м.Івано-Франківськ, 30.11.2018 р. Івано-Франківськ, 2018. С.82-86.

127. Кобець Ю., Ставичний Р. Використання морально-етичного підходу в умовах розгортання інформаційної війни. *Національні інтереси України.* 2025. №5 (10). С. 1420-1429.

128. Козловський, С., Горун, С., Мамашвілі, Л. Підвищення економічної безпеки держави на основі інноваційних та цифрових трансформацій. Економіка та суспільство. 2024. № 59. URL: https://economyandsociety.in.ua/index.php/journal/article/view/3387 (дата звернення: 16 березня 2025 р.).

129. Коваленко Є. Д., Виганяйло С. Інформаційна безпека суспільства та держави. *Безпека у кіберсфері : зб. матеріалів Міжнар. наук.-практ. конф*. (м. Кам'янець-Подільський, 28 трав. 2025 р.) / МВС України, Харків. нац. ун-т внутр. справ, Нац. акад. прав. наук України, Орг. з безпеки та співробітництва в Європі. Кам'янець-Подільський: ХНУВС, 2025. С. 225-226.

130. Коваленко О. Фейки Кремля про Україну: в хід пішли «фейкові фактчекінги». URL: https://www.radiosvoboda.org/a/ukrayina-feyky-kremlya/32942386.html (дата звернення: 16 липня 2024 р.).

131. Кононенко В. П., Здоровко С. С., Корольова А. Є. Інформаційна безпека як стан. *Науковий вісник Ужгородського Національного Університету,* 2023. Серія Право. Випуск 76: частина 2. С. 244–250.

132. Конощук Я. Кабмін доручив підготувати пропозиції щодо посилення відповідальності за поширення недостовірної інформації, що створює позитивний образ РФ. URL: https://sud.ua/uk/news/publication/266504-kabmin-poruchil-podgotovit-predlozheniya-po-usileniyu-otvetstvennosti-za-rasprostranenie-nedostovernoy-informatsii-sozdayuschey-polozhitelnyy-obraz-rf (дата звернення: 8 березня 2025 р.).

133. Конрад А. Які фейки поширювала Росія про Україну впродовж війни? URL: https://svidomi.in.ua/page/yaki-feiky-poshyriuvala-rosiia-pro-ukrainu-vprodovzh-viiny (дата звернення: 16 квітня 2023 р.).

134. Конституція України. URL: https://zakon.rada.gov.ua/laws/show/254к/96-вр#Text (дата звернення: 16 квітня 2023 р.).

135. Копинець Ю. Інформаційна гігієна та гібридна безпека: як українці та діаспора в США можуть протидіяти дезінформації? URL: https://vilni-

media.com/2025/05/17/informatsijna-hihiiena-ta-hibrydna-bezpeka-iak-ukraintsi-ta-diaspora-v-ssha-mozhut-protydiiaty-dezinformatsii/ (дата звернення: 22 вересня 2025 р.).

136. Кормич Б.А. Інформаційна безпека: організаційно-правові основи [Текст] : навч. посібник для студ. вищих навч. закл. / Б.А. Кормич. К. : Кондор, 2004. 73-84 с

137. Корнієнко С. Путін веде в Україні гібридну війну – генерал Каппен. *Радіо Свобода*, 27.04.2014. URL: http://www.radiosvoboda.org/content/article/25363591.html (дата звернення: 16 грудня 2023 р.).

138. Корнієнко Т. Аналіз стану економічної безпеки України та пріоритети її зміцнення. *Економіка та суспільство.* 2022. №38. URL: https://economyandsociety.in.ua/index.php/journal/article/view/1314/126910 (дата звернення: 26 листопада 2023 р.).

139. Костюченко О.В. Інформаційна політика держави в умовах воєнного стану. *Національна безпека і оборона*. 2023. № 2(158). С. 18–24

140. Коткова В. LinkedIn: професійна мережа. URL: https://startup.co.ua/linkedin_profesiyna_merezha/ (дата звернення: 21 липня 2025 р.).

141. Кравець В.М. Інформаційна безпека в умовах глобалізації. *Інформаційна безпека суспільства в умовах дії правового режиму воєнного стану та повоєнний період : зб. матеріалів* (Київ, 29 трав. 2025 р.) / Редкол. : О. С. Тарасенко та ін. Київ : Нац. акад. внутр. справ, 2025. С.53-56.

142. Краудсорсинг – це що таке, визначення, суть та приклади. URL: https://karapuziki.com.ua/kraudsorsynh-tse-shcho-take-vyznachennia-sut-ta-pryklady/ (дата звернення: 21 липня 2025 р.).

143. “Кремлівська гідра”: 300 телеграм-каналів, які отруюють український інфопростір. URL: https://detector.media/monitorynh-internetu/article/205954/2022-12 14-kremlivska-gidra-300-telegrm-kanaliv-yaki-otruyuyut-ukrainskyy-infoprostir/ (дата звернення: 26 листопада 2023 р.).

144. Крижний А. Прем'єр спрогнозував час відновлення реєстрів Мін'юсту від кібератаки РФ. URL: https://web.archive.org/web/20241221120653/https://epravda.com.ua/oborona/massht abna-kiberatka-na-ukrajinu-shmigal-skazav-koli-zapracyuye-diya-801158/ (дата звернення: 26 січня 2025 р.).

145. Кримський референдум 2014, неконституційний Кримський референдум 16 березня 2014. Енциклопедія історії України: Додатковий том. Кн. 1: А–Я / Редкол.: В. А. Смолій (голова) та ін. НАН України. Інститут історії України. К.: В-во «Наукова думка», 2021. 773 с. URL: http://www.history.org.ua/?termin=krymskyj_referendum_2014_nekonstytutsijnyj_krymskyj_referendum_16_bereznja_2014 (дата звернення: 22 вересня 2023 р.).

146. Курбан О. В. Теорія інформаційної війни: базові основи, методологія та понятійний апарат. *ScienceRise.* 2015. № 11(1). С. 95-100.

147. Куркіна Д. Росіяни поширюють фейки про ЗСУ, які на ТОТ "скидають м’які заміновані іграшки", - ЦПД. URL: https://espreso.tv/viyna-z-rosiyeyu-rosiyani-poshiryuyut-feyki-pro-zsu-yaki-na-tot-skidayut-myaki-zaminovani-igrashki-tspd (дата звернення: 16 вересня 2025 р.).

148. Лавренюк А. У Франції прагнуть запобігти дезінформації напередодні загальноєвропейських виборів у 2019 році. *Укрінформ*. URL: https://www.ukrinform.ua/rubric-world/2585916-stop-fejk-pofrancuzki-parlament-uhvaliv-zorstkij-zakon.html (дата звернення: 26 листопада 2023 р.). .

149. Лапка О.Я., Назаренко О.А. Штучний інтелект як інструмент забезпечення інформаційної безпеки: сучасні виклики та перспективи. Інформаційна безпека суспільства в умовах дії правового режиму воєнного стану та повоєнний період : зб. матеріалів (Київ, 29 трав. 2025 р.) / Редкол. : О. С. Тарасенко та ін. Київ : Нац. акад. внутр. справ, 2025. С.67-69.

150. Лапка О.Я., Прилуцька К.В. Методи забезпечення інформаційної безпеки в умовах воєнного стану. Інформаційна безпека суспільства в умовах дії правового режиму воєнного стану та повоєнний період : зб. матеріалів (Київ, 29

трав. 2025 р.) / Редкол. : О. С. Тарасенко та ін. Київ : Нац. акад. внутр. справ, 2025. С.70-73.

151. Ларіончева, Н. Маніпуляція як ключовий інструмент інформаційної війни в епоху ЗМІ та соціальних мереж. *Науково-теоретичний альманах Грані*, 2025. № *28*(1), С.176-181.

152. Левченко О. В. Концептуальний підхід до комплексної оцінки стану інформаційної безпеки. *Наука і техніка Повітряних Сил Збройних Сил України.* 2015. № 3 (20). С. 47-50.

153. Лисецький Ю. М., Семенюк Ю. В. Гібридна війна. сутність, складові, модель. Держава і право. Частина 2: Політичні науки. 2024. Вип. 96. С.286-305.

154. Лисецький Ю. М., Семенюк Ю. В., Старовойтенко О. О. Гібридна війна як багатовимірне протистояння. *Вісник воєнної розвідки.* 2021. № 67. С. 7–10.

155. Литвиненко О. Інформація і безпека. *Нова політика*. 1998. № 1. С. 47-49.

156. Лікарчук Н., Лікарчук Д. Інформаційно-психологічні війни: міжнародно-політичний аналіз. *Міжнародні відносини: теоретико-практичні аспекти.* 2022. №9. С.157-171.

157. Ліпкан В.А. Інформаційна безпека України в умовах євроінтеграції / В.А. Ліпкан, Ю.Є. Максименко,В.М. Желіховський: [навч. посібник]. К.: КНТ, 2006. 280 с.

158. Ліпкан В.А., Харченко Л.С., Логінов О.В. Інформаційна безпека України : Глосарій. К. : Текст, 2004. 136 с.

159. Ломака І.І., Липчук О.І., Кобець Ю.В. Інформаційна безпека держави: теоретико-методологічні засади та особливості в умовах збройного конфлікту . Регіональні студії, 2022, №31. С. 113-117.

160. Лось Д. І. Інформаційна безпека суспільства в умовах дії правового режиму воєнного стану та повоєнний період. *Інформаційна безпека суспільства в умовах дії правового режиму воєнного стану та повоєнний період : зб.*

матеріалів (Київ, 29 трав. 2025 р.) / Редкол. : О. С. Тарасенко та ін. Київ : Нац. акад. внутр. справ, 2025. С 156-158.

161. Магда Є. Гібридна агресія Росії: уроки для Європи. Київ : КАЛАМАР, 2017. 268 с.

162. Магда Є. В., Водотика Т. С. Гібридна війна як явище. *Енциклопедія історії України*: Додатковий том. Кн. 1: А–Я / Редкол.: В. А. Смолій (голова) та ін. НАН України. Інститут історії України. К.: В-во «Наукова думка», 2021. 773 с.

163. Майсук Р.Р. Інформаційна безпека суспільства в умовах воєнного стану: правові виклики та правозастосування. *Інформаційна безпека суспільства в умовах дії правового режиму воєнного стану та повоєнний період : зб. матеріалів* (Київ, 29 трав. 2025 р.) / Редкол. : О. С. Тарасенко та ін. Київ : Нац. акад. внутр. справ, 2025. С.158-160.

164. Малинка В. Як Франція бореться з фейками: деталі ухвалених законів URL: https://detector.media/infospace/article/142843/2018-11-26-yak-frantsiya-boretsya-z-feykamy-detali-ukhvalenykh-zakoniv/ (дата звернення: 16 листопада 2023 р.).

165. Марчук В. В. До проблеми політичної консолідації і збереження національної ідентичності українського інформаційного простору. Аксіологічні аспекти трансформації сучасного українського суспільства. Івано-Франківськ, 2012. С.113-115.

166. Матвієнків С., Братах Л. Інформаційне поле сучасної України. Стан, перспективи розвитку та вплив на національну безпеку держави. *Національні інтереси України*. 2025. №5 (10). С.1430-1443.

167. Матвієнків С., Головчинський Н. Теоретико-методологічні засади дослідження поняття «війна». *Вісник Прикарпатського університету. Сер. Політологія.* Плай. Прикарпатський національний університет імені Василя Стефаника. Івано-Франківськ. 2020. Вип. 14. С. 103-113.

168. Матвієнків С. М. Державна інформаційна політика в контексті інтеграції України в Європейський Союз. *Вісник Прикарпатського*

університету. Політологія. Прикарпатський національний університет імені Василя Стефаника. Івано-Франківськ: ЛІК, Вип.12. 2018. С.227-234.

169. Матвієнків С. М. Інформаційна безпека як складова національної безпеки держави. *Національна безпека України: навчальний посібник* за заг.ред. В.В.Марчука. Львів-Торунь: Liha-Pres.2025.С.169-200.

170. 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.

171. 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.

172. Матвієнків С., Пучко Я. Російсько-українська війна в інформаційному просторі: виклики та їх подолання. *Вісник Прикарпатського університету. Серія: Політологія. 2025*. Випуск 20. С.225-233.

173. 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.

174. Машталір В.В., Гук О.М., Мурасов Р.К., Фараон С.І., Лоза В.В. Кіберборотьба в умовах збройного протистояння: аналіз, стратегії та виклики. *Сучасні інформаційні технології у сфері безпеки та оборони*. 2024. №1 Том 49. С. 93-104.

175. Методологія наукових досліджень в парадигмі синергетики: Монографія. За заг. ред. д-ра екон. наук Є.І. Ходаківського. Житомир: Житомирський державний технологічний університет, 2009. 340 с.

176. Миколаєнко І. Компаративістика як метод політології. *Методологія політичної науки: матеріали Всеукраїнської наукової конференції. Перші*

методологічні читання /Укл. Денисенко В.М., Угрин Л.Я. Львів: ЛНУ 2010. С.9-11.

177. Михайлов Д. За 2023 рік кіберполіція виявила понад 3600 кіберзлочинів. URL: https://suspilne.media/673484-za-2023-rik-kiberpolicia-viavila-ponad-3600-kiberzlociniv/ (дата звернення: 11 грудня 2024 р.). г

178. Мідттун Г. П. Битва умів. Гібридна війна – це вплив на людей, з метою підвести їх до свідомого чи несвідомого вибору, корисного для агресора. URL: https://texty.org.ua/articles/101043/bytva-umiv-gibrydna-vijna-ce-vplyv-na-lyudej-z-metoyu-pidvesty-yih-do-svidomoho-chy-nesvidomoho-vyboru-korysnoho-dlya-ahresora/ (дата звернення: 26 листопада 2023 р.).

179. Міноборони Данії спростувало російський фейк про загибель інструктора F-16 в Україні. URL: https://armyinform.com.ua/2025/01/20/minoborony-daniyi-sprostuvalo-rosijskyj-fejk-pro-zagybel-instruktora-f-16-v-ukrayini/ (дата звернення: 9 травня 2025 р.).

180. Младьонова А. Д. Інформаційна війна і політика безпеки: політико-правовий вимір. Кваліфікаційна наукова праця на правах рукопису. Дисертація на здобуття ступеня доктора філософії за спеціальністю 052 Політологія (галузь знань 05 Соціальні та поведінкові науки). Харківський національний університет імені В. Н. Каразіна Міністерства освіти і науки України, Харків, 2021. 200 с.

181. Можаровська А. Джек Дорсі: засновник Twitter, який перетворив дитячу мрію у мільярди. URL: https://24tv.ua/tech/dzhek_dorsi_biografiya_istoriya_uspihu_statok_zasnovnika_twitter_n1007200 (дата звернення: 11 січня 2024 р.).

182. Молоткіна Ю. Вербальне маніпулювання «фабрики тролів» у контексті антиукраїнської пропаганди кремля в англомовному дискурсі соціальних мереж TikTok та Twitter. Society. Document. Communication. 2022. Volume 7. № 4. С.155-181. URL: https://sdc-journal.com.ua/uk/journals/vipusk-17/verbalne-manipulyuvannya-fabriki-troliv-u-konteksti-antiukrayinskoyi-propagandi-kremlya-v-anglomovnomu-diskursi-sotsialnikh-merezh-tiktok-ta-twitter.

183. Морозова А. Фейки рф: як російська пропаганда налаштовує мешканців Сумщини проти ЄС? URL: https://kordon.media/fejky-rf-shho-rosijska-propaganda-vygaduye-pro-sumshhynu/ (дата звернення: 11 травня 2025 р.).

184. Музиченко О. Топ найбрехливіших фейків Кремля про Україну за останній час: як роспропаганда дурить світ. URL: https://tsn.ua/ato/top-naybrehlivishih-feykiv-kremlya-pro-ukrayinu-za-ostanniy-chas-yak-rospropaganda-durit-svit-2496712.html (дата звернення: 11 лютого 2024 р.).

185. Наймасштабніша в історії кібератака NotPetya була вчинена Росією проти України – США. URL: https://detector.media/infospace/article/134755/2018-02-16-naymasshtabnisha-v-istorii-kiberataka-notpetya-bula-vchynena-rosiieyu-proty-ukrainy-ssha/(дата звернення: 26 листопада 2023 р.).

186. Наместнік В. Соціальні мережі як середовище проведення інформаційно-психологічних операцій противника. *Стратегічні комунікації у сфері забезпечення національної безпеки та оборони: проблеми, досвід, перспективи:* зб. тез доп. IV міжнар. наук.-практ. конф. Національного університету оборони України. м. Київ, 27 верес. 2023 р. Київ: НУОУ, 2023. С. 105–107.

187. НАТО і представники України вивчали протидію гібридним атакам на тлі агресії РФ URL: https://www.rbc.ua/rus/news/nato-razom-ukrayintsyami-vivchalo-protidiyu-1700764615.html (дата звернення: 11 січня 2024 р.).

188. Національна рада з питань телебачення і радіомовлення України. URL: https://www.nrada.gov.ua (дата звернення: 11 січня 2024 р.).

189. Нашинець-Наумова А. Ю. Інформаційна безпека: питання правового регулювання: монографія. Київ: Видавничий дім «Гельветика», 2017. 168 с.

190. На Курщині знищена перша група українських контрактників віком 18-24 роки, а Порошенко заперечив удари Росії по лікарнях та критичній інфраструктурі України. Гвара медіа. URL: https://gwaramedia.com/na-kurshhini-znishhena-persha-grupa-ukrayinskih-kontraktnikiv-vikom-18-24-roki-a-poroshenko-

zaperechiv-udari-rosiyi-po-likarnyah-ta-kritichnij-infrastrukturi-ukrayini-fejkotnya-17-03-30-03/ (дата звернення: 11 травня 2025 р.).

191. На Миколаївщині місцева жителька виправдовувала збройну агресію РФ – прокуратура. URL: https://imi.org.ua/news/na-mykolayivshhyni-mistseva-zhytelka-vypravdovuvala-zbrojnu-agresiyu-rf-prokuratura-i52380 (дата звернення: 26 листопада 2023 р.).

192. На Прикарпатті СБУ затримала адміністратора прокремлівської групи. URL: https://imi.org.ua/news/na-prykarpatti-sbu-zatrymala-administratora-prokremlivskoyi-grupy-i54068 (дата звернення: 26 листопада 2023 р.).

193. На Хмельниччині викрили інтернет-агітаторку, яка поширювала кремлівські наративи. URL: https://imi.org.ua/news/na-hmelnychchyni-vykryly-internet-agitatorku-yaka-poshyryuvala-kremlivski-naratyvy-i56951 (дата звернення: 26 листопада 2023 р.).

194. Некрасов В. Україна програє кібервійну. Хакери атакують державні фінанси. URL: https://epravda.com.ua/publications/2016/12/9/613957/ (дата звернення: 21 січня 2023 р.).

195. Не ведіться на емоційний контент. Як розрізнити російські фейки. URL: https://ukr.radio/news.html?newsID=105429 (дата звернення: 16 липня 2025 р.).

196. Недохлєбов І.І. Інформаційна безпека України в умовах сучасних загроз: організаційно-правові аспекти. – Кваліфікаційна наукова праця на правах рукопису. Дисертація на здобуття наукового ступеня кандидата юридичних наук за спеціальністю 12.00.07 – адміністративне право і процес; фінансове право; інформаційне право. Запорізький національний університет, Запоріжжя, 2024. 240 с.

197. Нова хакерська атака на Україну: постраждали органи юстиції та нотаріусів URL: https://ua.news/ua/technologies/novaya-hakerskaya-ataka-na-ukrainu-postradali-organy-yustitsii-i-notariusov#google_vignette (дата звернення: 26 листопада 2023 р.).

198. . Новицький В.А. Генеза поняття «інформаційна безпека»: походження та становлення. *Вчені записки ТНУ імені В.І. Вернадського. Серія: Публічне управління та адміністрування*. 2024. Том 35 (74). С.38-44.

199. Носов В. Системний підхід у забезпеченні інформаційної безпеки. *Правове, нормативне та метрологічне забезпечення системи захисту інформації в Україні : науково-технічний збірник*. 2010. Вип. 1(20). С. 92-97.

200. Обмін полоненими і репатріація загиблих: маніпуляції Кремля. URL: https://spravdi.gov.ua/obmin-polonenymy-i-repatriacziya-zagyblyh-manipulyacziyi-kremlya/ (дата звернення: 26 вересня 2025р.).

201. Огнева М. Ми всі із цим стикалися. Що таке “астротурфінг” URL: https://bahmut.in.ua/my-vsi-iz-czym-stykalysya-shho-take-astroturfing/ (дата звернення: 16 липня 2025 р.).

202. Окупанти тримають у полоні адмінів двох українських тг-каналів і звинувачують у тероризмі. URL: https://imi.org.ua/news/okupanty-trymayut-u-poloni-adminiv-dvoh-ukrayinskyh-tg-kanaliv-i-zvynuvachuyut-u-teroryzmi-i56530 (дата звернення: 22 липня 202 4р.).

203. Окупаційний суд Криму оштрафував користувачку соцмереж за “дискредитацію російської армії”. URL: https://imi.org.ua/news/okupatsijnyj-sud-krymu-oshtrafuvav-koyrstuvachku-sotsmerezh-za-dyskredytatsiyu-rosijskoyi-armiyi-i52808 (дата звернення: 12 липня 2023р.).

204. Окупанти поширюють фейки про те, що ЗСУ здійснюватимуть хімічні атаки. URL: https://armyinform.com.ua/2024/07/17/okupanty-poshyryuyut-fejky-pro-pidgotovku-zsu-himichnyh-atak/ (дата звернення: 10 липня 2025 р.).

205. Омельченко А. В. Організаційно-правові засади забезпечення кібербезпеки України. *Київський часопис права*. 2022. №3. С.140-145.

206. Оприлюднено звіт про кіберінциденти та кібератаки протягом 2022 року. URL: https://cybersec.net.ua/novyny/506-opryliudneno-zvit-pro-kiberintsydenty-ta-kiberataky-protiahom-2022-roku.html дата звернення: 26 листопада 2023 р.).

207. Осьодло В., Савінцев В. Тенденції розвитку та завдання інформаційно-пропагандистського забезпечення в сучасних умовах. *Воєнна історія*. 2006. № 4-6. С. 110-118.

208. Панченко В. М. Зарубіжний досвід формування систем захисту критичної інфраструктури від кіберзагроз. *Інформаційна безпека людини, суспільства, держави: наук.-практ. журн.* К. 2012. №3 (10). С. 100-109.

209. Панченко О. Інформаційна складова національної безпеки. *Вісник Національної академії Державної прикордонної служби України.* Серія : Державне управління. 2019. Вип. 3. URL: http://nbuv.gov.ua/UJRN/Vnadpsdu_2019_3_11 (дата звернення: 11 січня 2024 р.).

210. Патока М. Російська пропаганда розповсюджує фейки про нібито "звірства ЗСУ" в Курській області - Центр протидії дезінформації. URL: https://suspilne.media/938099-rosijska-propaganda-rozpovsudzue-fejki-pro-nibito-zvirstva-zsu-v-kurskij-oblasti-centr-protidii-dezinformacii/ (дата звернення: 2 липня 2025 р.).

211. . Пендюра М.М. Інформаційна безпека суспільства в умовах правового режиму воєнного стану та післявоєнний період. *Інформаційна безпека суспільства в умовах дії правового режиму воєнного стану та повоєнний період : зб. матеріалів* (Київ, 29 трав. 2025 р.) / Редкол. : О. С. Тарасенко та ін. Київ : Нац. акад. внутр. справ, 2025. С.94-98.

212. Перелік кібератак. *Вікіпедія*. URL: https://surl.li/aqbqcn (дата звернення: 16 липня 2025 р.).

213. Петрик В. Сутність і особливості проведення спеціальних інформаційних операцій та акцій інформаційного впливу. *Сучасні інформаційні технології у сфері безпеки та оборони*. 2009. №3(6). С. 71-75.

214. Пєвцов Г.В., Залкін С.В., Сідченко С.О., Хударковський К.І. Методичний підхід до формування сценарію проведення інформаційно-психологічного впливу на осіб, що приймають рішення. *Наука і техніка Повітряних Сил Збройних Сил України*. 2021. № 3. С. 35-40.

215. Пивовар В., Драчук С. Філософські проблеми безпеки як методологічна основа забезпечення безпеки фондового ринку. *Правова інформатика*. 2007. № 2 (4). С. 77–82.

216. Пігуль Н. Г., Пігуль Є. І. Економічна безпека держави: сутність та актуальні загрози. *Бізнес Інформ*. 2024. №7. С. 6-13.

217. Під час ракетного удару РФ по Хмельниччині загинув пілот ВПС США, а український художник у Польщі ампутував здорову ногу на знак солідарності із ЗСУ. *Гвара медіа.* 13 жовтня 2024. URL: https://gwaramedia.com/pid-chas-raketnoho-udaru-rf-po-khmelnychchyni-zahynuv-pilot-vps-ssha-a-ukrainskyy-khudozhnyk-u-polshchi-amputuvav-zdorovu-nohu-na-znak-solidarnosti-iz-zsu-feykotnia-07-10-13-10/ (дата звернення: 2 травня 2025 р.).

218. Повідомлено підозру тіктокеру з Києва, який поширював наративи Кремля та влаштовував провокації в Лаврі. URL: https://imi.org.ua/news/povidomleno-pidozru-tiktokeru-z-kyyeva-yakyj-poshyryuvav-naratyvy-kremlya-ta-vlashtovuvav-i52994 (дата звернення: 9 травня 2023 р.).

219. Порошенко ввів санкції проти соцмереж Вконтакте, Одноклассники, поштового сервісу Mail.ru. URL: https://gv.kr.court.gov.ua/sud1103/pres-centr/news/351027/ (дата звернення: 28 травня 2023 р.).

220. Порошенко підписав наказ про заборону "Яндекс", "Вконтакте" й "Одноклассники". URL: https://day.kyiv.ua/news/271221-poroshenko-pidpysav-nakaz-pro-zaboronu-yandeks-vkontakte-y-odnoklassnyky (дата звернення: 9 травня 2023 р.).

221. . Порощук Н. РФ поширює фейковий «лист Шмигаля» про евакуацію держустанов: названо мету. URL: https://glavcom.ua/country/society/rf-poshirjuje-fejkovij-list-shmihalja-pro-evakuatsiju-derzhustanov-nazvano-metu-1066532.html (дата звернення: 15 вересня 2025 р.).

222. Постанова Кабінету Міністрів України від 23.12.2020 №1295 «Деякі питання забезпечення функціонування системи виявлення вразливостей і реагування на кіберінциденти та кібератаки». URL:

https://zakon.rada.gov.ua/laws/show/1295-2020-п#Text (дата звернення: 2 вересня 2023 р.).

223. Пролорензо А. Савлюк М. Кіберзахист як складник інформаційної безпеки держави в умовах гібридної війни. *Національні інтереси України*. 2025. №6 (11). С.198-213

224. Пропаганда рф готує фейки про Україну перед зустріччю Трампа і путіна – ЦПД. URL: https://ipress.ua/news/propaganda_rf_gotuie_feyky_pro_ukrainu_pered_zustrichchyu_trampa_i_putina__tspd_375049.htm (дата звернення: 12 вересня 2025 р.).

225. Про LinkedIn. URL: https://about.linkedin.com/uk-ua.

226. Про основні засади забезпечення кібербезпеки України: Закон України від 04. 04. 2024 № 2163-VIII. URL: https://zakon.rada.gov.ua/laws/show/2163-19#Text дата звернення: 9 травня 2025 р.).

227. Протидія гібридним загрозам в Україні. URL: https://www.irf.ua/protidiya_gibridnim_zagrozam_v_ukraini/ (дата звернення: 9 липня 2023 р.).

228. Проць А. Алгоритми соцмереж та інформаційні бульбашки: виклики для журналістики. *Медіакритика*. 11 лютого 2025. URL: http://mediakrytyka.lnu.edu.ua/ohlyady-analityka/alhorytmy-sotsmerezh-ta-informatsiyni-bulbashky-vyklyky-dlya-zhurnalistyky.html (дата звернення: 9 липня 2025 р.).

229. «путінські спецслужби добре вміють влаштовувати провокації»: ГУР про фейк рф щодо «терактів України проти дипломатів ЄС». URL: https://armyinform.com.ua/2025/02/20/putinski-speczsluzhby-dobre-vmiyut-vlashtovuvaty-provokacziyi-gur-pro-fejk-rf-shhodo-teraktiv-ukrayiny-proty-dyplomativ-yes/ (дата звернення: 19 липня 2024 р.).

230. Пфо О. М. Основні поняття і класифікація кіберзлочинності. *Актуальні задачі та досягнення у галузі кібербезпеки* : матеріали Всеукр. наук.-

практ. конф. (м. Кропивницький, 23-25 лист. 2016 р.). Кропивницький, 2016. С. 33-34.

231. Рада національної безпеки і оборони України. URL: https://www.rnbo.gov.ua (дата звернення: 19 липня 2024 р.). .

232. Радченко О., Чмир, Я. Гібридна війна як ключова загроза національному суверенітету України. *Таврійський науковий вісник. Серія: Публічне управління та адміністрування*. 2022. №3. С. 100-108.

233. Реформа системи цивільної готовності Швеції. URL: https://niss.gov.ua/doslidzhennya/natsionalna-bezpeka/reforma-systemy-tsyvilnoyi-hotovnosti-shvetsiyi (дата звернення: 9 травня 2025 р.).

234. Рижук О. Аналіз концепцій визначення «інформаційної безпеки» в умовах глобалізації. *Освіта регіону*. 2016. №4. URL: https://social-science.uu.edu.ua/article/1400 (дата звернення: 26 листопада 2023 р.).

235. Рік свободи слова в блогосфері: пропагандисти, публікація роботи ППО, цензура платформ. URL: https://imi.org.ua/monitorings/rik-svobody-slova-v-blogosferi-propagandysty-publikatsiya-roboty-ppo-tsenzura-platform-i58448/ (дата звернення: 9 травня 2024 р.).

236. Робота медіа не повинна бути секретом або Як навчають медіаграмотності у Фінляндії. URL: https://airpu.org/news/robota-media-ne-povinna-buti-sekretom-abo-yak-navchayut-mediagramotnosti-u-finlyandiyi/ .(дата звернення: 16 липня 2025 р.).

237. . Рожок-Капранова І. Фейки й лякалки росії про обмеження прав в Україні. URL: https://nakypilo.ua/rozbory/feiky-y-liakalky-rosii-pro-obmezhennia-prav-v-ukraini/ (дата звернення: 9 січня 2025 р.).

238. Романюк О. "Путін - демократ" та "третій майдан" у Києві: що Росія вигадує про Україну та як поширює брехню. URL: https://tsn.ua/exclusive/putin-demokrat-ta-tretiy-maydan-u-kiyevi-scho-rosiya-vigaduye-pro-ukrayinu-ta-yak-poshiryuye-brehnyu-2561551.html (дата звернення: 9 липня 2024 р.).

239. Російська пропаганда поширює фейки щодо планів України підірвати окуповану ЗАЕС. URL: https://www.ukrinform.ua/rubric-

factcheck/3853306-rospropaganda-posirue-fejki-pro-nibito-plani-ukraini-pidirvati-zaes.html (дата звернення: 9 травня 2024 р.).

240. Російські пропагандисти поширили фейк про загибель нібито мобілізованого до ЗСУ підлітка. URL: https://zmina.info/news/rosijski-propagandysty-poshyryly-fejk-pro-zagybel-nibyto-mobilizovanogo-do-zsu-pidlitka/.

241. Російські спецслужби розпочали ІПСО із залученням родин українських військовополонених – ЦПД. URL: https://www.ukrinform.ua/rubric-ato/4011214-rosijski-specsluzbi-rozpocali-ipso-iz-zalucennam-rodin-ukrainskih-vijskovopolonenih-cpd.html (дата звернення: 19 серпня 2024 р.).

242. Російські хакери зламали державні реєстри України. Що відомо. URL: https://web.archive.org/web/20241220165826/https://www.bbc.com/ukrainian/articles/c7ve1298ndgo.amp (дата звернення: 9 січня 2025 р.).

243. Росія поширює в Ізраїлі фейки про Україну на «популярних сайтах» – ЗМІ. URL: https://www.ukrinform.ua/rubric-world/3738744-rosia-posirue-v-izraili-fejki-pro-ukrainu-na-popularnih-sajtah-zmi.html (дата звернення: 9 січня 2025 р.).

244. Росія поширює фейки про Україну в Сирії на тлі успіхів повстанців. URL: https://unn.ua/news/rosiia-poshyriuie-feiky-pro-ukrainu-v-syrii-na-tli-uspikhiv-povstantsiv (дата звернення: 22 січня 2025 р.).

245. Росіяни активно створюють фейкові телеграм-канали українських бригад і батальйонів – ЦПД. URL: https://zmina.info/news/rosiyany-aktyvno-stvoryuyut-fejkovi-telegram-kanaly-ukrayinskyh-brygad-i-bataljoniv-spravdi/ (дата звернення: 13 січня 2024 р.).

246. Росіяни видають наслідки власних обстрілів Харківщини за “розстріл цивільних” українськими бійцями. URL: https://zmina.info/news/rosiyany-vydayut-naslidky-vlasnyh-obstriliv-harkivshhyny-za-rozstril-czyvilnyh-ukrayinskymy-bijczyamy/ (дата звернення: 2 листопада 2024 р.).

247. Росіяни використовують штучний інтелект для створення фейкових сюжетів нібито від українських телеканалів. URL: https://www.ukrinform.ua/rubric-ato/4016118-rosiani-vikoristali-stucnij-intelekt-dla-

stvorenna-fejku-pro-otocenna-zsu-na-kupanskomu-napramku-cpd.html (дата звернення: 2 листопада 2024 р.).

248. Росіяни розсилають фейкові листи до українських держструктур про підготовку евакуації міністерств з Києва. URL: https://www.ukrinform.ua/rubric-society/4011517-rosiani-rozsilaut-fejkovi-listi-do-ukrainskih-derzstruktur-pro-pidgotovku-evakuacii-ministerstv-z-kieva.html (дата звернення: 16 вересня 2025 р.).

249. Росіяни шантажем змушують українців на ТОТ дивитися пропагандистські канали Кремля – ЦНС. URL: https://kyiv24.news/news/rosiyany-shantazhem-zmushuyut-ukrayincziv-na-tot-dyvytysya-propagandystski-kanaly-kremlya-czns (дата звернення: 9 вересня 2025 р.).

250. Рюле М., Робертс К. Розширення інструментарію НАТО з протидії гібридним загрозам. URL: https://www.nato.int/docu/review/uk/articles/2021/03/19/rozshirennya-nstrumentaryu-nato-z-protid-gbridnim-zagrozam/index.html (дата звернення: 26 листопада 2023 р.).

251. Рудник Л. Соціальні мережі як засіб здійснення терористичних актів. Глобальна організація союзницького лідерства. 2016. URL: https://goal-int.org/socialni-merezhi-yak-zasib-zdijsnennya-teroristichnix-aktiv/ (дата звернення:7 листопада 2023 р.).

252. Савлюк М. Теоретико-методологічні засади дослідження інформаційної безпеки. *Вісник Прикарпатського університету. Серія: Політологія. 2023.* Випуск 15. 2023. С.60-68

253. Савлюк М. Гібридна війна в Україні: сучасні підходи. *Вісник Прикарпатського університету. Серія: Політологія*. 2024. Випуск 17. С.187-197.

254. Савлюк М. Важливість інформаційної безпеки в соціальних мережах для загальнонаціональної безпеки: безпековий вимір України. *Вісник*

Прикарпатського університету. Серія: Політологія. 2024. Випуск 18. С.300-309.

255. Савченко С. В. Гібридна війна: сутність поняття та основні сучасні прояви. *Вісник Луганського національного університету імені Тараса Шевченка. Педагогічні науки*. 2017. № 7(1). С. 103-112.

256. Савчук С. О. Державна політика протидії кіберзлочинності. – Кваліфікаційна наукова праця на правах рукопису. Дисертація на здобуття наукового ступеня кандидата наук з державного управління за спеціальністю 25.00.05 – державне управління у сфері державної безпеки та охорони громадського порядку. Державний університет «Житомирська політехніка». Житомир, 2024. 184 с.

257. Саєнко О. Г. Механізм інформаційно-психологічного впливу в умовах гібридної війни. *Вісник Національної академії Державної прикордонної служби України. Серія : Психологія*. 2015. Вип. 1. URL: https://nadpsu.edu.ua/wp-content/uploads/2021/09/visnik_1_2015_psh.pdf (дата звернення: 26 листопада 2023 р.).

258. Самохвалова Л. Московський слід колорадського Жука, або Хто і як готує «Майдан-3». URL: https://www.ukrinform.ua/rubric-polytics/1948496-moskovskij-slid-koloradskogo-zuka-abo-hto-i-ak-gotue-majdan3.html (дата звернення: 9 травня 2025 р.).

259. Сащук Г. Інформаційна безпека в системі забезпечення національної безпеки. *Бізнес і безпека*. 2014. №1. С.46-50.

260. СБУ викрила міжрегіональну мережу проросійських інтернет-агітаторів. URL: https://imi.org.ua/news/sbu-vykryla-mizhregionalnu-merezhu-prorosijskyh-internet-agitatoriv-i52184 (дата звернення: 26 листопада 2023 р.).

261. СБУ викрила 11 проросійських інтернет-агітаторів. URL: https://imi.org.ua/news/sbu-vykryla-11-prorosijskyh-internet-agitatoriv-i53650 (дата звернення: 26 листопада 2023 р.).

262. СБУ заблокувала мережу інтернет-агітаторів, що поширювали кремлівські фейки. URL: https://imi.org.ua/news/sbu-zablokuvala-merezhu-

internet-agitatoriv-shho-poshyryuvaly-kremlivski-fejky-i52563 дата звернення: 26 листопада 2023 р.).

263. СБУ затримала блогера, який виправдовував збройну агресію РФ та цькував військових. URL: https://imi.org.ua/news/sbu-zatrymala-blogera-yakyj-vypravdovuvav-zbrojnu-agresiyu-rf-ta-tskuvav-vijskovyh-i54261 (дата звернення: 26 листопада 2023 р.).

264. СБУ ліквідувала ботоферму в Кропивницькому. URL: https://imi.org.ua/news/sbu-likviduvala-botofermu-v-kropyvnytskomu-i52000 (дата звернення: 26 листопада 2023 р.).

265. СБУ повідомила про підозру блогеру-священнику, який закликав російських військових убивати українців. URL: https://imi.org.ua/news/sbu-povidomyla-pro-pidozru-rosijskomu-blogeru-svyashhennyku-rpts-yakyj-zaklykav-ubyvaty-ukrayintsiv-i52007 (дата звернення: 26 листопада 2023 р.).

266. СБУ повідомила про підозру в держзраді та пропаганді прокремлівському блогеру Юрію Подоляці. URL: https://imi.org.ua/news/sbu-povidomyla-pro-pidozru-u-derzhzradi-ta-propagandi-prokremlivskomu-blogeru-yuriyu-podolyatsi-i51911 (дата звернення: 26 листопада 2023 р.).

267. СБУ радить українцям видаляти аккаунти з російських соцмереж. *Еспресо.* 24 липня 2014. URL: https://espreso.tv/news/2014/07/28/sbu_radyt_ukrayincyam_vydalyaty_akkaunty_z_rosiyskykh_socmerezh (дата звернення: 16 липня 2023 р.).

268. Світлична В.Ю. Інформаційна безпека: сутність та порядок реалізації. *Young Scientist.* 2014. №11 (14). С.97-100.

269. Світова гібридна війна: український фронт : монографія / за заг. ред. В. П. Горбуліна. Київ : НІСД, 2017. 496 с.

270. Священник ПЦУ в Чернівцях відмовився відспівувати загиблих військових ЗСУ, бо вони були хрещені УПЦ МП, а у Полтаві загинули військові інструктори зі Швеції. *Гвара медіа.* URL: https://gwaramedia.com/sviashchennyk-ptsu-v-chernivtsiakh-vidmovyvsia-vidspivuvaty-zahyblykh-viyskovykh-zsu-bo-vony-buly-khreshcheni-upts-mp-a-u-

poltavi-zahynuly-viyskovi-instruktory-zi-shvetsii-feykotnia-16-09-22-09/ (дата звернення: 22 жовтня 2024 р.).

271. Северина С. В. Інформаційна безпека та методи захисту інформації. *Вісник Запорізького національного університету. Економічні науки.* 2016. № 1. С. 155-161.

272. Селецький О. В., Костюченко Н. Д. Поняття та зміст інформаційної безпеки як складової національної безпеки. *Науковий вісник Сіверщини. Серія: Право.* 2025. №2 (25). С. 98-106.

273. Сенюк О. П., Лапка О. Я. Роль цифрових технологій у забезпеченні інформаційної безпеки в умовах воєнного стану. *Інформаційна безпека суспільства в умовах дії правового режиму воєнного стану та повоєнний період : зб. матеріалів* (Київ, 29 трав. 2025 р.) / Редкол. : О. С. Тарасенко та ін. Київ : Нац. акад. внутр. справ, 2025. С.167-169.

274. Серед дезінформаційних тем, які росіяни розповсюджували в березні, з'явилися п'ять нових - Платформа прав людини. URL: https://zmina.info/news/sered-dezinformatsiynykh-tem-yaki-rosiyany-rozpovsyudzhuvaly-v-berezni-z″yavylysya-p″yat′-novykh-platforma-prav-lyudyny/ (дата звернення: 28 травня 2023 р.).

275. Ситник О. Гібридний характер російсько-української війни 2014–2017 років та пошук ефективних засобів протидії. *Центр ім.Д.Донцова.* 28 квітня 2017 р. URL: http://dontsov-nic.com.ua/hibrydnyj-harakter-rosijsko-ukrajinskoji-vijny-2014-2017-rokiv-ta-poshuk-efektyvnyh-zasobiv-protydiji/ (дата звернення: 18 травня 2025 р.).

276. Сінгапур представив законопроект проти фейків, який дозволить владі прибирати матеріали. URL: https://ms.detector.media/media-i-vlada/post/22700/2019-04-03-singapur-predstavyv-zakonoproekt-proty-feykiv-yakyy-dozvolyt-vladi-prybyraty-materialy/ (дата звернення: 22 травня 2024 р.).

277. Сінгапур ухвалив закон про іноземне втручання, що дозволяє владі блокувати вміст інтернету. URL: https://yur-gazeta.com/golovna/singapur-uhvaliv-

zakon-pro-inozemne-vtruchannya-shcho-dozvolyae-vladi-blokuvati-vmist-internetu.html (дата звернення: 22 травня 2024 р.).

278. SKYPE припиняє роботу з травня 2025 року: користувачів переводять на MICROSOFT TEAMS. URL: https://dp.tram.news/ukr/news/techno/a1255653-skype-pripinjaje-robotu-z-travnja-2025-roku-koristuvachiv-perevodjat-na-microsoft-teams.html (дата звернення: 2 серпня 2025 р.).

279. Снайдер Т. Росія потрапила у свою пастку. Як одна брехня призвела до великої війни. URL: https://nv.ua/ukr/opinion/navishcho-rosiya-pochala-viynu-snayder-pro-brehnyu-pro-rozp-yatogo-hlopchika-novini-ukrajini-50233793.html (дата звернення: 5 травня 2024 р.).

280. Собенко Н. На Заході думають, як відповісти на диверсії РФ в Європі – FT. URL: https://suspilne.media/760851-na-zahodi-dumaut-ak-vidpovisti-na-diversii-rf-v-evropi-ft/ (дата звернення: 9 травня 2025 р.).

281. Соколов О. Економічна безпека України в умовах воєнного стану. *Науковий вісник Ужгородського Національного Університету. Серія Право*. 2024. Випуск 86: частина 1. URL: https://visnyk-juris-uzhnu.com/wp-content/uploads/2025/01/43.pdf (дата звернення: 2 серпня 2025 р.).

282. Сологуб С. І.. Соціальні мережі в науковій роботі: Навчальний посібник. К. ІПДО. 2023. 89 с.

283. Соціальні мережі: поняття, історія виникнення. URL: htttps://zounb.zp.ua/resourse/zaporizkyy-kray/zaporizhzhya-bibliotechne/fahova-osvita/socialni-merezhi-piv.

284. Соціальні мережі під час війни: український досвід модерації контенту. URL: https://www.ukrinform.ua/rubric-presshall/3815532-socialni-merezi-pid-cas-vijni-ukrainskij-dosvid-moderacii-kontentu.html (дата звернення: 26 вересня 2025 р.).

285. Соціальні мережі під час війни: як мають змінитися платформи і самі користувачі - Центр демократії та верховенства права. URL:

https://cedem.org.ua/news/sotsialni-merezhi-pid-chas-viyny/ (дата звернення: 24 вересня 2025 р.).

286. Соціальні мережі як рушій громадської підтримки під час війни: аналіз впливу. *Благодійний фонд ТВІЙ КРОК*. 23 листопада 2024. URL: https://tviykrok.com.ua/info/articles/socialni-merezhi-yak-rushij-gromadskoyi-pidtrimki-pid-chas-vijni-analiz-vplivu/ (дата звернення: 24 грудня 2024 р.).

287. Стало відомо, чому Янукович передумав підписувати Угоду про асоціацію. URL: https://tsn.ua/politika/stalo-vidomo-chomu-yanukovich-peredumav-pidpisuvati-ugodu-pro-asociaciyu-393729.html дата звернення: 7 грудня 2023 р.).

288. Статистичний звіт за результатами роботи Системи виявлення вразливостей і реагування на кіберінциденти та кібератаки в 2023 році. URL: https://scpc.gov.ua/uk/articles/334 (дата звернення: 2 жовтня 2024 р.).

289. Стратегічний оборонний бюлетень України: Указ Президента України №473/2021 від 20 серпня 2021 р. URL: https://www.president. gov.ua/documents/4732021-40121 (дата звернення: 26 листопада 2023 р.).

290. Стратегічні комунікації для безпекових і державних інституцій : практичний посібник / [Л. Компанцева, О. Заруба, С. Череватий, О. Акульшин; за заг. ред. О. Давліканової, Л. Компанцевої]. Київ: ТОВ «ВІСТКА», 2022. 278 с.

291. Стратегічні комунікації : [словник] / Т. В. Попова, В. А. Ліпкан ; за заг. ред. доктора юридичних наук В. А. Ліпкана. К. : ФОП Ліпкан О.С., 2016. 416 с.

292. Стратегія кібербезпеки України: затверджена Указом Президента України від 26 серпня 2021 року № 447/2021. URL: https://zakon.rada.gov.ua/laws/show/447/2021#n12 (дата звернення: 26 листопада 2023 р.).

293. Стратегія національної безпеки України: Указ Президента України від 14 вересня 2020 року № 392/2020. Офіційний сайт представництва Президента України. URL: https://www. president.gov.ua/documents/3922020-35037 (дата звернення: 26 листопада 2023 р.).

294. Сугестивні технології маніпулятивного впливу: навч. посіб. / [В. М. Петрик, М. М. Присяжнюк, Л. Ф. Компанцева, Є. Д. Скулиш, О. Д. Бойко, В. В. Остроухов]; за заг. ред. Є. Д. Скулиша. 2-ге вид. Київ: ЗАТ «ВІПОЛ», 2011. 48 с.

295. США також звинуватили у вірусі NotPetya Росію. URL: https://www.bbc.com/ukrainian/news-43082212 (дата звернення: 9 травня 2025 р.).

296. Тарасова Д. Росія поширює фейк про нібито підготовку Україною "провокацій" з небезпечними речовинами у Донецькій області, - ЦПД. URL: https://espreso.tv/viyna-z-rosiyeyu-rosiya-poshiryue-feyk-pro-nibito-pidgotovku-ukrainoyu-provokatsiy-z-nebezpechnimi-rechovinami-u-donetskiy-oblasti-tspd (дата звернення: 19 вересня 2025 р.).

297. Тарасюк А. В. Теоретико-правові основи забезпечення кібербезпеки України. Кваліфікаційна наукова праця на правах рукопису. Дисертація на здобуття наукового ступеня доктора юридичних наук за спеціальністю 12.00.07 – адміністративне право і процес; фінансове право; інформаційне право (081 – Право). Державна наукова установа «Інститут інформації, безпеки і права Національної академії правових наук України». Київ, 2021. 461 с.

298. Тимчук С. Цікаве про Україну: якими соцмережами переважно користуються українці. URL: https://gk-press.if.ua/tsikave-pro-ukrayinu-yakymy-sotsmerezhamy-perevazhno-korystuyutsya-ukrayintsi/ (дата звернення: 16 липня 2025 р.).

299. Тихомиров О. О. Сучасне розуміння інформаційної безпеки: виміри та рівні забезпечення. *Інформаційна безпека суспільства в умовах дії правового режиму воєнного стану та повоєнний період : зб. матеріалів* (Київ, 29 трав. 2025 р.) / Редкол. : О. С. Тарасенко та ін. Київ : Нац. акад. внутр. справ, 2025. С.26-29.

300. Тлумачний словник української мови. URL: http://www.inmo.org.ua/sum.html?wrd=%D0%B1%D0%B5%D0%B7%D0%BF%D0%B5%D0%BA%D0%B0 (дата звернення: 26 листопада 2023 р.).

301. Ткачук П.П., Черник П.П. Діяльність структур інформаційно-психологічних операцій (на прикладі воєнної операції в Іраку). *Україна на*

рубежі XXI ст.: суспільно-політичні трансформації – це геополітичні виклики сучасності: Матеріали міжвузівської науково-практичної конференції, присвяченої 14-річчю незалежності України. Львів. 2005. 8 жовтня. С.69-84.

302. Топ абсурдних російських фейків про Україну за час повномасштабної війни. URL: https://www.slovoidilo.ua/2023/05/12/infografika/bezpeka/top-absurdnyx-rosijskyx-fejkiv-pro-ukrayinu-chas-povnomasshtabnoyi-vijny (дата звернення: 26 листопада 2023 р.).

303. Топчій В.В., Бодунова О.М., Проблемні питання забезпечення кібербезпеки в Україні. Аналітично-порівняльне правознавство. 2025. №1. С.664-669.

304. Увага! Нова кібератака групи Armageddon на державні органи України. URL: https://cip.gov.ua/ua/news/uvaga-nova-kiberataka-grupi-armageddon-na-derzhavni-organi-ukrayini (дата звернення: 16 липня 2025 р.).

305. Уздєнова Ю.М. Гібридна війна: сутність, складові та ключові поняття. *Вчені записки ТНУ імені В.І. Вернадського. Серія: Публічне управління та адміністрування*. 2024. №4. Том 35 (74). С.172-179.

306. Указ Президента України №685/2021 Про рішення Ради національної безпеки і оборони України від 15 жовтня 2021 року "Про Стратегію інформаційної безпеки". URL: https://www.president.gov.ua/documents/6852021-41069 (дата звернення: 26 листопада 2023 р.).

307. Україна-НАТО: спільна невійськова співпраця у протидії гібридній війні URL: https://ucipr.org.ua/index.php?option=com_content&view=article&id=516:ukra-na-nato-sp-lna-nev-yskova-sp-vpracya-u-protid-g-bridn-y-v-yn&catid=16& Itemid=186&lang=ua (дата звернення: 9 травня 2025 р.). .

308. Українці масово реєструються в Покровську, щоб стати громадянами Росії, а Терехов звернувся до Зеленського щодо протиправних дій з боку керівництва Харківської облради. Гвара медіа. URL: https://gwaramedia.com/ukraintsi-masovo-reiestruiutsia-v-pokrovsku-shchob-staty-

hromadianamy-rosii-a-terekhov-zvernuvsia-do-zelenskoho-shchodo-protypravnykh-diy-z-boku-kerivnytstva-kharkivskoi-oblrady-feykotnia-14-10-20-10/ (дата звернення: 9 травня 2025 р.).

309. У Генштабі ЗСУ спростували фейки рф щодо «причини» ракетного удару по Кривому Рогу. URL: https://armyinform.com.ua/2025/04/05/u-genshtabi-zsu-sprostuvaly-fejky-rf-shhodo-prychyny-raketnogo-udaru-po-kryvomu-rogu/ . (дата звернення: 5 червня 2025 р.).

310. У Запоріжжі СБУ викрила двох інтернет-агітаторів: закликали до підтримки окупантів. URL: https://imi.org.ua/news/u-zaporizhzhi-sbu-vykryla-dvoh-internet-agitatoriv-zaklykaly-do-pidtrymky-okupantiv-i53928 (дата звернення: 2 листопада 2023 р.).

311. У Сингапурі схвалили закон щодо боротьби з фейковими новинами URL: https://www.ukrinform.ua/rubric-world/2696925-u-singapuri-shvalili-zakon-sodo-borotbi-z-fejkovimi-novinami.html (дата звернення: 26 листопада 2023 р.).

312. У Сінгапурі ухвалили закон проти фейків і маніпуляцій URL: https://detector.media/infospace/article/167132/2019-05-09-u-singapuri-ukhvalyly-zakon-proty-feykiv-i-manipulyatsiy/ (дата звернення: 26 листопада 2023 р.).

313. У Сінгапурі штрафуватимуть або ув’язнюватимуть за фейкові новини URL: https://imi.org.ua/news/u-sinhapuri-shtrafuvatymut-abo-uv-iazniuvatymut-za-feykovi-novyny-i23200 (дата звернення: 22 травня 2024 р.).

314. У Франції виявили масштабну онлайн-кампанію, спрямовану на поширення дезінформації про війну РФ в Україні. URL: https://zmina.info/news/u-francziyi-vyyavyly-masshtabnu-onlajn-kampaniyu-spryamovanu-na-poshyrennya-dezinformacziyi-pro-vijnu-rf-v-ukrayini/ (дата звернення: 22 травня 2024 р.).

315. У Франції прийняли закон проти фейків та пропаганди: росіяни обурені. URL: https://www.eurointegration.com.ua/news/2018/07/8/7084090/ (дата звернення: 22 травня 2024 р.).

316. У Черкасах після бійки в храмі вірянам УПЦ МП відмовили у медичній допомозі, а Міноборони України створило агітаційний ролик з

військовими КНДР. Гвара медіа. URL: https://gwaramedia.com/u-cherkasakh-pislia-biyky-v-khrami-virianam-upts-mp-vidmovyly-u-medychniy-dopomozi-a-minoborony-ukrainy-stvorylo-ahitatsiynyy-rolyk-z-viyskovymy-kndr-feykotnia-04-10-10-11/ (дата звернення: 22 грудня 2024 р.).

317. Фанок Н. "Крематорій для ЗСУ у Тернопільській області" – новий фейк від російських пропагандистів. URL: https://zahid.espreso.tv/suspilstvo-krematoriy-dlya-zsu-u-ternopilskiy-oblasti-noviy-feyk-vid-rosiyskikh-propagandistiv (дата звернення: 16 вересня 2025 р.).

318. Федонюк С. Інформаційно-психологічні операції на геополітичній арені: навч. посіб.. Луцьк: Вежа-Друк, 2024. URL: https://evnuir.vnu.edu.ua/bitstream/123456789/24508/1/pos_ipo2%2021.06.pdf (дата звернення: 16 липня 2025 р.).

319. Фейки, які цього тижня поширювала пропаганда рф. URL: https://armyinform.com.ua/2024/02/11/fejky-yaki-czogo-tyzhnya-poshyryuvala-propaganda-rf-2/ (дата звернення: 16 вересня 2025 р.).

320. Facebook - 20 років. Як він змінив світ URL: https://www.bbc.com/ukrainian/articles/clle6r729eeo (дата звернення: 9 травня 2025 р.).

321. Феклістов А.О. Особливості планування заходів інформаційної боротьби під час підготовки операції. *Збірник наукових праць "Системи управління, навігації та зв'язку"*. 2009. Вип. 3 (11). С. 184-186.

322. Фотофейк: Військовий 92-ї ОШБр напав з ножем на працівника ТЦК у Харкові. URL: https://voxukraine.org/fotofejk-vijskovyj-92-yi-oshbr-napav-z-nozhem-na-pratsivnyka-ttsk-u-harkovi (дата звернення: 16 вересня 2025 р.).

323. Фурашев В. Питання законодавчого визначення понятійно-категоріального апарату у сфері інформаційної безпеки. *Інформація і право*. 2012. № 1(4). С. 4 – 13.

324. Фурашев В.М. Сутність та визначення понять "інформаційна безпека" і "безпека інформації". URL: https://ippi.org.ua/sites/default/files/12fvmbbi.pdf (дата звернення: 6 вересня 2025 р.).

325. Хакери змогли зламати 70 урядових сайтів, зокрема сайт "Дії". Як це вдалося. URL: https://tech.liga.net/ua/ukraine/article/kak-hakery-smogli-vzlomat-70-pravitelstvennyh-saytov-i-kto-za-etim-mojet-stoyat (дата звернення: 9 травня 2025 р.).

326. Хакерська атака Росії на українську енергосистему: як це було? URL: https://texty.org.ua/articles/66125/Hakerska_ataka_Rosiji_na_ukrajinsku_jenergosystemu_jak-66125/ (дата звернення: 22 травня 2024 р.).

327. Цей день в історії: 4 лютого 2004 року почав роботу сервіс «The facebook» URL: https://mynizhyn.com/news/ukraina-i-svit/22644-cei-den-v-istoriyi-4-lyutogo-2004-roku-pochav-robotu-servis-thefacebook.html (дата звернення: 16 липня 2025 р.).

328. Центр стратегічних комунікацій та інформаційної безпеки. URL: https://mcsc.gov.ua/projects/a-href-https-spravdi-gov-ua-tsentr-stratehichnykh-komunikatsiy-ta-informatsiynoi-bezpeky-a (дата звернення: 22 травня 2024 р.).

329. Центр стратегічних комунікацій назвав найгучніші фейки росіян, спростовані минулого тижня. URL: https://zmina.info/news/tsentr-stratehichnykh-komunikatsiy-nazvav-nayhuchnishi-feyky-rosiyan-sprostovani-mynuloho-tyzhnya/ (дата звернення: 9 травня 2024 р.).

330. CS50: Вступ до кібербезпеки URL: https://prometheus.org.ua/prometheus-free/cs50-cybersecurity/ (дата звернення: 9 травня 2025 р.).

331. Цимбалюк В.С. Кібербезпека в системі національної безпеки України: теоретико-правовий аспект. Львів: Світ. 2015. 290 с.

332. Цифрова безпека та комунікація в онлайні. URL: https://vumonline.ua/course/digital-security-and-communication-online/ (дата звернення: 22 травня 2024 р.).

333. Черник П.П., Шумка А.В. Інформаційно-психологічні операції у війнах та збройних конфліктах другої половини XX – початку XXI ст. *Вісник*

Національного університету «Львівська політехніка». 2008. № 634: Держава та армія. С. 126–133.

334. Чуприна А. Роль соціальних мереж у кризовій комунікації в умовах війни. *European Business Association.* URL: https://eba.com.ua/rol-sotsialnyh-merezh-u-kryzovij-komunikatsiyi-v-umovah-vijny/ дата звернення: 26 листопада 2023 р.).

335. Шевченко Л. Microsoft зірвала спробу російської кібератаки проти України. URL: https://tech.liga.net/ua/other/novosti/microsoft-sorvala-popytku-rossiyskoy-kiberataki-protiv-ukrainy (дата звернення: 9 травня 2025 р.).

336. Шеломенцев В. П. Сутність організаційного забезпечення системи кібернетичної безпеки України та напрями його удосконалення. *Боротьба з організованою злочинністю і корупцією (теорія і практика)*. 2012. № 2 (28). С. 299-309.

337. Шостак В. "Хліб по 50 гривень, а в країні – немає світла": які фейки поширює пропаганда РФ на окупованих територіях. URL: https://suspilne.media/dnipro/868609-hlib-po-50-griven-a-v-kraini-nemae-svitla-aki-fejki-posirue-propaganda-rf-na-okupovanih-teritoriah/ (дата звернення: 16 липня 2025 р.).

338. Шульга В. І. Сучасні підходи до трактування поняття інформаційна безпека. *Ефективна економіка.* 2015. №4. URL: http://www.economy.nayka.com.ua/?op=1&z=5514 (дата звернення: 6 листопада 2025 р.).

339. Що таке астротурфінг? URL: https://uchoose.uacrisis.org/shho-take-astroturfing/. (дата звернення: 6 листопада 2025 р.).

340. Що таке великі дані (Big Data)? URL: https://university.sigma.software/what-is-big-data/ (дата звернення: 26 листопада 2024 р.).

341. Що таке Google+: Історія та особливості соціальної мережі. URL: https://miraa.com.ua/shho-take-google-istoriya-ta-osoblyvosti-soczialnoyi-merezhi/ (дата звернення: 16 липня 2025 р.).

342. Щодо інформаційно-психологічної складової агресії Російської Федерації проти України (за результатами подій 1-2 березня 2014 року). Аналітична записка. URL: https://web.archive.org/web/20160819094834/http://www.niss.gov.ua/articles/147/ (дата звернення: 26 листопада 2023 р.).

343. USAID втратила контроль над біолабораторіями в Україні, а командир 81-ї бригади ЗСУ розстріляв трьох підлеглих за невиконання наказу. Фейкотня 03.02 – 16.02. URL: https://gwaramedia.com/usaid-vtratila-kontrol-nad-biolaboratoriyami-v-ukrayini-a-komandir-81-yi-brigadi-zsu-rozstrilyav-troh-pidleglih-za-nevikonannya-nakazu-fejkotnya-03-02-16-02/ (дата звернення: 9 вересня 2025 р.).

344. Яворська Г Гібридна війна як дискурсивний конструкт. URL: https://ippi.org.ua/sites/default/files/yavorskaya.pdf (дата звернення: 19 вересня 2025 р.).

345. Яковець А.Ю., Лапка О.Я. Протидія дезінформації та фейковим новинам в умовах надзвичайних правових режимів. *Інформаційна безпека суспільства в умовах дії правового режиму воєнного стану та повоєнний період : зб. матеріалів* (Київ, 29 трав. 2025 р.) / Редкол. : О. С. Тарасенко та ін. Київ : Нац. акад. внутр. справ, 2025. С.177-179.

346. Як Кремль відродив фейк про "американські біолабораторії" в Україні під час коронавірусу. URL: https://www.bbc.com/ukrainian/news-52615461 (дата звернення: 9 вересня 2025 р.).

347. Як російська пропаганда висвітлювала операцію ЗСУ в Курській області. URL: https://gwaramedia.com/ukraintsi-prodaiut-vkradeni-ikony-sudzha-tse-sumshchyna-ta-inshi-feyky-pro-kursku-oblast-iaki-poshyriuvala-rosiyska-propahanda-u-serpni/ (дата звернення: 3 січня 2025 р.).

348. Як російський інформаційний корабель пішов на...: суспільно-політичне видання. К.: Саміт-книга, 2023. URL: https://spravdi.gov.ua/wp-content/uploads/2024/02/yak-rosijskyj-informaczijnyj-korabel-pishov-na…-naratyvy-

propagandy-pid-chas-povnomasshtabnoyi-vijny.pdf (дата звернення: 19 травня 2024 р.).

349. Яровенко Г. Системний підхід до формалізації поняття «інформаційна безпека». *Причорноморські економічні студії.* 2018. №34. С.239-244.

350. Act to Improve Enforcement of the Law in Social Networks (Network Enforcement Act). URL: https://www.bmjv.de/SharedDocs/Downloads/DE/Gesetzgebung/RefE/NetzDG_engl.pdf?__blob=publicationFile&v=4&utm (дата звернення: 9 травня 2025 р.).

351. Analysis of russia's information campaign against Ukraine Examining non-military aspects of the crisis in Ukraine from a strategic communications perspectives. URL: https://stratcomcoe.org/cuploads/pfiles/russian_information_campaign_public_12012016fin.pdf (дата звернення: 26 листопада 2023 р.).

352. Aro J. The Cyberspace War: Propaganda and Trolling as Warfare Tools. European View, 2016. №15. PP. 121–132.

353. Cebrowski A. K., Garstka J. J. Network-centric warfare: Its origin and future. *Proceedings of the U.S. Naval Institute*. 1998. Vol. 124, No. 1. P. 103-116

354. Clausius M. The Banning of TikTok, and the Ban of Foreign Software for National Security Purposes. *Washington university global studies law review*. 2022. Volume 21, Issue 2. P.273-292.

355. Code of Practice on Disinformation. URL: https://digital-strategy.ec.europa.eu/en/policies/code-practice-disinformation (дата звернення: 9 травня 2025 р.).

356. Countering Foreign Interference URL: https://www.iss.europa.eu/projects/countering-foreign-interference (дата звернення: 22 травня 2024 р.).

357. Countering Foreign Propaganda and Disinformation Act. URL: https://www.congress.gov/bill/114th-congress/senate-bill/3274 (дата звернення: 2 жовтня 2024 р.).

358. Craig A. Horne, Sean B. Maynard, Atif Ahmad A. Theory on Information Security: A Pilot Study. URL: https://aisel.aisnet.org/cgi/viewcontent.cgi?article= 1014&context=wisp2019 (дата звернення: 2 серпня 2024 р.).

359. Cyber War in Perspective: Russian Aggression against Ukraine. URL: https://web.archive.org/web/20160816132103/https://ccdcoe.org/multimedia/cyber-war-perspective-russian-aggression-against-ukraine.html (дата звернення: 12 липня 2023 р.).

360. Digital Services Act. URL: https://eur-lex.europa.eu/eli/reg/2022/2065/oj/eng (дата звернення: 2 жовтня 2024 р.).

361. Invisible Russian cyberweapon stalked US and Ukraine since 2005, new research reveals. URL: https://web.archive.org/web/20160413202342/http://www.techworld.com/news/security/invisible-russian-cyberweapon-stalked-us-ukraine-since-2005-new-research-reveals-3505688/ (дата звернення: 9 травня 2025 р.).

362. Groseth C. An Economic Analysis of Banning TikTok: How to Weigh the Competing Interests of National Security and Free Speech in Social Media Platforms. URL: https://papers.ssrn.com/sol3/papers.cfm?abstract_id=3750779 (дата звернення: 9 травня 2025 р.).

363. Hoffman F. Conflict in the 21st Century: The Rise of Hybrid Wars. . Potomac Institute for Policy Studies, 2007. 72 p. URL: https://www.potomacinstitute.org/images/stories/publications/potomac_hybridwar_0108.pdf (дата звернення: 19 травня 2025 р.).

364. Hoffman F. G. Future Threats and Strategic Thinking. *Military Strategy Magazine*. 2011. Volume 1, Issue 4. URL: https://www.militarystrategymagazine.com/article/future-threats-and-strategic-thinking/ (дата звернення: 19 травня 2025 р.).

365. Hryshchuk R. Theoretical Foundations of Modeling the Processes of Attack on Information by the Methods of Theories of Differential Games and Differential Transformations. Zhytomyr: Ruta. 2010. 280 p

366. 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.

367. 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.

368. 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: 19 травня 2025 р.).

369. Laracy J.R., Marlowe T. Systems Theory and In-formation Security: Foundations for a New Educational Approach. *Information Security Education Journal*. 2018, Vol. 5. №2. P. 35-48.

370. McSweeney S. Our ongoing approach to the war in Ukraine. URL: https://blog.x.com/en_us/topics/company/2022/our-ongoing-approach-to-the-war-in-ukraine (дата звернення: 19 травня 2023 р.).

371. Media IQ. URL: https://media-iq.tilda.ws (дата звернення: 19 серпня 2024 р.).

372. Microsoft, Defending Ukraine: Early Lessons from the Cyber War. 2022. URL:https://query.prod.cms.rt.microsoft.com/cms/api/am/binary/RE50 KOK (дата звернення: 26 листопада 2023 р.).

373. New wave of cyberattacks against Ukrainian power industry | WeLiveSecurity. URL: https://www.welivesecurity.com/2016/01/20/new-wave-attacks-ukrainian power-industry/ (дата звернення: 9 травня 2025 р.).

374. Nmah Othello N. The effects of social media on national security. URL: https://apps.dtic.mil/sti/trecms/pdf/AD1105214.pdf (дата звернення: 9 травня 2025 р.).

375. Oremus W. Social media wasn’t ready for this war. It needs a plan for the next one. URL: https://www.washingtonpost.com/technology/2022/03/25/social-media-ukraine-rules-war-policy (дата звернення: 26 вересня 2024 р.).

376. Oxford English Dictionary. URL: http://www.askoxford.com (дата звернення: 22 травня 2024 р.).

377. Paul C., Matthews M. The Russian “Firehose of Falsehood” Propaganda Model. URL: https://www.rand.org/pubs/perspectives/PE198.html (дата звернення: 26 листопада 2023 р.).

378. Posthumus S., Von Solms R. A Framework for the Governance of Information Security. *Computers & Security.* 2004. №23(8). P.638-646.

379. ProtectEU: Нова стратегія внутрішньої безпеки ЄС із фокусом на кібербезпеку. URL: https://cybersec.net.ua/statti/846-protecteu-nova-stratehiia-vnutrishnoi-bezpeky-yes-iz-fokusom-na-kiberbezpeku.html (дата звернення: 2 жовтня 2024 р.).

380. Ribeiro A. European Commission rolls out ProtectEU strategy to boost internal security, resilience against hybrid threats. URL: https://industrialcyber.co/regulation-standards-and-compliance/european-commission-rolls-out-protecteu-strategy-to-boost-internal-security-resilience-against-hybrid-threats/ (дата звернення: 18 грудня 2024 р.).

381. Rogers R.W. A Protection Motivation Theory of Fear Appeals and Attitude Changeю *The Journal of Psychology.* 1975. №91 (1). P. 93-114.

382. Shakarian P., Shakarian Y., Ruef A. Introduction to cyber-warfare: a multidisciplinar/ approach. Amsterdam; Boston: Syngress, 2017. 318 p.

383. StopFake. URL: http://www.stopfake.org/ (дата звернення: 9 травня 2025 р.).

384. Strukturreform av krisberedskap och civilt försvar. URL: https://www.msb.se/sv/amnesomraden/krisberedskap--civilt-forsvar/det-svenska-civila-beredskapssystemet/strukturreform-av-krisberedskap-och-civilt-forsvar/ (дата звернення: 26 листопада 2023 р.).

385. Szwed R. Framing of the Ukraine–Russia conflict in online and social media. URL: https://stratcomcoe.org/publications/framing-of-the-ukrainerussia-conflict-in-online-and-social-media/175 (дата звернення: 2 жовтня 2024 р.).

386. Von Solms R., Van Niekerk, J. From Information Security to Cyber Security. *Computers & Security.* 2013. №38. P.97-102.

ДОДАТКИ

Додаток А

Список публікацій здобувача за темою дисертації та відомості про апробацію результатів дисертації

Статті у фахових виданнях України категорії Б:

1. Савлюк М. Теоретико-методологічні засади дослідження інформаційної безпеки. *Вісник Прикарпатського університету. Серія: Політологія*. *2023*. Випуск 15. 2023. С.60-68

DOI: https://doi.org/10.32782/2312-1815/2024-1-8

URL: https://journals.pnu.if.ua/index.php/politology/article/view/54

2. Савлюк М. Гібридна війна в Україні: сучасні підходи. *Вісник Прикарпатського університету. Серія: Політологія*. 2024. Випуск 17. С.187-197.

DOI: https://doi.org/10.32782/2312-1815/2024-17-23

URL: https://journals.pnu.if.ua/index.php/politology/article/view/130

3. Савлюк М. Важливість інформаційної безпеки в соціальних мережах для загальнонаціональної безпеки: безпековий вимір України. *Вісник Прикарпатського університету. Серія: Політологія.* 2024. Випуск 18. С.300-309.

DOI: https://doi.org/10.32782/2312-1815/2024-18-30

URL: https://journals.pnu.if.ua/index.php/politology/article/view/167

4. Пролорензо А. Савлюк М. Кіберзахист як складник інформаційної безпеки держави в умовах гібридної війни. *Національні інтереси України*. 2025. №6 (11). С.198-213

DOI: https://doi.org/10.52058/3041-1793-2025-6(11)-198-213

URL: https://perspectives.pp.ua/index.php/niu/article/view/25245/25222

Наукові праці, які засвідчують апробацію матеріалів дисертації:

5. Савлюк М. Інформаційна безпека в соціальних мережах: безпековий вимір для держави. *Публічне управління та адміністрування в Україні: Євроінтеграційний поступ:* збірник матеріалів ІІ Всеукраїнської науково-

практичної конференції за міжнародної участі (м. Івано-Франківськ, 30 травня 2025 р.). Івано-Франківськ, 2025. С.101-104.
URL:https://nung.edu.ua/sites/default/files/2025-06/Збірник_тез_ІФНТУНГ_Т.2_2025_0.pdf

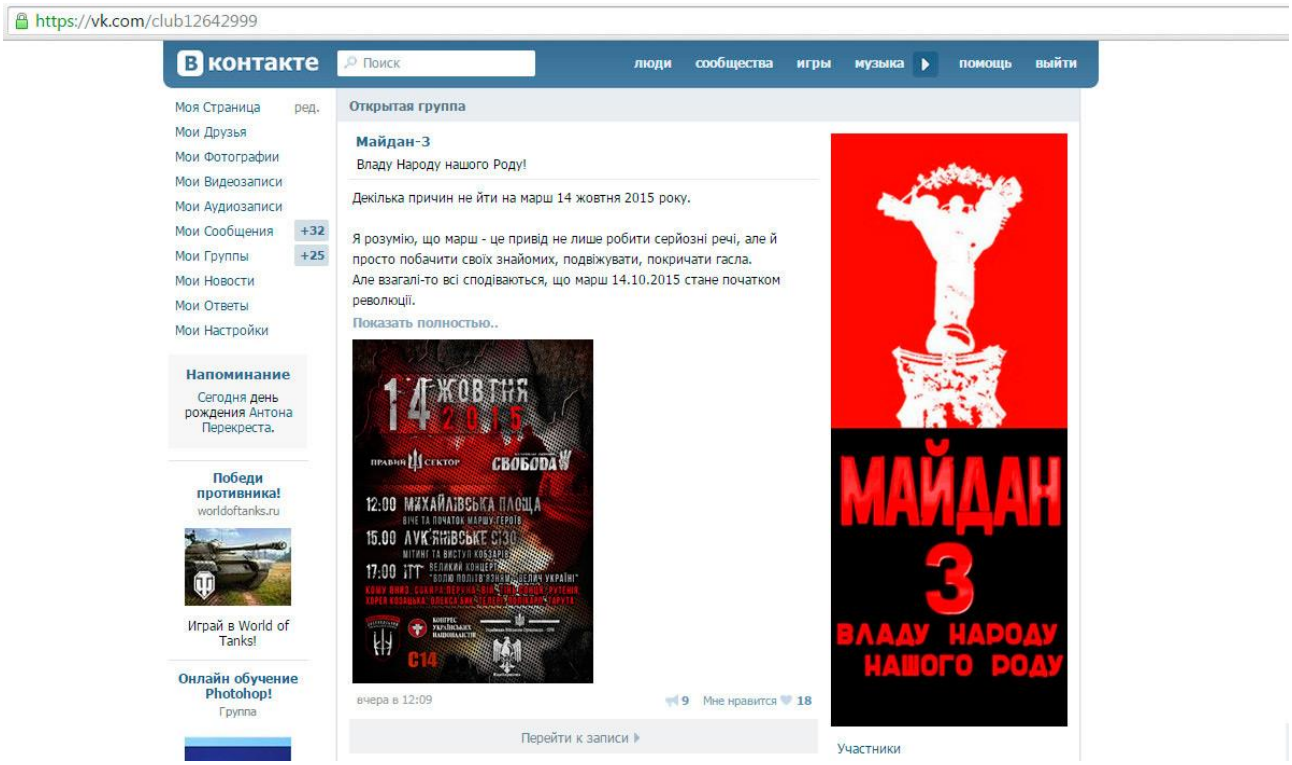
6. Савлюк М. Політика забезпечення інформаційної безпеки: міжнародний контекст. *Проблеми забезпечення інформаційної безпеки в міжнародному співробітництві*: матеріали міжнародної науково-практичної конференції, 5 вересня 2025 року. Ужгород, 2025. С.211-218.

7. Савлюк М. Теоретико-методологічні засади дослідження інформаційної безпеки як складник організаційно-правових засад функціонування системи безпеки критичної інфраструктури України. *Національна стійкість (резилієнтність) як ключовий елемент національної безпеки: архітектура, виклики та шляхи посилення*. Збірник матеріалів І Міжнародної науково-практичної конференції (м. Івано-Франківськ, 27 листопада 2025 р.). Івано-Франківськ, 2025. С.199-202.
URL: nung.edu.ua/sites/default/files/2025-12/Збірник_тез_ІФНТУНГ_2025.pdf

8.Савлюк М. Сучасна протидія інформаційним загрозам: вітчизняний та світовий досвід. *Всеукраїнська науково-практична конференція здобувачів вищої освіти та молодих учених: Національна безпека України в умовах воєнного стану: проблеми та шляхи їх вирішення*: зб. матеріалів всеукраїнської наук.-практ. конф. (м. Одеса, 20 березня 2026 р.). Одеса: Військова академія, 2026. С.359-360.

Додаток Б

Заклики до насильницьких дій проти української влади та провокували ідею «Третього Майдану»



Джерело: Саєнко О. Г. Механізм інформаційно-психологічного впливу в умовах гібридної війни. URL: https://nadpsu.edu.ua/wp-content/uploads/2021/09/visnik_1_2015_psh.pdf (дата звернення: 26 листопада 2023 р.).

Додаток В

СБУ рекомендують утриматися від використання інтернет-ресурсів російської доменної зони. Список російських соцмереж.

- 1. Яндекс – http://www.yandex.ru/
- 2. ВКонтакте – http://vk.com/
- 3. Одноклассники – http://www.odnoklassniki.ru/
- 4. Фотострана – http://fotostrana.ru/
- 5. Привет.ру – http://privet.ru/
- 6. LiveInternet – http://www.liveinternet.ru/
- 7. Toodoo – http://toodoo.ru/
- 8. LJ.Rossia.org – http://lj.rossia.org/
- 9. Блоги@Mail.Ru – http://blogs.mail.ru/
- 10. Моя живая страница – http://www.mylivepage.ru/
- 11. MirTesen.ru – http://mirtesen.ru/
- 12. Дневник на TKS.RU – http://blogs.tks.ru/portal.php
- 13. Клерк.ru – http://www.klerk.ru/
- 14. Beon.ru – http://beon.ru/
- 15. БебиБлог – http://www.babyblog.ru/
- 16. Блогус – http://www.blogus.ru/blog.php
- 17. ITBlogs – http://itblogs.ru/
- 18. Рыболовный клуб – http://www.fion.ru/
- 19. RuSpace – http://www.ruspace.ru/
- 20. Re: vision – http://www.revision.ru/
- 21. Diary.Ru – http://www.diary.ru/
- 22. LiveLib – http://www.livelib.ru/
- 23. Карта для любителей рыбалки – http://www.fishingmap.ru/
- 24. Сообщество влюбленных в кино – http://www.ilovecinema.ru/
- 25. 100 Друзей – http://www.100druzei.ru/
- 26. Dogster – http://www.dogster.ru/
- 27. Факультет.ру – http://www.facultet.ru/
- 28. Тейст – http://www.mmm-tasty.ru/
- 29. Вебкруг – http://www.webkrug.ru/
- 30. VeniVidi – http://venividi.ru/

- 31. Я талант – http://yatalant.ru/
- 32. Мой мир – http://my.mail.ru/
- 33. ЛИМП – http://www.limpa.ru/
- 34. Spaces.ru – http://spaces.ru
- 35. Мой Круг – http://moikrug.ru/
- 36. Соседи-Онлайн – http://sosedi-online.ru/
- 37. По Баранкой – http://zabarankoi.ru/
- 38. Юмами – http://www.u-mama.ru/
- 39. Автокадабру – http://autokadabra.ru/
- 40. Отдохнули.ру – http://www.otdohnuli.ru/
- 41. Telefoner.ru – http://www.telefoner.ru/
- 42. Одноклассники.КМ.РУ – http://vkrugudruzei.ru

Джерело: СБУ радить українцям видаляти аккаунти з російських соцмереж. URL:https://espreso.tv/news/2014/07/28/sbu_radyt_ukrayincyam_vydalyaty_akkaunty_z_rosiyskykh_socmerezh.

Додаток Г

Фейковий лист до органів влади та державних структур начебто за підписом прем'єр-міністра Дениса Шмигаля від 30 червня 2025 року.

Джерело: Богданьок О. Російська пропаганда поширює фейковий «лист Шмигаля» про евакуацію держустанов - ЦПД. URL: https://suspilne.media/1058665-rosijska-propaganda-posirue-fejkovij-list-smigala-pro-evakuaciu-derzustanov-cpd/.

Додаток Д

Джерело: Топ абсурдних російських фейків про Україну за час повномасштабної війни. URL: https://www.slovoidilo.ua/2023/05/12/infografika/bezpeka/top-absurdnyx-rosijskyx-fejkiv-pro-ukrayinu-chas-povnomasshtabnoyi-vijny.

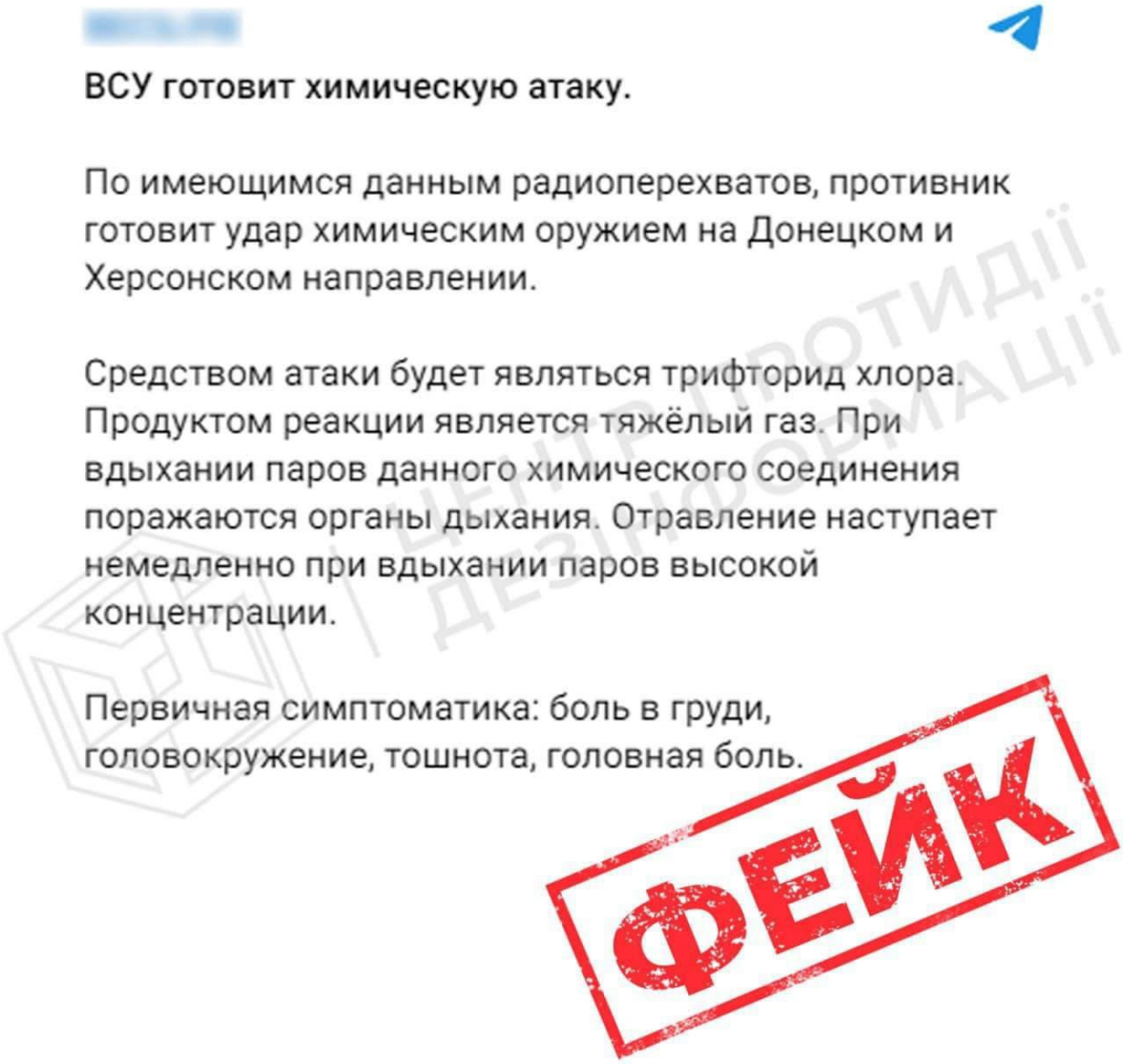
Додаток Е

Фейкові TG - канали

Джерело: Росіяни активно створюють фейкові телеграм-канали українських бригад і батальйонів – ЦПД. URL: https://zmina.info/news/rosiyany-aktyvno-stvoryuyut-fejkovi-telegram-kanaly-ukrayinskyh-brygad-i-bataljoniv-spravdi/.

Додаток Є

Окупанти поширюють фейки про те, що ЗСУ здійснюватимуть хімічні атаки



Джерело: Окупанти поширюють фейки про те, що ЗСУ здійснюватимуть хімічні атаки. URL: https://armyinform.com.ua/2024/07/17/okupanty-poshyryuyut-fejky-pro-pidgotovku-zsu-himichnyh-atak/.

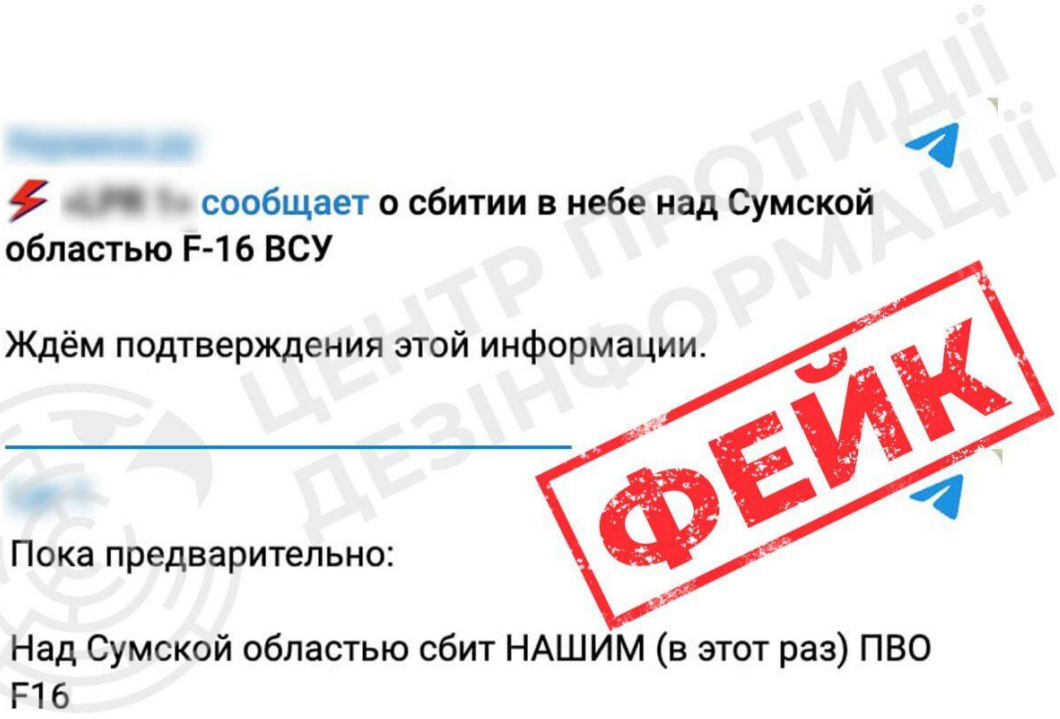
Додаток Ж

Російська пропаганда поширює фейки щодо планів України підірвати окуповану ЗАЕС

Джерело: Російська пропаганда поширює фейки щодо планів України підірвати окуповану ЗАЕС. URL: https://www.ukrinform.ua/rubric-factcheck/3853306-rospropaganda-posirue-fejki-pro-nibito-plani-ukraini-pidirvati-zaes.html

Додаток З

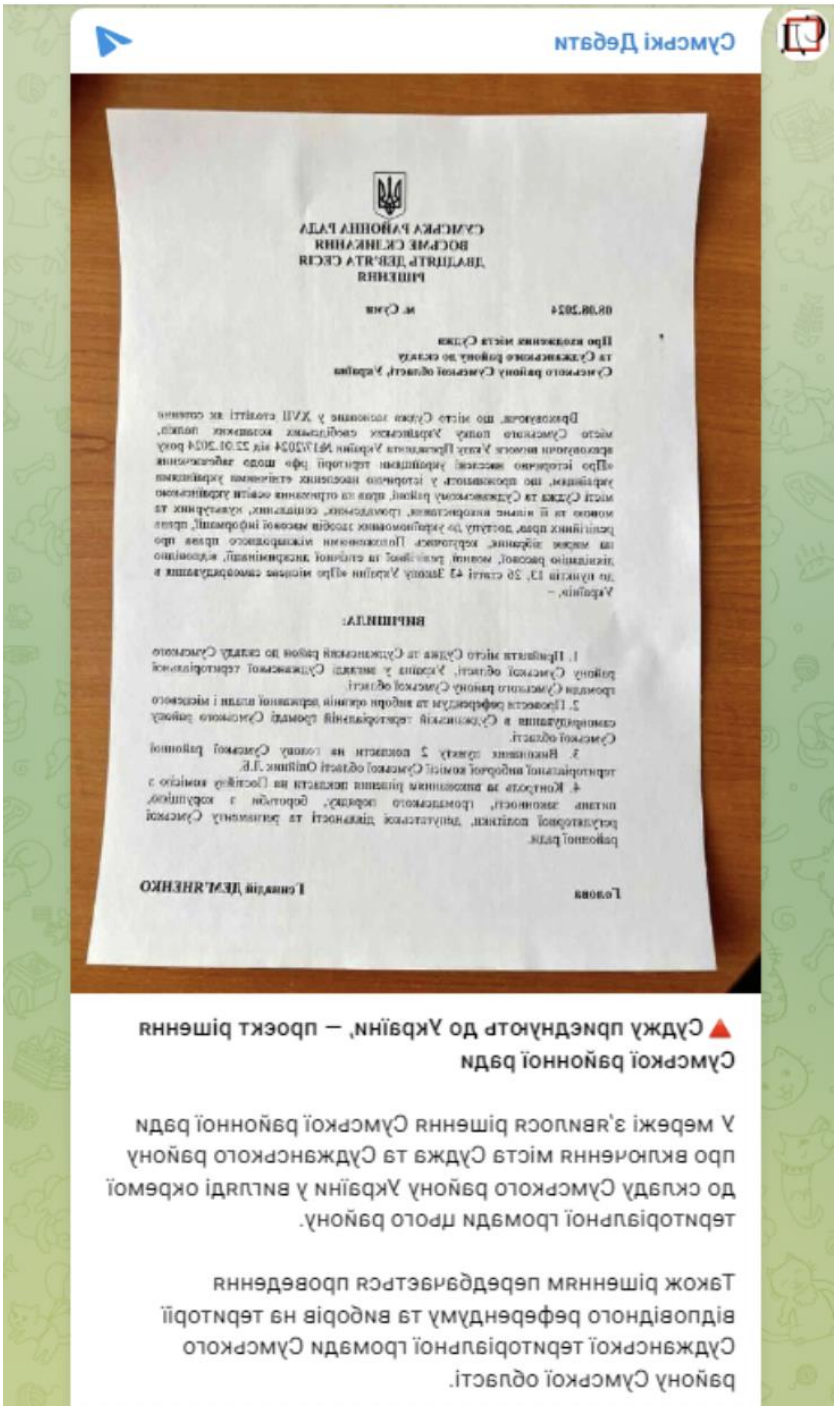
Збрехали - російські пропагандисти вигадали збиття F-16 над Сумщиною



Джерело: Збрехали - російські пропагандисти вигадали збиття F-16 над Сумщиною. URL: https://armyinform.com.ua/2025/03/19/zbrehaly-rosijski-propagandysty-vygadaly-zbyttya-f-16-nad-sumshhynoyu/.

Додаток І

Рішення нібито Сумської районної ради про включення міста Суджа та Суджанського району до складу Сумського району України



Джерело: Як російська пропаганда висвітлювала операцію ЗСУ в Курській області. URL: https://gwaramedia.com/ukraintsi-prodaiut-vkradeni-ikony-sudzha-tse-sumshchyna-ta-inshi-feyky-pro-kursku-oblast-iaki-poshyriuvala-rosiyska-

propahanda-u-serpni/.

Додаток Ї

Фейк про «крематорій у Тернопільській області», де нібито знищують тіла загиблих військових ЗСУ.

Джерело: Фанок Н. "Крематорій для ЗСУ у Тернопільській області" – новий фейк від російських пропагандистів. URL: https://zahid.espreso.tv/suspilstvo-krematoriy-dlya-zsu-u-ternopilskiy-oblasti-noviy-feyk-vid-rosiyskikh-propagandistiv

Додаток К

StopFake

Джерело: StopFake. URL: http://www.stopfake.org/

Додаток Л

Пропоновані зміни та ініціативи до Доктрини інформаційної безпеки України та Стратегії кібербезпеки України

Сфера вдосконалення	Доктрина інформаційної безпеки України	Стратегія кібербезпеки України
Нормативно-правове забезпечення	Оновлення положень з урахуванням сучасних гібридних загроз, включно з інформаційними операціями та когнітивними впливами	Гармонізація законодавства з нормами ЄС і НАТО у сфері кібербезпеки, уточнення відповідальності суб'єктів кіберзахисту
Інституційна система	Посилення координаційної ролі державних органів у сфері інформаційної безпеки	Розширення повноважень національного координаційного центру кібербезпеки та міжвідомчої взаємодії
Протидія дезінформації	Запровадження системного моніторингу інформаційного простору та механізмів оперативного реагування	Інтеграція автоматизованих систем виявлення кіберінцидентів та інформаційних атак
Співпраця з приватним сектором	Розвиток державно-приватного партнерства у сфері інформаційної безпеки	Розширення взаємодії з IT-компаніями, провайдерами та міжнародними платформами
Міжнародне співробітництво	Активізація участі у міжнародних інформаційно-безпекових ініціативах	Поглиблення інтеграції в системи кіберзахисту ЄС та НАТО, обмін кіберінформацією
Технологічний розвиток	Впровадження сучасних технологій аналізу інформаційних загроз (AI, Big Data)	Розвиток національних систем кіберзахисту з використанням штучного інтелекту
Захист критичної інфраструктури	Посилення інформаційного захисту об'єктів критичної інфраструктури	Розширення технічних та організаційних заходів кіберзахисту критичних систем
Кадровий потенціал	Підготовка фахівців з інформаційної безпеки та медіаграмотності	Формування національної системи підготовки кіберфахівців та підвищення кваліфікації

Джерело: розробка автора