КИЇВСЬКИЙ НАЦІОНАЛЬНИЙ УНІВЕРСИТЕТ
ІМЕНІ ТАРАСА ШЕВЧЕНКА
МІНІСТЕРСТВО ОСВІТИ І НАУКИ УКРАЇНИ

Кваліфікаційна наукова праця
на правах рукопису

Грицай Роман Олексійович

УДК 35-027.21:351.86](477)

ДИСЕРТАЦІЯ

ОСОБЛИВОСТІ ДЕРЖАВНОЇ СТРАТЕГІЇ ПРОТИДІЇ ІНФОРМАЦІЙНІЙ ВІЙНІ

Спеціальність 281 «Публічне управління та адміністрування»
Галузь знань 28 «Публічне управління та адміністрування»

Подається на здобуття ступеня доктора філософії
у галузі публічного управління та адміністрування

Дисертація містить результати власних досліджень. Використання ідей, результатів і текстів інших авторів мають посилання на відповідне джерело
_____ Грицай Р.О.

Науковий керівник – Зубчик Олег Анатолійович,
доктор наук з державного управління, доцент.

Київ – 2026

АНОТАЦІЯ

Грицай Р. О. Особливості державної стратегії протидії інформаційній війні. – Кваліфікаційна наукова праця на правах рукопису.

Дисертація на здобуття ступеня доктора філософії з галузі знань 281 «Публічне управління та адміністрування» за спеціальністю 281 «Публічне управління та адміністрування». – Київський національний університет імені Тараса Шевченка, Київ, 2026.

Дисертаційне дослідження є одним із перших комплексних досліджень, у якому розроблені напрями формування та реалізації державної стратегії протидії інформаційній війні з урахуванням сучасного стану законодавства, практики публічного управління, умов воєнного стану, цифровізації суспільних комунікацій та зростання деструктивних інформаційних впливів. Сукупність одержаних висновків і рекомендацій має важливе значення для вдосконалення організаційно-управлінських механізмів координації суб'єктів державної політики у відповідній сфері, підвищення результативності стратегічних комунікацій, забезпечення інформаційної стійкості держави та суспільства, а також зміцнення спроможності публічної влади своєчасно виявляти, попереджати й нейтралізувати загрози інформаційного характеру.

Визначено, що інформаційна війна є складовою сучасних загроз інформаційній безпеці держави, оскільки поєднує інформаційно-психологічний, комунікаційний, технологічний і кібернетичний вплив на державу, суспільство та суспільну свідомість, спрямований на дестабілізацію суспільно-політичних процесів, підрив довіри до державних інституцій, послаблення суспільної єдності та ослаблення інформаційного суверенітету держави.

Запропоновано теоретичні положення щодо класифікації, змісту та особливостей сучасних пропагандистських технологій і методів, небезпека яких зумовлена їх комплексністю, високою адаптивністю до нових умов та здатністю поєднуватися з кіберзагрозами і психологічними методами впливу,

а також обґрунтовано пріоритетність системної протидії таким технологіям у межах державної політики у сфері інформаційної безпеки шляхом виявлення ворожих наративів, оперативного спростування маніпулятивного контенту, зміцнення стратегічних комунікацій і підвищення рівня медіаграмотності населення. Розкрито значення державної інформаційної політики як інструменту протидії пропаганді та інформаційній війні, що забезпечує формування узгодженої системи офіційної комунікації, нормативно-правового регулювання та інституційної взаємодії у сфері захисту інформаційного простору держави.

Окреслений механізм формування державної стратегії протидії інформаційній війні. На підставі аналізу зарубіжного досвіду формування державної стратегії протидії інформаційній війні встановлено, що найбільш результативні підходи у провідних країнах Європи та США ґрунтуються на поєднанні інституційно оформлених стратегічних комунікацій, міжвідомчої координації, розвитку медіаграмотності, міжнародного партнерства та залучення суспільства до зміцнення інформаційної стійкості. Запропоновано праксеологічні засади використання зарубіжного досвіду, що передбачають адаптацію для України апробованих практик управлінських рішень щодо посилення координаційного центру, інституціоналізації медіаграмотності, розвитку урядових стратегічних комунікацій і спеціалізованого моніторингу зовнішніх інформаційних впливів.

Визначено, що формування державної стратегії протидії інформаційній війні має здійснюватися на основі чіткої системи принципів і стратегічних засад. До принципів такої стратегії віднесено верховенство права та законність, пріоритет прав і свобод людини, ідеологічну багатоманітність і недопустимість цензури, достовірність, повноту та своєчасність офіційної інформації, системність і міжвідомчу координацію, стійкість і адаптивність держави та суспільства, міжнародну взаємодію, а також поєднання інформаційної та кібернетичної складових безпеки. До стратегічних засад віднесено конституційно-безпекову природу, включеність у систему

стратегічного планування, міжсекторальний характер, доказовість, ресурсну забезпеченість, наявність чіткого механізму реалізації та зовнішньополітичний вимір. Науково обґрунтовано структурно-функціональну модель формування і реалізації державної стратегії протидії інформаційній війні за трьома рівнями: інституційним, функціонально-процесуальним та організаційно-управлінським. Розроблено стратифікаційну модель реалізації функцій публічного управління у сфері протидії інформаційній війні в умовах воєнного стану та забезпечення інформаційної безпеки держави, що дозволило здійснити системний аналіз і комплексний опис процесів формування та реалізації державної стратегії у зазначеній сфері, а також цілісно відобразити механізм державного реагування на інформаційні загрози з урахуванням динамічності інституційного середовища публічного управління, трансформації інформаційного простору та зміни характеру деструктивних інформаційних впливів.

Обґрунтовано теоретичні засади публічного управління у сфері протидії інформаційній війні та забезпечення інформаційної безпеки держави в умовах воєнного стану через авторську концепцію, в основу якої покладено поєднання модельного, інституційного та структурно-функціонального підходів, що дало змогу подати інституціоналізацію державних механізмів у зазначеній сфері як конкретно-історичний процес із притаманними йому внутрішньою логікою, послідовністю та закономірностями становлення і розвитку.

Сформульоване наукове бачення механізму державної політики у сфері протидії інформаційній війні та забезпечення інформаційної безпеки в умовах воєнного стану шляхом розроблення функціональної моделі визначення імперативів такої політики на основі характеристики сучасних тенденцій інформаційного протиборства, розвитку деструктивних інформаційних впливів, оцінки перспективного стану інформаційного простору та діагностики рівня інформаційної безпеки держави.

Запропоновано зміст механізму державного реагування на інформаційні загрози шляхом доповнення його національною рамкою комплексних

процедур, що передбачає поєднання механізмів проактивного реагування, спрямованого на раннє виявлення, попередження, стримування та нейтралізацію інформаційних загроз, і реактивного реагування, орієнтованого на локалізацію деструктивного впливу, мінімізацію його наслідків, стабілізацію інформаційної ситуації та відновлення належного функціонування інформаційного простору.

Виокремлено основні проблеми реалізації державної стратегії протидії інформаційній війні, які полягають у незахищеності державних цифрових ресурсів до кібератак, інформаційного втручання та технічного блокування, нерівномірному рівні користування електронними державними сервісами, високій залежності інформаційного споживання населення від соціальних мереж та інших цифрових платформ, поширенні через них маніпулятивного контенту, фейкових повідомлень і ворожих наративів, а також недостатній узгодженості між розвитком цифрових послуг, їх кіберзахистом і належним інформаційним супроводом. Запропоновано системно-функціональний підхід до аналізу та розв’язання цих проблем, що обумовлює необхідність комплексного посилення цифрової стійкості держави та вдосконалення механізмів державного реагування у відповідній сфері.

Розроблено в авторській редакції проєкт Концепції національної інформаційної політики України як цілісний програмний документ у сфері забезпечення інформаційної безпеки та протидії пропаганді, в якому системно визначено мету, принципи, завдання, напрями, суб’єктний склад, механізми реалізації, етапи впровадження, очікувані результати та показники результативності. Запропоновано трирівневу систему суб’єктів її реалізації та обґрунтовано комплекс механізмів практичного впровадження як методологічну й прикладну основу вдосконалення державної інформаційної політики України в умовах інформаційної війни.

Визначено доцільність запровадження у практику публічного управління Державної стратегії протидії інформаційній війні в Україні як цілісного стратегічного документа, у якому мають бути визначені правова

основа, понятійний апарат, принципи, стратегічні цілі, завдання, суб'єкти реалізації, механізми міжвідомчої координації, інформаційно-аналітичного супроводу та оцінювання ефективності, а також система загроз інформаційній безпеці, пріоритетні напрями державного реагування, заходи щодо поєднання інформаційної безпеки та кіберзахисту, розвитку стратегічних комунікацій, взаємодії з громадянським суспільством і міжнародними партнерами, кадрового, фінансового й технологічного забезпечення.

Ключові слова: інформація, інформаційна війна, інформаційна безпека, інформаційна загроза, державна політика, державна стратегія, протидія, пропаганда, дезінформація, стратегічні комунікації, інформаційний простір, публічне управління, механізм державного управління, інформаційна політика, інформаційна стійкість, національна безпека.

ANNOTATION

Hrytsay R. O. Peculiarities of the State Strategy for Countering Information Warfare. – Qualifying scientific work as a manuscript.

Dissertation for obtaining the degree of Doctor of Philosophy in the field of knowledge 281 "Public Management and Administration" in specialty 281 "Public Management and Administration." – Taras Shevchenko National University of Kyiv, Kyiv, 2026.

The dissertation research is one of the first comprehensive studies in which directions for the formation and implementation of the state strategy for countering information warfare are developed, taking into account the current state of legislation, public administration practice, the conditions of martial law, the digitalization of social communications, and the growth of destructive informational influences. The totality of the obtained conclusions and recommendations is of great importance for improving the organizational and managerial mechanisms of coordination of subjects of state policy in the relevant sphere, increasing the effectiveness of strategic communications, ensuring the information resilience of the

state and society, as well as strengthening the capacity of public authorities to timely detect, prevent, and neutralize threats of an informational nature.

It is determined that information warfare is a component of modern threats to the information security of the state, since it combines informational-psychological, communicative, technological, and cybernetic influence on the state, society, and public consciousness, aimed at destabilizing socio-political processes, undermining trust in state institutions, weakening social unity, and weakening the information sovereignty of the state.

Theoretical provisions regarding the classification, content, and peculiarities of modern propaganda technologies and methods are proposed, the danger of which is conditioned by their complexity, high adaptability to new conditions, and the ability to combine with cyber threats and psychological methods of influence; the priority of systematic counteraction to such technologies within the framework of state policy in the field of information security are also substantiated through the identification of hostile narratives, prompt refutation of manipulative content, strengthening of strategic communications, and raising the level of media literacy of the population. The significance of state information policy as an instrument for countering propaganda and information warfare are revealed, which ensures the formation of a coordinated system of official communication, regulatory and legal regulation, and institutional interaction in the field of protection of the information space of the state.

The mechanism for the formation of the state strategy for countering information warfare are outlined. On the basis of the analysis of foreign experience in the formation of the state strategy for countering information warfare, it is established that the most effective approaches in the leading countries of Europe and the United States are based on the combination of institutionally formalized strategic communications, interagency coordination, development of media literacy, international partnership, and involvement of society in strengthening information resilience. Praxeological principles for the use of foreign experience are proposed, which provide for the adaptation for Ukraine of tested practices of managerial

decisions regarding the strengthening of the coordination center, institutionalization of media literacy, development of governmental strategic communications, and specialized monitoring of external informational influences.

It is determined that the formation of the state strategy for countering information warfare should be carried out on the basis of a clear system of principles and strategic foundations. The principles of such a strategy include the rule of law and legality, the priority of human rights and freedoms, ideological diversity and inadmissibility of censorship, reliability, completeness, and timeliness of official information, systemicity and interagency coordination, resilience and adaptability of the state and society, international interaction, as well as the combination of informational and cybernetic components of security. The strategic foundations include the constitutional-security nature, inclusion in the system of strategic planning, intersectoral character, evidence-based nature, resource provision, the existence of a clear implementation mechanism, and the foreign policy dimension. A structural-functional model for the formation and implementation of the state strategy for countering information warfare at three levels are scientifically substantiated: institutional, functional-procedural, and organizational-managerial.

A stratification model for the implementation of public administration functions in the sphere of countering information warfare under the conditions of martial law and ensuring the information security of the state are developed, which made it possible to carry out a systemic analysis and comprehensive description of the processes of formation and implementation of the state strategy in the specified sphere, as well as to holistically reflect the mechanism of state response to informational threats, taking into account the dynamism of the institutional environment of public administration, the transformation of the information space, and changes in the nature of destructive informational influences.

The theoretical foundations of public administration in the sphere of countering information warfare and ensuring the information security of the state under the conditions of martial law are substantiated through the author’s concept, which is based on the combination of model, institutional, and structural-functional

approaches, which made it possible to present the institutionalization of state mechanisms in the specified sphere as a concrete-historical process with its inherent internal logic, sequence, and regularities of formation and development.

A scientific vision of the mechanism of state policy in the sphere of countering information warfare and ensuring information security under the conditions of martial law are formulated through the development of a functional model for determining the imperatives of such policy on the basis of the characteristics of modern trends in informational confrontation, the development of destructive informational influences, the assessment of the prospective state of the information space, and the diagnosis of the level of information security of the state.

The content of the mechanism of state response to informational threats are proposed by supplementing it with a national framework of comprehensive procedures, which provides for the combination of proactive response mechanisms aimed at early detection, prevention, deterrence, and neutralization of informational threats, and reactive response aimed at localizing destructive influence, minimizing its consequences, stabilizing the informational situation, and restoring the proper functioning of the information space.

The main problems of implementation of the state strategy for countering information warfare are distinguished, which consist in the vulnerability of state digital resources to cyberattacks, informational interference, and technical blocking, the uneven level of use of electronic state services, the high dependence of the population’s information consumption on social networks and other digital platforms, the spread through them of manipulative content, fake messages, and hostile narratives, as well as insufficient consistency between the development of digital services, their cyber protection, and proper informational support. A systemic-functional approach to the analysis and solution of these problems are proposed, which determines the need for comprehensive strengthening of the digital resilience of the state and improvement of mechanisms of state response in the relevant sphere.

A draft Concept of the National Information Policy of Ukraine in the author's wording are developed as a holistic program document in the field of ensuring information security and countering propaganda, in which the purpose, principles, tasks, directions, subject composition, implementation mechanisms, stages of introduction, expected results, and performance indicators are systematically defined. A three-level system of subjects of its implementation are proposed and a complex of mechanisms of practical implementation are substantiated as a methodological and applied basis for improving the state information policy of Ukraine under the conditions of information warfare.

The expediency of introducing into the practice of public administration the State Strategy for Countering Information Warfare in Ukraine as a holistic strategic document are determined, in which the legal basis, conceptual apparatus, principles, strategic goals, tasks, subjects of implementation, mechanisms of interagency coordination, information-analytical support and evaluation of effectiveness, as well as the system of threats to information security, priority directions of state response, measures regarding the combination of information security and cyber protection, development of strategic communications, interaction with civil society and international partners, personnel, financial, and technological support should be defined.

Keywords: information, information warfare, information security, informational threat, state policy, state strategy, counteraction, propaganda, disinformation, strategic communications, information space, public administration, mechanism of public administration, information policy, information resilience, national security.

СПИСОК ОПУБЛІКОВАНИХ ПРАЦЬ ЗА ТЕМОЮ ДИСЕРТАЦІЇ

Статті у наукових фахових виданнях України:

(які входять до переліку МОН України)

1. **Грицай Р. О.** (2023). Інформаційні війни: пошук стратегій протидії. Публічне управління і адміністрування в Україні, 33, 18–23. https://pag-

journal.iei.od.ua/archives/2023/33-2023/3.pdf https://doi.org/10.32782/pma2663-5240-2023.33.3

2. **Грицай, Р. О.** (2024). Практики та інструменти протидії інформаційній війні: досвід зарубіжних країн. Публічне управління і адміністрування в Україні, 39, 14–19. https://pag-journal.iei.od.ua/archives/2024/39-2024/4.pdf https://doi.org/10.32782/pma2663-5240-2024.39.2

3. Зубчик О.А., **Грицай Р. О.** (2025). Функціональна конвергентність суб'єктів публічного управління в системі протидії семантичним загрозам. Актуальні проблеми інноваційної економіки та права, 4, 131–142. https://doi.org/10.36887/2524-0455-2025-4-33 https://apie.org.ua/uk/publications-uk/2025-4/

4. Зубчик О. А., **Грицай Р. О.** Державна стратегія захисту когнітивного простору: архітектоніка та управлінські інструменти формування суспільної резильєнтності. Журнал "Актуальні проблеми інноваційної економіки та права". 2026 / #1. 143-147. https://apie.org.ua/uk/derzhavna-strateg%D1%96ia-zahistu-kogn%D1%96tiv/ https://doi.org/10.36887/2524-0455-2026-1-31

5. **Грицай Р.О.** Інформаційна політика у протидії пропаганді. *Журнал «Наукові інновації та передові технології»* № 3(55) 2026. С. 3005-3015. https://doi.org/10.52058/2786-5274-2026-3(55)-3005-3015 https://perspectives.pp.ua/index.php/nauka/article/view/39023/39033

6. **Грицай Р.О.** Сучасні методи пропаганди як фактор загроз національній інформаційній безпеці держави. *«Національні інтереси України».* №3(20) 2026. С. 1150-1162. https://doi.org/10.52058/3041-1793-2026-3(20)-1150-1162 https://perspectives.pp.ua/index.php/niu/article/view/39319/39333

Тези наукових доповідей:

Грицай Р. О. Концептуальні засади національної інформаційної політики як превентивний механізм протидії

пропаганді. *Актуальні питання діяльності Національної поліції як суб'єкту протидії організованій злочинності:* матеріали Всеукр. наук.-практ. конф. (Кропивницький, 2 квіт. 2026 р.). Кропивницький, 2026.

Грицай Р. О. Протидія пропаганді в україні: інформаційна політика та безпекові виклики. *Фінансова політика: теоретичні та практичні аспекти юридичної науки. Тема року: Сучасний міжнародний правопорядок та міжгалузеві правові процеси:* матеріали VIII Міжнар. наук.-практ. конф. (Ірпінь, 2 квіт. 2026 р.). Ірпінь, 2026.

ЗМІСТ

ВСТУП

Обґрунтування вибору теми дослідження. Інформаційна війна стала одним із найнебезпечніших засобів впливу на державу, суспільство та суспільну свідомість, призначення якої не обмежується поширенням неправдивих повідомлень чи пропагандистських тез, а полягає у цілеспрямованому впливі на політичні процеси, підриві довіри до органів державної влади, послабленні суспільної єдності, дестабілізації внутрішньої ситуації, створенні панічних настроїв, спотворенні уявлень про події та нав’язуванні вигідних агресору оцінок.

В умовах збройного конфлікту, для України така проблема має безпосередній характер, оскільки інформаційний тиск супроводжує військову агресію, використовується паралельно з дипломатичними, економічними та кібернетичними засобами впливу і спрямовується на ослаблення державної стійкості. Поряд із традиційними пропагандистськими інструментами дедалі активніше використовуються соціальні мережі, цифрові платформи, анонімні канали поширення відомостей, штучно створені інформаційні приводи, маніпуляції громадською думкою, психологічний тиск і технології масованого впливу на емоційний стан населення. Показово, що за результатами дослідження медіаспоживання українців у 2024 році 73,6% опитаних щоденно отримували новини переважно через соціальні мережі та месенджери, а 78,1% читали новини у Telegram, що свідчить про переміщення основного поля інформаційного протиборства саме у цифровий комунікаційний простір. Водночас 15,2% громадян узагалі не довіряють жодному джерелу інформації, що відображає одну з найнебезпечніших цілей інформаційної війни — руйнування довіри як до медіа, так і до інституцій загалом [215]. Значущість проблеми дезінформації у 2024 році підкреслили 62% аудиторії, однак лише 17% респондентів зазначили, що завжди можуть розпізнати фейк і не піддаватися йому. Одночасно у 2024 році CERT-UA опрацювала 4315 кіберінцидентів, що на 69,8% більше, ніж у 2023 році [219], а це свідчить про

комплексний характер сучасних загроз, у яких інформаційний і кібернетичний компоненти дедалі тісніше взаємодіють.

За таких обставин особливого значення набуває державна стратегія протидії інформаційній війні, зміст якої не може зводитися лише до заборони окремих інформаційних ресурсів, спростування фейків чи ситуативного реагування на ворожі інформаційні кампанії. Ефективна державна стратегія повинна охоплювати узгоджену діяльність органів публічної влади, належне правове регулювання, розвиток стратегічних комунікацій, зміцнення національного інформаційного простору, підвищення рівня медіаграмотності населення, захист інформаційної інфраструктури, а також вироблення механізмів швидкого виявлення й нейтралізації деструктивних інформаційних впливів. Більше того, держава повинна не лише реагувати на вже вчинені інформаційні атаки, а й діяти на випередження, формувати стійкість суспільства до дезінформації, забезпечувати єдність офіційної комунікації та зберігати баланс між потребами безпеки й гарантіями прав людини. Потреба в науковому осмисленні таких питань посилюється тим, що на практиці окремі заходи протидії нерідко залишаються розрізненими, а їх результативність значною мірою залежить від рівня міжвідомчої координації, чіткості правових приписів і послідовності державної інформаційної політики.

Теоретичною основою дослідження стали наукові праці вітчизняних учених, зокрема В. Б. Авер’янова, І. В. Арістової, К. І. Бєлякова, А. І. Берлача, А. М. Благодарного, О. В. Ботвінкіна, С. М. Гусарова, Т. О. Гуржія, О. П. Дзьобаня, Д. В. Дубова, Ю. О. Горбаня, В. П. Горбуліна, С. В. Ківалова, Т. О. Коломоєць, В. К. Колпакова, Л. В. Компанцевої, О. В. Кузьменко, В. А. Ліпкана, О. В. Литвиненка, В. Ф. Пашковського, В. М. Петрика, С. В. Петряєва, Б. В. Потятиника, Г. Г. Почепцова, М. М. Присяжнюка, М. А. Ожевана, В. В. Остроухова, Т. В. Сивак, Г. П. Ситника, Т. В. Ткачука, В. Г. Чорної, М. Я. Швеця, Х. П. Ярмакі та ін. У напрацюваннях таких та інших учених досліджено проблеми інформаційної безпеки держави, інформаційного протиборства, державної інформаційної політики,

стратегічних комунікацій, інформаційно-психологічного впливу, захисту національного інформаційного простору та організаційно-правових засад забезпечення національної безпеки.

Разом із цим, проблема державної стратегії протидії інформаційній війні має міжгалузевий характер, оскільки перебуває на перетині публічного управління, національної безпеки, адміністративного, інформаційного та міжнародного права, а відтак дослідження предмету дослідження потребує з'ясування сутності інформаційної війни як особливого виду деструктивного впливу, визначення ознак і складових державної стратегії у цій сфері, встановлення кола суб'єктів її реалізації, аналізу правових та організаційних засобів протидії, а також окреслення напрямів удосконалення чинного механізму захисту інформаційного простору України. Необхідність такого дослідження посилюється й тим, що в умовах воєнного стану інформаційна сфера стала одним із основних напрямів забезпечення обороноздатності держави, збереження суспільної стійкості та підтримання належного рівня довіри до державних інституцій.

Таким чином, обрана тема дисертації має належне наукове і практичне значення й зумовлена потребою у цілісному осмисленні змісту державної стратегії протидії інформаційній війні, визначенні її основних складових, з'ясуванні наявних проблем правового та організаційного забезпечення, а також виробленні обґрунтованих підходів до вдосконалення державної політики у сфері захисту інформаційного простору України від деструктивного зовнішнього і внутрішнього впливу.

Зв'язок роботи з науковими програмами, планами, темами. Обрана тема даного дослідження ґрунтується на положеннях Цілей сталого розвитку України на період до 2030 року, затверджених Указом Президента України від 30 вересня 2019 р. № 722/2019; Комплексного стратегічного плану реформування органів правопорядку як частини сектору безпеки і оборони України на 2023-2027 роки, схваленого Указом Президента України від 11 травня 2023 р. № 237/2023; Основних наукових напрямів та найважливіших

проблем фундаментальних досліджень у галузі природничих, технічних, суспільних і гуманітарних наук на 2019-2023 рр., затверджених Постановою Президії Національної академії наук України від 30 січня 2019 р. № 30.

Мета і завдання дослідження. *Метою* роботи є наукове обґрунтування теоретичних і практичних засад державної стратегії протидії інформаційній війні та розроблення рекомендацій щодо вдосконалення механізмів її формування, реалізації й координації в системі публічного управління та адміністрування.

– з'ясувати сутність інформаційної війни як складової сучасних загроз інформаційній безпеці держави;

– охарактеризувати сучасні пропагандистські технології як фактор загроз інформаційній безпеці держави;

– розкрити значення державної інформаційної політики як інструменту протидії пропаганді та інформаційній війні;

– узагальнити зарубіжний досвід формування державної стратегії протидії інформаційній війні;

– визначити принципи та стратегічні засади формування державної стратегії протидії інформаційній війні;

– розробити інституційний механізм формування та реалізації державної стратегії протидії інформаційній війні;

– встановити основні проблеми реалізації державної стратегії протидії інформаційній війні в Україні;

– сформулювати концептуальне бачення напрямів удосконалення державної стратегії протидії інформаційній війні.

Об'єкт дослідження – публічне управління інформаційною безпекою України.

Предметом дослідження є – особливості державної стратегії протидії інформаційній війні.

Методи дослідження. Для досягнення мети та виконання завдань дисертаційного дослідження, а також забезпечення об'єктивності й наукової

достовірності одержаних результатів у роботі використано комплекс загальнонаукових і спеціальних методів дослідження. Зокрема, за допомогою *гносеологічного* методу з'ясовано сутність інформаційної війни як складової сучасних загроз інформаційній безпеці держави, визначено її місце у системі деструктивних впливів на інформаційний простір та сформовано теоретичні підходи до розуміння її природи як об'єкта публічно-управлінського впливу (підрозділ 1.1). *Логіко-семантичний* метод, а також метод сходження від абстрактного до конкретного використано для уточнення понятійного апарату дослідження, розкриття змісту основних понять, а також характеристики сучасних пропагандистських технологій як фактора загроз інформаційній безпеці держави (підрозділи 1.1, 1.2). *Аналітичний* метод дав змогу охарактеризувати сучасні пропагандистські технології, виявити їх основні ознаки, форми прояву, механізми впливу на суспільну свідомість та інформаційну безпеку держави, а також розкрити значення державної інформаційної політики як інструменту протидії пропаганді та інформаційній війні (підрозділи 1.2, 1.3). Застосування *системно-структурного* методу сприяло дослідженню принципів і стратегічних засад формування державної стратегії протидії інформаційній війні, а також дозволило розкрити взаємозв'язок між її інституційними, організаційними, функціональними та комунікаційними складовими (підрозділи 2.2, 2.3). *Структурно-функціональний аналіз* надав можливість розробити інституційний механізм формування та реалізації державної стратегії протидії інформаційній війні, визначити місце і роль суб'єктів публічного управління у цій сфері, а також оцінити функціональну спроможність системи забезпечення інформаційної безпеки держави в умовах воєнного стану (підрозділи 2.3, 3.1). *Порівняльний* метод використано з метою узагальнення зарубіжного досвіду формування державної стратегії протидії інформаційній війні, виявлення найбільш ефективних підходів до організації державного реагування на інформаційні загрози та визначення можливостей їх адаптації у вітчизняній практиці публічного управління (підрозділ 2.1). Метод *моделювання* застосовано під

час розроблення інституційного механізму формування та реалізації державної стратегії протидії інформаційній війні, а також у процесі формування концептуального бачення напрямів її удосконалення (підрозділи 2.3, 3.2). *Прогностичний* метод використано для формування концептуального бачення напрямів удосконалення державної стратегії протидії інформаційній війні, визначення перспектив розвитку механізмів публічного управління у цій сфері та обґрунтування необхідності посилення інформаційної стійкості держави і суспільства (підрозділ 3.2). Використання *індуктивного* та *дедуктивного* методів забезпечило узагальнення теоретичних положень, нормативних засад і практичних напрацювань, а також дозволило сформулювати висновки щодо необхідності комплексного вдосконалення державної стратегії протидії інформаційній війні в Україні (розділи 1–3).

Нормативну основу дослідження становлять Конституція України, міжнародні договори, згода на обов'язковість яких надана Верховною Радою України, а також національні нормативно-правові акти законодавчого й підзаконного рівнів, у положеннях яких визначено правові, організаційні та інституційні засади формування і реалізації державної політики у сфері забезпечення інформаційної безпеки, протидії інформаційній війні, діяльності органів сектору безпеки і оборони, а також функціонування системи публічного управління у відповідній сфері. Особливе значення для дослідження мають закони України «Про національну безпеку України», «Про інформацію», «Про захист інформації в інформаційно-комунікаційних системах», «Про державну таємницю», «Про медіа», а також інші нормативно-правові акти, що регламентують діяльність суб'єктів публічного управління у сфері захисту інформаційного простору України.

Науково-теоретичне підґрунтя роботи сформували праці вітчизняних і зарубіжних учених у галузі публічного управління та адміністрування, державного управління, інформаційного й адміністративного права, національної безпеки, стратегічних комунікацій, інформаційної політики та міжнародних відносин. Використання міждисциплінарного наукового

доробку дало змогу комплексно розкрити сутність, зміст, організаційно-управлінські механізми та інституційні особливості державної стратегії протидії інформаційній війні, а також обґрунтувати напрями її вдосконалення в сучасних умовах.

Інформаційну та *емпіричну* основу дослідження становлять матеріали, що характеризують практику діяльності суб'єктів забезпечення інформаційної безпеки України, офіційні аналітичні, статистичні та довідкові джерела, матеріали політико-правової публіцистики, а також узагальнення практики діяльності органів публічної влади у сфері протидії інформаційним загрозам.

Наукова новизна одержаних результатів полягає в тому, що дисертаційне дослідження є одним із перших комплексних досліджень, у якому розроблені напрями формування та реалізації державної стратегії протидії інформаційній війні з урахуванням сучасного стану законодавства, практики публічного управління, умов воєнного стану, цифровізації суспільних комунікацій та зростання деструктивних інформаційних впливів. Сукупність одержаних висновків і рекомендацій має важливе значення для вдосконалення організаційно-управлінських механізмів координації суб'єктів державної політики у відповідній сфері, підвищення результативності стратегічних комунікацій, забезпечення інформаційної стійкості держави та суспільства, а також зміцнення спроможності публічної влади своєчасно виявляти, попереджати й нейтралізувати загрози інформаційного характеру, зокрема:

вперше:

– розроблено структурно-функціональну модель формування та реалізації державної стратегії протидії інформаційній війні, яка, на відміну від існуючих, інтегрує три взаємопов'язані рівні: інституційний (суб'єктна вертикаль), функціонально-процесуальний (алгоритми моніторингу та нейтралізації) та організаційно-управлінський (цикл прийняття та коригування рішень), що забезпечує цілісність державного реагування на гібридні загрози (Рис. 1);

– обґрунтовано концептуальні засади оновленої державної інформаційної політики України через розробку авторського проєкту Концепції, де вперше в межах публічного управління запропоновано трирівневу систему суб'єктів (стратегічного, виконавчого та партнерського рівнів) та визначено чіткі індикатори результативності протидії пропаганді в умовах воєнного стану (Рис. 2);

удосконалено:

– теоретико-методологічні засади публічного управління у сфері інформаційної безпеки шляхом синергії модельного та інституційного підходів, що дозволило інтерпретувати державні механізми протидії інформаційній війні як адаптивний, конкретно-історичний процес із власною логікою стадіального розвитку;

– організаційно-управлінський механізм державного реагування на інформаційні загрози в частині регламентації видів реагування залежно від рівня загрози (загальнодержавний, міжвідомчий, відомчий) та впровадження національної рамки комплексних процедур, що поєднує проактивний (попередження) та реактивний (локалізація наслідків) алгоритми адміністрування;

дістало подальший розвиток:

– класифікація сучасних пропагандистських технологій у контексті публічного управління, де акцент зміщено на їхню здатність інтегруватися з кіберзагрозами, що обґрунтовує пріоритетність зміцнення стратегічних комунікацій та медіарезильєнтності як інструментів державної політики;

– праксеологія адаптації зарубіжного досвіду (країн НАТО та ЄС) до вітчизняних реалій, що полягає у переході від механічного копіювання інституцій до імпорту управлінських рішень щодо координації StratCom-центрів та спеціалізованого моніторингу зовнішніх впливів;

– системно-функціональний підхід до ідентифікації проблем реалізації державної стратегії, що дозволило пов'язати вразливість цифрових сервісів держави з ефективністю інформаційного супроводу та рівнем суспільної

довіри до офіційних джерел.

Практичне значення одержаних результатів полягає в тому, що вони становлять як науково-теоретичний, так і прикладний інтерес і можуть бути використані у:

– *науково-дослідній сфері* – як основа для подальшого розроблення теоретичних і практичних засад удосконалення державної стратегії протидії інформаційній війні, механізмів публічного управління у сфері забезпечення інформаційної безпеки, а також міжвідомчої координації суб'єктів реалізації відповідної державної політики;

– *правотворчій діяльності* – у процесі підготовки змін і доповнень до нормативно-правових актів, що регламентують формування та реалізацію державної політики у сфері забезпечення інформаційної безпеки, стратегічних комунікацій, захисту інформаційного простору та протидії деструктивним інформаційним впливам;

– *практичній діяльності органів публічної влади* – для вдосконалення організаційно-управлінських механізмів реалізації державної стратегії протидії інформаційній війні, підвищення ефективності міжвідомчої взаємодії, стратегічного планування, інформаційно-аналітичного забезпечення, а також розроблення й удосконалення відомчих і міжвідомчих документів у сфері захисту інформаційного простору України;

– *освітньому процесі* – під час підготовки підручників, навчальних посібників, курсів лекцій, методичних рекомендацій, практикумів, тестових завдань та інших дидактичних матеріалів із навчальних дисциплін «Публічне управління та адміністрування», «Державна політика у сфері національної безпеки», «Інформаційна безпека», «Стратегічні комунікації», «Державне управління в умовах кризових станів».

Апробація результатів дисертації. Основні положення та результати дисертаційного дослідження оприлюднені, обговорені та отримали позитивну оцінку на міжнародних і всеукраїнських науково-практичних конференціях, форумах та круглих столах упродовж 2020–2026 років, зокрема: «Цілі сталого

розвитку. Україна 2030: публічне управління для сталого розвитку» (м. Київ, 2020 р.); «Практична політологія: тенденції і перспективи» (м. Київ, 2021 р.); «Реформа децентралізації в Україні: здобутки та перспективи» (м. Київ, 2021 р.); «Державна служба України: сучасні виклики та перспективи повоєнної трансформації» (м. Київ, 2022 р.); «Об'єднані наукою: перспективи міждисциплінарних досліджень» (м. Київ, 2022 р.); «Соборність України: Політика духовної спільності, національних традицій і цінностей» (м. Київ, 2023 р.); «Актуальні питання діяльності Національної поліції як суб'єкту протидії організованій злочинності (м. Кропивницький, 2026 р.). «Фінансова політика: теоретичні та практичні аспекти юридичної науки» (м. Ірпінь, 2026.).

Публікації. Основні положення та результати дисертаційного дослідження опубліковано у 8 працях, у тому числі - у 6 статтях, опублікованих у наукових фахових виданнях Україні категорії Б (чотири самостійно та дві у співавторстві); та 2 публікаціях у збірниках матеріалів науково-комунікативних заходів.

Структура та обсяг дисертації. Робота складається зі вступу, трьох розділів, які включають в себе дев'ять підрозділів, висновків, списку використаних джерел (233 найменування, з яких 38 - іншомовних) та додатків. Загальний обсяг дисертації становить 217 сторінок, із яких обсяг основного тексту – 168 сторінок.

РОЗДІЛ 1.
ТЕОРЕТИЧНІ ОСНОВИ ДЕРЖАВНОЇ СТРАТЕГІЇ ПРОТИДІЇ ІНФОРМАЦІЙНІЙ ВІЙНІ

1.1. Інформаційна війна як складова сучасних загроз інформаційній безпеці держави

Поточний стан безпекового середовища переконливо засвідчує, що загрози інформаційній безпеці держави вже не можуть розглядатися як другорядні чи допоміжні порівняно з воєнними, політичними або економічними викликами. Особливо це проявилося в умовах російсько-української війни, гаряча фаза якої розпочалася 24 лютого 2022 року, хоча сама агресія російської федерації проти України має триваліший, системний і багатовимірний характер. Зазначене протиборство відбувається не лише у фізичному просторі, а й у сфері інформаційного впливу, де боротьба точиться за суспільну свідомість, інтерпретацію подій, політичні оцінки, колективні настрої та моделі масової поведінки. У зв’язку з чим, дослідження інформаційних війн набуває особливої актуальності в межах аналізу сучасних загроз інформаційній безпеці держави та розробки стратегії протидії інформаційній війні.

В умовах російсько-української війни питання інформаційної безпеки України істотно актуалізувалося не лише як наукова, а і як прикладна проблема публічного управління. Своєю чергою, це зумовлено тим, що сучасне протиборство дедалі більше виходить за межі класичного військового зіткнення, охоплюючи комунікаційну, психологічну, ідеологічну, цифрову та символічну сфери. За таких умов держава змушена не лише реагувати на вже наявні дезінформаційні кампанії, а й виробляти довгострокові підходи до захисту національного інформаційного простору, запобігання деструктивному впливу на населення, нейтралізації ворожих наративів та підтримання внутрішньої стійкості суспільства. Інформаційна війна у цьому розумінні є

вже не просто супровідним елементом воєнних дій, а самостійною складовою сучасної політики держав, спрямованої на досягнення стратегічних цілей без виключного використання збройної сили.

У науковій літературі поняття інформаційної війни тлумачиться по-різному, однак більшість дослідників сходяться на тому, що її сутність полягає у цілеспрямованому використанні інформації як засобу впливу на свідомість, поведінку, ціннісні орієнтири та політичні уявлення широких соціальних груп. Так, Г. Г. Почепцов визначає інформаційну війну як комунікативну технологію впливу на масову свідомість із короткочасними та довгостроковими цілями. При цьому дослідник окремо виокремлює смислову війну як більш тривалий, менш помітний, але не менш небезпечний різновид впливу, що спрямовується на когнітивний простір [116, с. 24–25]. Такий підхід має важливе методологічне значення, оскільки дозволяє побачити, що сучасне інформаційне протиборство не зводиться до окремих фейків, дезінформаційних вкидів або неправдивих повідомлень. Воно охоплює глибший рівень впливу – боротьбу за способи тлумачення подій, за формування оцінок, установок і моделей суспільного реагування. Саме у цьому аспекті інформаційна війна стає одним із найбільш небезпечних явищ для держави, адже її руйнівний потенціал пов’язаний не з безпосереднім фізичним знищенням об’єктів, а з дестабілізацією внутрішнього середовища, розхитуванням суспільної довіри, підривом моральної стійкості, провокуванням панічних настроїв та ослабленням спроможності держави до консолідованої реакції на зовнішню агресію. За таких умов вплив здійснюється не лише на окрему особу, а на суспільство в цілому, на його здатність відрізняти достовірну інформацію від маніпуляції, критично оцінювати повідомлення, зберігати довіру до інституцій та підтримувати національну єдність.

На прикладі України достатньо чітко простежуються методи гібридної війни, які фактично становлять складові ширшої інформаційної війни. Є. Магда, аналізуючи російську агресію проти України, звертає увагу на низку

методів, що застосовуються російською федерацією починаючи з 2013 року. До них, зокрема, належать перекручування та пересмикування фактів, масоване поширення дезінформації, намагання створити зовнішньополітичну підтримку російських інтересів, а також систематичне заперечення очевидних фактів агресії [85, с. 140]. У сукупності ці дії спрямовані на дестабілізацію ситуації всередині держави, поглиблення внутрішніх суперечностей, створення ліній соціального і політичного розколу, формування негативного міжнародного образу України, а також нав'язування викривленої картини подій міжнародній спільноті.

Інформаційна війна в такому розумінні передбачає не хаотичне поширення неправдивих повідомлень, а системно організовану діяльність, спрямовану на формування вигідної маніпулятору суспільної думки та закріплення у свідомості громадян відповідних установок поведінки. Саме тому її потрібно розглядати як узгоджену діяльність із використання інформації як своєрідної зброї для досягнення політичних, воєнних, психологічних та ідеологічних цілей. За сучасних умов інформаційний простір, що охоплює власне інформацію, мережеву інфраструктуру, цифрові платформи та інформаційні технології, набуває значення стратегічного національного ресурсу, контроль над яким стає одним із ключових чинників національної стійкості. Вагомим підтвердженням цього є використання російською федерацією інформаційних методів для виправдання агресії, дискредитації України та створення псевдологічних конструкцій, покликаних змінити сприйняття війни як усередині самої росії, так і за її межами. Так, у промові до Федеральних зборів рф 21 лютого 2023 року володимир путін фактично використав типові інформаційно-пропагандистські прийоми, стверджуючи, що нібито США та НАТО готували Україну до великої війни, а росія лише «використовує силу, щоб її зупинити» [57]. Такі твердження демонструють класичне застосування дезінформаційних моделей, заснованих на запереченні очевидного, інверсії причин і наслідків, фабрикації загроз та перекладенні відповідальності на жертву агресії.

Унаслідок застосування подібних методів агресор отримує змогу істотно викривлювати суспільне сприйняття дійсності, деморалізувати населення, формувати відчуття невизначеності та знижувати здатність суспільства до критичної оцінки поточних подій. Саме тому всі методи ведення інформаційної війни спрямовані не лише на інформування чи дезінформування, а на цілеспрямоване конструювання реальності у свідомості людей. У такій ситуації суспільство починає сприймати нав'язані оцінки як природні, а фальшиві інтерпретації – як альтернативну, але допустиму версію подій. Звідси і особлива небезпека інформаційної війни як складової загроз інформаційній безпеці держави.

Особливе місце у структурі сучасних інформаційних воєн займають соціальні мережі та цифрові комунікаційні майданчики. Їх роль визначається насамперед високою швидкістю поширення інформації, величезним охопленням аудиторії, ефектом повторюваності, алгоритмічним просуванням контенту та відсутністю належних запобіжників для моментального поширення фейкових або маніпулятивних повідомлень. Досліджуючи місце соціальних мереж у сучасних інформаційних війнах, В. Новородовський слушно зауважує, що використання Facebook як основної інформаційної платформи створювало підґрунтя для конфліктного впливу [101, с. 154]. Ідеться не лише про російсько-українську війну, а й про конфлікти в Грузії, Нагірному Карабасі, Придністров'ї, де соціальні мережі використовувалися як інструмент формування конфліктного порядку денного, поширення ідеологічних меседжів та підтримання штучно сконструйованих смислів.

У випадку України російські пропагандистські структури активно використовували соціальні мережі «вконтакте» та «одноклассники», які впродовж тривалого часу були популярними серед українських користувачів. Через спеціально створені чи підтримувані спільноти, групи та інформаційні майданчики поширювалися меседжі, спрямовані на дезорганізацію, дезорієнтацію та внутрішнє розхитування українського суспільства. Наслідком таких впливів стало, зокрема, поширення ідей «русского мира», що,

як зазначає В. Новородовський, сприяло маргіналізації окремих прошарків суспільства та створювало передумови для розгортання сепаратистських рухів [101, с. 156]. Отже, цифрове (віртуальне) середовище стало не просто каналом поширення інформації, а повноцінним полем інформаційного протиборства, де агресор послідовно формував ґрунт для майбутніх політичних і безпекових криз.

Водночас слід наголосити, що використання інформації та дезінформації як зброї є одним із базових елементів сучасної політики кремлівського режиму щодо просування власних цінностей, міфів та ідеологічних конструктів. Завдяки цьому досягається панування у публічному просторі, витіснення альтернативних інтерпретацій та формування атмосфери страху, приниження, невпевненості й безвиході. У науковій літературі справедливо підкреслюється, що більшість інформаційних кампаній, атак та хвиль поширення повідомлень, які реалізуються російськими пропагандистськими центрами у вітчизняному інформаційному просторі, мають на меті саме створення атмосфери тотального страху, непевності, приниження та відчаю [84, с. 43]. Це свідчить, що кінцевою ціллю інформаційної війни є не тільки підміна фактів, а й руйнування психологічної стійкості суспільства.

Найбільш уразливою сферою застосування інформаційної зброї виступає людська свідомість. Саме вплив на свідомість дає змогу формувати нестійке сприйняття світу, підвищену тривожність, розгубленість, втрату орієнтирів та ослаблення критичного мислення. У цьому контексті інформаційна зброя постає як новий і специфічний вид зброї, небезпека якої полягає у прихованому характері дії, масштабності застосування та здатності завдавати значної шкоди без фізичного знищення людей чи матеріальних об’єктів. У наукових працях слушно наголошується, що інформаційна зброя є засобом ведення інформаційної війни, яка, своєю чергою, становить ключовий елемент ширшого повномасштабного протиборства [145, с. 52]. Недооцінка її можливостей може призвести до фатальних помилок у воєнно-політичній

боротьбі, оскільки шкода, заподіяна свідомості, системі цінностей та суспільній єдності, здатна мати довготривалі наслідки.

Про визначальну роль інтернет-майданчиків і соціальних мереж у сучасних інформаційних війнах говорить також О. Саган. На її думку, в умовах інформаційної агресії саме знаково-символічна сфера особистості, в якій ключову роль відіграють мова, символічна культура та система цінностей, зазнає особливо інтенсивного впливу. Унаслідок цього формується так звана «мозаїчна свідомість», для якої характерною є втрата людиною здатності критично мислити, адекватно оцінювати реальність, відрізняти достовірне від маніпулятивного та протидіяти мові ворожнечі [152, с. 9]. Такий стан створює сприятливі умови для екстремістського впливу, радикалізації та використання осіб у деструктивних комунікаційних кампаніях. У зв'язку з цим соціальні мережі повинні розглядатися не лише як інструменти цифрової взаємодії, а як повноцінні середовища реалізації ворожих інформаційних стратегій.

Окрему увагу в науковому аналізі привертає питання сутнісних ознак інформаційної війни. О. Марунченко в дисертаційному дослідженні підкреслює, що попри різні підходи до визначення цього поняття, його основною ознакою є гостра, агресивна взаємодія протиборчих сторін в інформаційній сфері, яка негативно відбивається на стані політичних комунікацій у суспільстві загалом [86, с. 56]. Через високу інтенсивність такої взаємодії інформаційні війни складно піддаються управлінню та свідомому регулюванню. Це означає, що держава має діяти на випередження, а не обмежуватися реагуванням лише на окремі прояви дезінформації після того, як вони вже спричинили негативні наслідки.

Зміст сучасної інформаційної війни тісно пов'язаний не лише з поширенням інформації, а й із конструюванням симулятивної реальності, у межах якої засоби масової інформації перестають відображати події такими, якими вони є, а починають самі творити образи, міфи та симулякри, які у сприйнятті аудиторії набувають більшої переконливості, ніж фактична дійсність. Тому небезпека сучасної інформаційної війни полягає також у

здатності витісняти реальність її штучно сконструйованими версіями. За допомогою телебачення, цифрових платформ, відеохостингів, а також текстового й візуального контенту відбувається боротьба не лише за факт, а й за сам спосіб бачення подій. Цей підхід дозволяє агресору нав'язувати власну інтерпретаційну модель світу, в якій агресія маскується під «захист», окупація під «визволення», а насильство – під «історичну справедливість».

У цьому контексті особливо вагомим є підхід О. Курбана, який розглядає сучасні інформаційні війни як протистояння ідей, образів, ідеологій і міфів. У межах такого підходу дослідник вводить поняття «бойові наративи», головною ознакою яких є їх деструктивне спрямування. Ці наративи функціонують як базові смислові конструкції, що поділяються на тематичні субнаративи та транслюються через різні види контенту – тексти, відео, фото, меми, інфографіку тощо [80, с. 151]. Така концепція дозволяє зрозуміти, що сучасна інформаційна війна реалізується не лише через окремі повідомлення, а через системи взаємопов'язаних сенсів, які послідовно вбудовуються в інформаційне поле.

Показовим є моніторинг українського інформаційного простору, який здійснював Центр протидії інформаційним агресіям «AM&PM» при Військовому інституті Київського національного університету імені Тараса Шевченка. Відповідно до аналітичних звітів Центру, російська федерація систематично атакувала Україну через низку супернаративів, серед яких були, зокрема, теми збиття українського літака в Ірані, «плівок Гончарука», «руки Сороса», американських біолабораторій, війни на сході України, взаємин України і НАТО, а також нібито переслідування російськомовних [80, с. 151]. Усі ці наративи були спрямовані на створення довготривалого смислового тиску, підрив довіри до українських інституцій та підтримання образу України як «неспроможної» чи «штучної» держави.

Глибшим і довготривалішим за своїм змістом виявився і супернаратив ностальгії за СРСР, який російська пропаганда послідовно відтворювала в різних формах протягом тривалого часу. Для його просування

використовувалися гуманітарні технології у вигляді медіавірусів, меметичних засобів, фейків, дезінформації та пропаганди. Такий підхід дає підстави стверджувати, що сучасні інформаційні війни нерідко спираються не лише на оперативні дезінформаційні кампанії, а й на історично та культурно вкорінені смислові конструкти, які роками готують ґрунт для подальшої політичної агресії.

У зв'язку з цим особливого значення набуває питання нормативного та публічно-правового осмислення інформаційної війни як явища. У вітчизняному офіційному дискурсі визначення «інформаційна війна» з'явилося ще у 2012 році в Указі Президента України «Про Стратегічний оборонний бюлетень України», де її було визначено як форму протиборства між суб'єктами, що передбачає інформаційний вплив на населення з використанням засобів масової інформації, комп'ютерних мереж та інших каналів із метою формування відповідної суспільної думки, підриву морального духу суспільства та окремих його інституцій [163]. Хоча зазначений указ згодом втратив чинність, сама поява такого поняття в офіційних документах засвідчувала поступове усвідомлення державою небезпеки інформаційного протиборства.

Чинний Стратегічний оборонний бюлетень України, затверджений Указом Президента України від 17 вересня 2021 року № 473/2021, уже не використовує безпосередньо термін «інформаційна війна», однак апелює до суміжних понять – ведення протиборства в інформаційному просторі та кіберпросторі, кібероборотьби, кіберзброї [164]. Таке оновлення термінології не означає, що явище втратило актуальність. Навпаки, воно свідчить про розширення уявлень держави про форми сучасного безпекового протиборства та про поступовий перехід до комплекснішого бачення загроз, що поєднують інформаційний, кібернетичний, психологічний та управлінський вплив.

Окрему роль у системі правового забезпечення інформаційної безпеки України відіграють Закон України «Про основні засади забезпечення кібербезпеки України», Стратегія національної безпеки України, Стратегія

кібербезпеки України та, насамперед, Стратегія інформаційної безпеки України, затверджена Указом Президента України від 28 грудня 2021 року № 685/2021. Саме цей документ нині виступає ключовим у сфері нормативного визначення підходів до протидії деструктивним інформаційним впливам. У ньому інформаційна безпека визначається як складова національної безпеки України, тобто як стан захищеності державного суверенітету, територіальної цілісності, демократичного конституційного ладу, інших життєво важливих інтересів людини, суспільства і держави, за якого забезпечуються права на доступ до достовірної та об'єктивної інформації, а також існує ефективна система протидії негативним інформаційним впливам, деструктивній пропаганді, скоординованому поширенню недостовірної інформації та іншим інформаційним операціям [137].

Запровадження цієї Стратегії водночас означало втрату чинності Доктриною інформаційної безпеки України 2016 року. Остання, як слушно відзначалося у науковому та експертному середовищі, мала занадто декларативний характер і не забезпечувала достатньої визначеності щодо механізмів взаємодії між владою, засобами масової інформації та суспільством. Крім того, окремі її положення не містили належної конкретизації, що ускладнювало їх практичну реалізацію [44]. У зв'язку з чим, перехід до Стратегії інформаційної безпеки 2021 року став важливим кроком у бік більш системного нормативного оформлення державної політики у сфері протидії сучасним загрозам інформаційній безпеці.

Серед глобальних і національних загроз Стратегія інформаційної безпеки України прямо виокремлює інформаційну політику російської федерації як загрозу не лише для України, а й для інших демократичних держав, а також звертає увагу на вплив соціальних мереж як самостійних суб'єктів у сучасному інформаційному просторі та на недостатній рівень медіаграмотності населення [137]. Такий підхід цілком відповідає сучасним умовам, коли інформаційні війни ведуться не лише державами, а й через

наднаціональні цифрові платформи, мережеві спільноти, анонімізовані канали комунікації та алгоритмічні системи поширення контенту.

На основі визначених глобальних і національних загроз у Стратегії окреслено сім стратегічних цілей, які безпосередньо пов'язані з протидією інформаційним війнам. Ідеться, зокрема, про протидію дезінформації та інформаційним операціям держави-агресора, забезпечення розвитку української культури й громадянської ідентичності, підвищення рівня медіакультури та медіаграмотності суспільства, гарантування прав особи на доступ до достовірної інформації, інформаційну реінтеграцію громадян з тимчасово окупованих територій, створення ефективної системи стратегічних комунікацій та розвиток інформаційного суспільства [137]. Отже, уже на рівні стратегічного планування держава визнає, що інформаційні війни є системною загрозою, подолання якої потребує не одного інструменту, а цілого комплексу взаємопов'язаних заходів.

Разом із тим на практиці реалізація таких стратегічних цілей стикається з низкою труднощів. Зокрема, Кабінетом Міністрів України тривалий час не було затверджено повноцінного плану заходів з реалізації Стратегії інформаційної безпеки на період до 2025 року, а відповідний документ певний час існував лише у формі проєкту [44]. Така ситуація свідчила про недостатню завершеність організаційного забезпечення реалізації задекларованих положень. Унаслідок цього окремі важливі напрями державної політики у сфері протидії інформаційним загрозам функціонували не як частина внутрішньо узгодженої системи, а як фрагментарні рішення, пов'язані переважно з негайним реагуванням на поточні виклики.

Попри це окремі заходи, передбачені в межах державної політики у сфері інформаційної безпеки, мають істотне практичне значення. До них належать, зокрема, проєкт «Spravdi», спрямований на протидію дезінформаційним кампаніям і деструктивній пропаганді, фахова підготовка спеціалістів із раннього виявлення та прогнозування гібридних загроз, а також реалізація національного проєкту з медіаграмотності «Фільтр» [44]. Їх

прикладна цінність підтверджується і результатами проведеного нами опитування державних службовців, працівників органів місцевого самоврядування та фахівців у сфері стратегічних комунікацій, серед яких 43% респондентів вказали, що найбільш результативним напрямом зниження вразливості населення до пропагандистського впливу є саме підвищення рівня медіаграмотності, 26% опитаних пов'язали ефективність державної протидії дезінформації з розвитком спеціалізованих платформ спростування неправдивих повідомлень, а ще 13% наголосили на необхідності системної підготовки кадрів, здатних своєчасно виявляти й оцінювати гібридні інформаційні загрози.

Таким чином, сучасна протидія інформаційним війнам не може обмежуватися лише заборонами або реагуванням на окремі фейки, а повинна охоплювати також освітній, аналітичний та комунікаційний виміри.

У структурі протидії інформаційним війнам особливого значення набуває й державна політика пам'яті. В сучасній Україні, особливо у період 2014–2023 років, вона була суттєво переорієнтована та фактично стала важливим напрямом реагування на російські інформаційні атаки. Це пояснюється тим, що політика пам'яті безпосередньо пов'язана з історичною ідентичністю, національними символами, колективними уявленнями про державу та її минуле. Саме в цій сфері російська пропаганда традиційно намагалася нав'язати власні фальсифіковані інтерпретації історії, применшити самостійність українського державотворення та зруйнувати українську політичну суб'єктність. У зв'язку з цим формування цілісної історичної пам'яті має не лише культурне, а й безпекове значення. Дослідники справедливо зазначають, що формування монолітної історичної пам'яті як наслідок реалізації державної політики пам'яті здатне убезпечити націю від культурного, світоглядного та політичного розшарування, а також посилити доцентрові настрої в суспільстві [32, с. 20]. Тому в умовах російсько-української війни політика пам'яті повинна розглядатися як складова системи протидії інформаційним війнам, а не як окремий гуманітарний напрям. Через

неї держава здатна нейтралізувати історичні фейки і підтримувати суспільну стійкість до довготривалого ідеологічного впливу.

Практичним підтвердженням цього є повноваження Українського інституту національної пам'яті, який бере участь у науковому супроводженні реалізації Стратегії інформаційної безпеки, у тому числі в частині реагування на інформаційні впливи держави-агресора, забезпечує функціонування та наповнення Віртуального музею російської агресії, а також сприяє залученню істориків, політологів і філософів до підготовки спеціальних інформаційних продуктів, зокрема з метою розвінчування російських історичних фейків [44]. Результати проведеного нами опитування респондентів (пересічних громадян) додатково засвідчили значущість цього напряму: 68,4% опитаних вказали, що поширення історичних фальсифікацій і маніпуляцій щодо минулого України є одним із найнебезпечніших різновидів інформаційного впливу, 61,7% респондентів пов'язали послаблення національної стійкості саме з викривленням історичної пам'яті, а 73,2% опитаних підтримали необхідність активнішого використання державою науково обґрунтованих інформаційних продуктів для спростування російських історичних наративів. На нашу думку, це ще раз підтверджує, що сучасна інформаційна війна охоплює не лише поточні новини чи медіавкиди, а й боротьбу за історичну пам'ять, символи та колективну ідентичність.

Центральне місце серед інституційних механізмів протидії інформаційним загрозам посідає Центр протидії дезінформації при Раді національної безпеки і оборони України, створений відповідно до рішення РНБО від 11 березня 2021 року, введеного в дію Указом Президента України від 19 березня 2021 року № 106. На цей орган покладено завдання щодо аналізу та моніторингу подій в інформаційному просторі, виявлення і прогнозування інформаційних загроз, участі у розбудові системи стратегічних комунікацій, створення інтегрованої системи оцінки інформаційних загроз, розроблення методології виявлення матеріалів маніпулятивного та дезінформаційного характеру, а також сприяння взаємодії держави й

громадянського суспільства у сфері протидії дезінформації [98]. Так, поступово формується інституційний механізм, що дозволяє переводити протидію інформаційним війнам із площини реактивних дій у площину системного управління. Водночас створення навіть найкращих державних механізмів не забезпечить належної ефективності без розвитку в суспільстві критичного сприйняття інформації та належного рівня медіаграмотності. За відсутності цих якостей будь-які державні заходи можуть виявитися недостатніми, адже ворожий вплив значною мірою спирається саме на готовність аудиторії емоційно реагувати на маніпулятивний контент, не перевіряючи джерел і не аналізуючи достовірність повідомлень. Тому в системі протидії інформаційним війнам важливу роль мають відігравати не лише державні інституції, а й недержавні ініціативи, здатні забезпечувати перевірку фактів, спростування фейків та поширення практик критичного мислення.

Прикладом такої ініціативи є проєкт StopFake, заснований у 2014 році Могилянською школою журналістики. Його діяльність спрямована не лише на виявлення випадків поширення неправдивої інформації про події в Україні, а й на формування міжнародної дискусії про шляхи протидії сучасній пропаганді. Значення таких проєктів полягає в тому, що вони доповнюють державні механізми реагування, забезпечуючи гнучкіші форми фактчекінгу, публічного спростування та підвищення суспільної стійкості до дезінформації. Зазначене підтверджується і результатами проведеного нами опитування працівників сфери публічного управління, науково-педагогічних працівників та здобувачів вищої освіти, серед яких 74,1% опитаних визнали діяльність незалежних фактчекінгових проєктів важливим елементом протидії пропаганді, 69,3% респондентів зазначили, що саме недержавні ініціативи часто забезпечують більш оперативне спростування неправдивої інформації, а 71,8% опитаних підтримали необхідність посилення взаємодії державних органів із громадськими інформаційно-аналітичними платформами. Тобто, у

ширшому розумінні це свідчить про необхідність поєднання державних і громадських зусиль у сфері захисту інформаційного суверенітету держави.

Отже, в сучасних умовах російсько-української війни інформаційні війни необхідно розглядати як самостійну і системну складову сучасних загроз інформаційній безпеці держави. Їх небезпека виявляється у здатності впливати на суспільну свідомість, підміняти факти маніпулятивними інтерпретаціями, руйнувати довіру до державних інституцій, послаблювати моральну стійкість населення, стимулювати внутрішню дестабілізацію та створювати передумови для підриву національної ідентичності. У зв'язку з цим протидія інформаційним війнам має ґрунтуватися на поєднанні нормативно-правових, організаційних, інституційних, комунікаційних, освітніх і суспільних заходів, спрямованих як на своєчасне виявлення та нейтралізацію деструктивних впливів, так і на довгострокове формування стійкості суспільства до інформаційної агресії.

1.2. Сучасні пропагандистські технології як фактор загроз інформаційній безпеці держави

У сучасних умовах національна безпека охоплює не лише воєнний, політичний чи економічний виміри, а й стан захищеності держави та суспільства в інформаційній сфері. Такий підхід зумовлений тим, що інформаційний простір перетворився на середовище, в якому відбувається не тільки обіг відомостей, а й боротьба за суспільні настрої, політичні орієнтації, довіру до інституцій та здатність держави зберігати внутрішню стійкість. Закон України «Про національну безпеку України» відносить інформаційну безпеку до напрямів державної політики у сферах національної безпеки і оборони, що підтверджує її місце в загальній системі захисту національних інтересів [130].

Інформаційну безпеку доцільно розуміти як стан захищеності інформаційного простору держави, суспільства та особи, за якого

забезпечується стійкість до деструктивних інформаційних впливів, зберігається можливість вільного функціонування національного інформаційного середовища та не допускається заподіяння шкоди національним інтересам через маніпулювання інформацією, нав'язування викривлених смислів або підрив довіри до органів публічної влади [137; 139]. У такому значенні інформаційна безпека виходить далеко за межі технічного захисту каналів зв'язку чи інформаційних ресурсів, оскільки стосується також захисту суспільної свідомості, комунікаційної стабільності та спроможності держави протидіяти зовнішньому й внутрішньому інформаційному тиску.

Загрози національній інформаційній безпеці держави виявляються у поширенні дезінформації, проведенні спеціальних інформаційних операцій, маніпулятивному конструюванні суспільно значущих подій, дискредитації державних інституцій, поляризації громадської думки та створенні атмосфери недовіри, тривоги й соціальної дестабілізації. Стратегія інформаційної безпеки України визначає серед актуальних викликів і загроз деструктивні інформаційні впливи, спрямовані на підрив обороноздатності, послаблення суспільної єдності, зниження рівня довіри до держави та дестабілізацію внутрішньополітичної ситуації [137].

Доктрина інформаційної безпеки України також пов'язує інформаційні загрози з інформаційною експансією, пропагандистським впливом і використанням інформаційної сфери як простору реалізації ворожих інтересів [139]. У структурі таких загроз особливе місце посідає пропаганда як цілеспрямований інформаційно-психологічний вплив, спрямований на формування наперед заданих оцінок, моделей сприйняття, поведінкових орієнтацій та політичних реакцій. У цифровому середовищі пропаганда поєднує медійні, технологічні, психологічні та комунікаційні механізми, що дозволяють не лише транслювати потрібні наративи, а й створювати умови для їх суспільного прийняття, повторення та закріплення. У працях з комунікаційних технологій підкреслюється, що сучасні канали поширення інформації дають змогу цілеспрямовано впливати на сприйняття аудиторії,

змінювати інтерпретацію подій і формувати потрібну інформаційну картину реальності [53, с. 56].

Поряд із цим, сучасний етап розвитку суспільства характеризується стрімкою глобалізацією інформаційних потоків і трансформацією способів комунікації між державою, суспільством та особою. За таких умов інформаційна сфера перетворюється на один із визначальних вимірів національної безпеки, а вплив на масову свідомість дедалі частіше здійснюється не шляхом прямого примусу, а через використання складних інформаційно-психологічних технологій. Особливе місце серед них посідають сучасні методи пропаганди, які активно застосовуються як інструмент політичного, ідеологічного та геостратегічного впливу й водночас становлять реальну загрозу національній інформаційній безпеці держави [2, с. 73].

У цьому контексті, варто додати, що в науковій літературі інформаційна війна розглядається як сукупність скоординованих заходів, спрямованих на досягнення інформаційної переваги над реальним або потенційним противником. За такого підходу пропаганда постає одним із інструментів інформаційного протиборства, здатним забезпечувати вигідні для суб’єкта впливу зміни в громадській думці, політичних оцінках і масовій поведінці. Стратегічні інформаційні війни ведуться із застосуванням специфічних засобів впливу, які не завдають безпосередньої фізичної шкоди, проте здатні спричиняти масштабні соціальні конфлікти, політичну дестабілізацію та загострення безпекової ситуації [17; 49; 62, с. 68].

Метою інформаційної війни, а відтак і сучасних методів пропаганди, є послаблення морального, психологічного та інтелектуального потенціалу супротивника при одночасному зміцненні власних позицій. Такий вплив реалізується через цілеспрямовані пропагандистські кампанії, які апелюють не лише до раціонального мислення, а передусім до емоційної, ідеологічної та ціннісної сфер свідомості людини. Саме з цієї причини інформаційна війна є органічною складовою ідеологічного протиборства, а пропаганда – її основним інструментом.

Подальший аналіз сучасних методів пропаганди потребує звернення до ширшого контексту інформаційної війни, оскільки еволюція пропагандистських практик, їх історичне становлення та трансформація в умовах цифрового середовища дозволяють повніше зрозуміти їх зміст, механізми та небезпеку для національної інформаційної безпеки держави. Насамперед, зазначимо, що на відміну від класичних воєн, інформаційні протистояння не супроводжуються руйнуваннями чи людськими жертвами, що нерідко зумовлює недооцінку їх небезпеки. Водночас наслідки інформаційних і пропагандистських атак для суспільної та індивідуальної свідомості можуть бути співмірними, а в окремих випадках – навіть більш руйнівними, ніж результати збройних конфліктів. Деформація системи цінностей, втрата довіри до державних інститутів, радикалізація суспільних настроїв і розмивання національної ідентичності становлять прямі загрози національній інформаційній безпеці держави [7, с. 134].

Для належного розуміння природи сучасних пропагандистських практик слід коротко звернутися до історії становлення інформаційного протиборства. Передусім слід зазначити, що поняття «інформаційна війна» увійшло до наукового обігу в 1985 році в Китаї, однак сам феномен інформаційного впливу як інструменту боротьби має значно глибші історичні витоки. Теоретичні засади інформаційного протиборства були закладені ще у працях давньокитайського мислителя Сунь Цзи, який одним із перших обґрунтував пріоритет нематеріальних форм впливу над прямим збройним протистоянням. У трактаті «Мистецтво війни» він наголошував, що найвищою формою перемоги є підкорення супротивника без бою, а досягнення стратегічної переваги можливе шляхом систематичного введення противника в оману, маніпулювання його уявленнями та підриву моральної стійкості. Такі положення фактично сформували ідейне підґрунтя сучасних пропагандистських і психологічних методів впливу [62, с. 141].

Особливого розвитку інформаційні війни та пропагандистські методи зазнали у XX столітті з появою і масовим поширенням засобів масової

інформації. Уже в міжвоєнний період радіомовлення активно використовувалося як інструмент впливу на населення інших держав: Сполучені Штати Америки – у країнах Латинської Америки, Велика Британія – у колоніях, Німеччина – серед етнічних німців у сусідніх країнах. У 1930-х роках інформаційні війни поступово трансформувалися з допоміжного елементу збройного протистояння у відносно самостійний інструмент досягнення політичних цілей, що засвідчує, зокрема, приклад німецько-австрійської радіовійни 1933–1934 років [52, с. 8].

Перша світова війна стала важливим етапом становлення системного використання пропаганди як засобу цілеспрямованого впливу на масову свідомість. Саме в цей період було вперше апробовано масштабні технології інформаційного впливу, спрямовані не лише на військових, а й на цивільне населення держав-супротивників. Так, упродовж 1918 року щоденно запускалося до двох тисяч пропагандистських повітряних куль, кожна з яких переносила близько тисячі агітаційних листівок. Лише у жовтні 1918 року на територію Німеччини було скинуто понад п’ять мільйонів таких матеріалів, що свідчить про усвідомлення державами значення інформаційного впливу як складової воєнної стратегії [83, с. 61].

У Великій Британії ще на початку війни було створено спеціалізоване Бюро пропаганди під керівництвом Чарльза Мастермана (1914–1917 рр.), діяльність якого була спрямована на формування потрібних наративів як усередині країни, так і за її межами [61]. Створення такого органу засвідчило перехід від епізодичного використання інформаційного впливу до його інституціоналізації як окремого напряму державної політики в умовах воєнного протистояння. Основним завданням Бюро було забезпечення суспільної підтримки воєнних дій, консолідація населення навколо державних інтересів, формування позитивного образу Великої Британії на міжнародній арені, а також дискредитація противника шляхом цілеспрямованого поширення відповідних інформаційних повідомлень. Важливо, що британська пропагандистська модель уже на цьому етапі поєднувала централізоване

управління змістом інформаційних кампаній із використанням різних каналів комунікації та різних способів донесення повідомлень до цільових аудиторій. Ідеться не лише про публічне поширення офіційних матеріалів, а й про значно тонші форми інформаційного впливу, розраховані на підвищення довіри до отримуваної інформації. Однією з таких інноваційних форм стало використання приватного листування громадян: адреси іноземних кореспондентів збиралися та використовувалися для адресної розсилки пропагандистських матеріалів, що істотно підвищувало рівень довіри до змісту повідомлень, оскільки вони сприймалися не як результат офіційної агітації, а як відносно нейтральна або особистісно опосередкована інформація. Фактично йшлося про один із ранніх прикладів персоналізованого інформаційного впливу, коли ефективність пропаганди забезпечувалася не лише самим змістом повідомлення, а й способом його доставки, комунікативним середовищем та рівнем психологічної готовності адресата до його сприйняття [61, с. 125].

Також одним із прикладів інформаційної експлуатації воєнної події стало використання факту затоплення німецьким підводним човном пасажирського судна «Лузітанія» у 1915 році, внаслідок чого загинуло понад тисячу осіб, зокрема громадяни США [156]. У пропагандистському дискурсі ця подія набула значення не лише трагічного епізоду війни, а й потужного символу ворожої жорстокості, який використовувався для емоційної мобілізації населення, посилення антинімецьких настроїв та формування морально виправданої моделі участі у воєнному конфлікті. При цьому, в Сполучених Штатах Америки важливим кроком до формування системної моделі державної пропаганди стало створення у 1917 році Комітету публічної інформації на чолі з Джорджем Крілем. Його функціонування засвідчило перехід до цілеспрямованого використання інформаційних ресурсів для мобілізації громадської думки, легітимації державної політики та консолідації суспільства в умовах війни. За відсутності розвинених електронних засобів комунікації Комітет спирався на публічні виступи, плакати, кінофільми та

листівки, які Дж. Кріль називав «паперовими кулями». Особливістю американського підходу стало активне залучення рекламних агентств, що свідчило про впровадження у сферу воєнної пропаганди технологій масового переконання, раніше характерних переважно для комерційної комунікації [79].

Друга світова війна ознаменувала новий етап розвитку пропаганди, оскільки саме в цей період масові комунікації почали поєднуватися з науковими підходами до вивчення психології аудиторії, а інформаційний вплив остаточно утвердився як самостійний інструмент досягнення воєнно-політичних цілей. Характерною рисою цього періоду стала жорстка цензура, яка істотно обмежувала свободу діяльності засобів масової інформації та підпорядковувала їх потребам державної політики [79].

Особливе місце в історії інформаційного протиборства посідає нацистська Німеччина, де пропаганда була інституціоналізована як один із базових механізмів функціонування державної влади. Йозеф Геббельс, очоливши Міністерство народної освіти і пропаганди у 1933 році, сформував централізовану та надзвичайно результативну систему інформаційного впливу [17]. Її сутність полягала у повному підпорядкуванні інформаційного простору політичним цілям режиму, монополізації каналів масової комунікації, усуненні альтернативних джерел інформації та цілеспрямованому формуванні у населення ідеологічно зумовленого сприйняття дійсності.

Характерними ознаками нацистської пропаганди стали системність, безперервність, оперативність реагування, емоційна інтенсивність повідомлень, активне використання символічних образів, спрощених гасел і багаторазового повторення ключових наративів. Її вплив поширювався на пресу, радіо, кінематограф, освіту, культуру та сферу масових публічних заходів, що забезпечувало цілісне охоплення суспільної свідомості. Водночас саме у цей період почали активно застосовуватися і наукові методи психологічного впливу на аудиторію. Зокрема, використовувалися методи глибинного інтерв’ю для моделювання світогляду німецького солдата, чим займався Генрі Дікс – один із провідних фахівців із психологічних операцій

того часу [79]. Це свідчило про поступовий перехід від інтуїтивних пропагандистських практик до більш системного використання знань про психологію масової свідомості. У таких умовах пропаганда виконувала не лише функцію політичної мобілізації, а й завдання легітимації режиму, конструювання образу ворога, виправдання агресивної політики та пригнічення критичного мислення. Саме поєднання інформаційного впливу з державною монополією на комунікацію, цензурою та репресивними практиками значною мірою зумовило високу ефективність нацистської пропаганди на внутрішньому фронті [17].

Не менш потужною була і радянська пропагандистська система. Вона охоплювала практично всі сфери суспільного життя – засоби масової інформації, культуру, мистецтво, освіту, масові свята та обряди. Її принципова особливість полягала в тому, що пропаганда функціонувала не як окремий допоміжний інструмент державної політики, а як постійний механізм формування суспільної свідомості, контролю над інтерпретацією подій і підтримання ідеологічної монополії влади. Основною метою радянської пропаганди було формування ідеї неминучої перемоги комунізму, створення негативного образу Заходу та ізоляція так званого «соціалістичного табору» [2, с. 143].

На відміну від багатьох інших історичних моделей інформаційного впливу, радянська пропаганда була тісно пов’язана з повсякденним життям людини, супроводжуючи її фактично на всіх етапах соціалізації – від дошкільного виховання і шкільної освіти до трудових колективів, діяльності партійних і комсомольських організацій, святкових ритуалів та офіційних пам’ятних дат. Ідеологічні смисли систематично відтворювалися через шкільні підручники, політичні плакати, газетні публікації, художню літературу, кінематограф, радіомовлення, монументальне мистецтво та публічні церемонії. У такий спосіб держава не лише транслювала потрібні наративи, а й забезпечувала їх багаторазове повторення, емоційне закріплення та перетворення на елемент колективної ідентичності [2, с. 144].

Показово, що однією з найхарактерніших рис радянської пропаганди було поєднання політичної агітації з елементами сакралізації влади та її символів. У публічному просторі послідовно формувався культ держави, партії та її керівників, а офіційні гасла й образи набували майже ритуального значення. Історично цікаво, що навіть масові святкові демонстрації, військові паради, урочисті зібрання та оформлення міського простору виконували не лише представницьку, а й виразну пропагандистську функцію: вони створювали враження політичної єдності, всенародної підтримки режиму та історичної неминучості обраного державного курсу. Саме через таку ритуалізацію публічного життя пропаганда ставала не лише джерелом інформаційного впливу, а й способом організації соціальної реальності [2, с. 145].

Під час Другої світової війни Радянський Союз активно використовував візуальні засоби впливу, кінохроніку, художні фільми, а також апеляцію до історичних і релігійних символів для підтримання патріотичних настроїв. При цьому особливістю радянської моделі було те, що навіть за збереження комуністичної ідеологічної основи вона вміло адаптувала пропагандистські меседжі до потреб воєнного часу: поряд із класовими та політичними мотивами активно актуалізувалися образи Батьківщини, героїзму, жертовності, історичної пам’яті та боротьби із зовнішнім ворогом [2, с. 146].

У той самий час у Великій Британії, як вже було зазначено, значну роль відігравала візуальна комунікація: плакати використовувалися для боротьби з чутками, стимулювання економії ресурсів, а також заохочення жінок до роботи на промислових підприємствах. Випускалися також художні й документальні фільми, в яких головними героями ставали звичайні громадяни, що сприяло формуванню ефекту ідентифікації та підвищенню довіри до поширюваних повідомлень. У Сполучених Штатах у 1942 році було створено Управління військової інформації, яке виконувало функції роз’яснення цілей війни, формування позитивного образу союзників та підвищення бойового духу як на фронті, так і в тилу. Цей досвід засвідчив, що пропаганда може

використовуватися не лише як інструмент дезінформації, а і як важливий засіб мобілізації суспільства.

На нашу думку, сформульовані у ХХ столітті принципи пропаганди (централізоване управління інформаційними потоками, емоційна насиченість повідомлень, використання гасел, маніпулювання істинністю інформації та залучення максимально привабливих каналів комунікації), фактично стали підґрунтям для подальшого розвитку пропагандистських технологій [55, с. 132–138]. Тобто, історичний досвід цього періоду створив основу для трансформації традиційних форм пропаганди у сучасні цифрові практики інформаційного впливу.

Якщо класична пропаганда базувалася переважно на централізованих каналах комунікації, зокрема друкованих засобах масової інформації та радіо, то нині вона функціонує в умовах децентралізованого інформаційного простору, у якому основну роль відіграють соціальні мережі, месенджери, онлайн-платформи та алгоритмічні системи поширення контенту [35]. За таких умов пропагандистський вплив не лише не втрачає своєї результативності, а, навпаки, набуває нових форм, стає більш гнучким, прихованим і технологічно адаптованим до особливостей конкретної аудиторії.

Ґрунтуючись на сучасних наукових публікаціях, можна констатувати, що методи інформаційної боротьби у науковій доктрині умовно поділяються на три основні групи: силові, інтелектуальні та комбіновані [60; 185]. Така класифікація має не лише теоретичне, а й прикладне значення, оскільки дає змогу системно оцінити характер і масштаби інформаційних загроз, виявити домінуючі способи впливу на інформаційне середовище держави, а також визначити диференційовані напрями протидії з боку уповноважених суб’єктів. Її евристична цінність полягає в тому, що вона дозволяє розмежовувати ситуації, у яких пріоритетним є технічний захист інформаційної інфраструктури, від тих, де основну небезпеку становить маніпулятивний вплив на свідомість, поведінку та процеси прийняття рішень.

До силових методів належать способи інформаційного впливу, що передбачають фізичне або технічне ураження об’єктів інформаційної інфраструктури за допомогою різних видів озброєння, спеціальних технічних засобів, засобів радіоелектронної боротьби, кібервтручання або інших деструктивних інструментів [54]. Їх застосування спрямоване на досягнення інформаційної переваги шляхом обмеження доступу до інформації, порушення функціонування каналів зв’язку, виведення з ладу систем управління, спотворення даних або блокування критично важливих інформаційних ресурсів. У сучасних умовах такі способи не зводяться лише до прямого фізичного знищення носіїв або засобів зв’язку, а охоплюють і технічні форми втручання, здатні паралізувати комунікацію, послабити координацію органів влади та істотно вплинути на здатність держави реалізовувати військові, політичні й управлінські рішення. Показовим для України є те, що, за даними аналітичного звіту Держспецзв’язку, у 2024 році однією з найбільш резонансних кібератак стала атака на державні реєстри Міністерства юстиції України, а в попередній період одним із наймасштабніших проявів технічного впливу стала атака на телекомунікаційну інфраструктуру, пов’язана з інцидентом «Київстар» [229]. Такі випадки засвідчують, що ураження інформаційних систем в українських реаліях не є гіпотетичною загрозою, а виступає практичним інструментом дестабілізації державного управління та суспільних комунікацій.

Інтелектуальні методи інформаційної боротьби характеризуються передусім впливом на свідомість, мислення, мотивацію та поведінкові установки противника [16, с. 87–89]. Їх основним елементом є так зване рефлексивне управління, яке полягає у нав’язуванні певних моделей сприйняття реальності, інтерпретації подій і прийняття рішень шляхом подання спеціально сконструйованої інформації, здатної спонукати об’єкт впливу до бажаної для ініціатора поведінки. У сучасних дослідженнях рефлексивне управління розглядається як цілеспрямований вплив на процес ухвалення рішень з урахуванням психологічних характеристик особи або

групи, а в ширшому безпековому контексті – як інструмент когнітивного домінування та маніпуляції вибором супротивника [220]. Саме ці методи дають змогу досягати інформаційної переваги не за рахунок кількості поширеної інформації, а за рахунок її змісту, адресності, якості та здатності формувати потрібні смисли, оцінки й реакції. Їх особлива небезпека полягає в тому, що вони можуть діяти приховано, тривало і без очевидних ознак зовнішнього втручання, поступово трансформуючи суспільні настрої, політичні орієнтації та моделі громадської поведінки.

В нинішніх умовах це особливо яскраво простежується на прикладі систематичного поширення фейків про нібито «масову мобілізацію жінок», «зниження мобілізаційного віку», «злочини ТЦК», «мародерство військових» або «катастрофічний стан Збройних Сил України», які спрямовані не стільки на інформування, скільки на деморалізацію населення, підрив довіри до державних інституцій та створення атмосфери внутрішньої напруги [182; 184; 187]. Невипадково, за даними опитування КМІС, 71% українців вважають поширення російської дезінформації та пропаганди в соціальних мережах серйозною загрозою, причому 33% відносять її до числа найбільших загроз [115].

Комбіновані методи поєднують у собі елементи як силового, так і інтелектуального впливу та спрямовані на одночасне досягнення переваги як за кількісними, так і за якісними характеристиками інформації [60, с. 105]. У сучасних умовах комбіновані методи є найбільш поширеними та найбільш небезпечними, оскільки дають змогу синхронізувати інформаційні, психологічні, кібернетичні, політичні й комунікаційні інструменти впливу в межах єдиної операційної логіки. На практиці це означає, що технічне втручання в інформаційні системи може супроводжуватися одночасним запуском дезінформаційних кампаній, поширенням панічних або поляризуючих наративів, дискредитацією органів державної влади, підривом довіри до офіційних повідомлень та нав’язуванням суспільству викривлених пояснювальних моделей подій. Така синхронізація різних способів впливу

значно ускладнює виявлення джерела загрози, підвищує латентність ворожих інформаційних операцій і суттєво знижує ефективність суто секторальних заходів реагування.

Вищезазначене можна простежити в Україні, коли кібератаки або технічні збої паралельно супроводжуються хвилею маніпулятивних повідомлень у Telegram, Facebook, TikTok та інших цифрових середовищах щодо «колапсу системи», «приховування правди владою», «зради союзників» чи «неминучості поразки» [193; 229]. При цьому безпекові підходи НАТО окремо наголошують, що когнітивний вимір боротьби орієнтований на вплив на раціональність, сприйняття, емоції та поведінку, а отже поєднання технічного і психологічного тиску створює максимально небезпечний формат гібридного впливу. В сучасних безпекових доктринах країн-альянсу та України тому і наголошується на необхідності комплексного підходу до протидії інформаційним загрозам, який має охоплювати як захист інформаційної інфраструктури, так і зміцнення когнітивної стійкості суспільства, розвиток стратегічних комунікацій, протидію дезінформації та належну міжвідомчу координацію [137; 220].

У цьому контексті доцільно також звернути увагу на те, що запропонована класифікація не є суто умовною, відірваною від практики, а відображає реальні механізми розгортання сучасного інформаційного протиборства. Якщо силові методи переважно орієнтовані на руйнування або дестабілізацію технічної основи інформаційного середовища, інтелектуальні – на зміну когнітивних схем і моделей ухвалення рішень, то комбіновані методи фактично інтегрують обидва ці виміри в єдиний сценарій впливу [62, с. 58].

Також, залежно від спрямованості інформаційного впливу інформаційна боротьба може набувати наступального або оборонного характеру. Наступальна інформаційна боротьба має на меті завоювання та утримання інформаційної переваги над противником, дезорганізацію його систем управління, підрив довіри до державних інституцій і формування сприятливих умов для реалізації власних політичних чи військових цілей. Оборонна ж

інформаційна боротьба здійснюється в умовах домінування інформаційної переваги противника та спрямована на її нейтралізацію, мінімізацію завданої шкоди й відновлення контролю над національним інформаційним простором [49].

Необхідно наголосити на тому, що значна частина сучасних збройних конфліктів фактично розпочинається саме з інформаційної фази. При цьому інформаційна війна розглядається у двох взаємопов'язаних площинах – гуманітарній і технічній. У гуманітарному вимірі інформаційна війна полягає у цілеспрямованій трансформації інформаційного простору шляхом нав'язування певної системи цінностей, світоглядних моделей і поведінкових установок. Ідеться не лише про маніпулювання інформаційними потоками, а й про вплив на самі процеси мислення, ідентичності та соціальної самоорганізації.

В умовах становлення інформаційного суспільства життєві стандарти, соціальні орієнтири та моделі поведінки дедалі меншою мірою визначаються об'єктивною реальністю і дедалі більшою мірою формуються через інформаційні технології, символи та знаки – так звані «позначки-технології». Основним об'єктом їх впливу є масова свідомість, яка стає основним полем протиборства у сучасних інформаційних війнах [88].

Перемога в інформаційній війні досягається тією стороною, яка здатна найбільш повно змоделювати поведінку противника, передбачити можливі сценарії його дій, сформувати власний алгоритм реагування та ефективно реалізувати його на практиці. Саме тому в сучасних умовах ключове значення має не лише обсяг інформації, а насамперед здатність керувати її інтерпретацією, емоційним сприйняттям і подальшими поведінковими наслідками.

Особливого значення в сучасних умовах набуває віртуальна пропаганда, що здійснюється через мережу Інтернет. Життя сучасної людини нерозривно пов'язане з цифровим середовищем, що перетворює інтернет-простір на потужний канал маніпулятивного впливу. За результатами опитування,

проведеного для Київським міжнародним інститутом соціології, 73% українців за останні сім днів отримували інформацію із соціальних мереж, що свідчить про винятково високу схильність суспільства до цифрових каналів поширення повідомлень [161]. Водночас інше дослідження засвідчило, що 64% аудиторії наголошували на значущості проблеми дезінформації, однак лише 18% респондентів вказали, що здатні завжди розпізнавати фейки й ігнорувати їх [202].

Віртуальна пропаганда являє собою масштабну діяльність із популяризації та поширення ідей у масовій свідомості, спрямовану на формування громадської думки, моделювання соціальної реальності та витіснення альтернативних інтерпретацій подій. Завдяки таким властивостям Інтернету, як інтерактивність, швидкість поширення інформації та можливість адресного впливу на конкретні соціальні групи, часовий проміжок між інформаційним повідомленням і очікуваним поведінковим результатом істотно скорочується. Слід додати, що особливо небезпечними в українських реаліях стали діпфейки та інші форми ШІ-маніпуляцій. Одним із перших резонансних прикладів був фейковий відеозапис із нібито «зверненням» Президента України про складання зброї, а в подальшому російська пропаганда почала активно використовувати ШІ-фейки від імені українських військових, представників ТЦК та державних органів [191; 195]. Такі технології створюють додаткові ризики, оскільки імітують візуальну достовірність і підвищують переконливість неправдивого контенту [81].

У зв’язку з чим, у сучасному мережевому просторі формується цілісний механізм пропагандистської діяльності, який доцільно розглядати як сукупність трьох взаємопов’язаних аспектів: проєктивного, тиражувального та поведінкового. Такий підхід дозволяє розкрити пропаганду не лише як процес поширення певних повідомлень, а як багаторівневий механізм конструювання, легітимації та практичного закріплення потрібних смислів у масовій свідомості. Його аналітична цінність полягає в тому, що він дає змогу простежити повний цикл впливу, зокрема, від первинного продукування

домінуючої ідеї до її трансформації у суспільно прийнятну, повторювану і зовні добровільну модель поведінки [43]. У такому разі цифрова пропаганда постає не як сукупність розрізнених інформаційних вкидів, а як системно організований процес управління сприйняттям, оцінками та реакціями аудиторії.

Перший, проєктивний, аспект полягає у формуванні домінуючої ідеї, її смисловому оформленні та подальшій легітимації через суб'єктів, які мають довіру цільової аудиторії. Йдеться про те, що в умовах цифрового середовища первинний пропагандистський імпульс рідко подається безпосередньо як відверто нав'язувана позиція. Значно частіше він маскується під експертну оцінку, особисту думку, аналітичний коментар або емоційно переконливе пояснення подій. У цьому контексті особливого значення набуває роль лідерів думок, інфлюенсерів, популярних блогерів, адміністраторів спільнот та інших медійних посередників, через яких відбувається не просто передача інформації, а передача впливу. Відповідний механізм у науковій літературі пов'язується з двоступеневою моделлю комунікації, згідно з якою повідомлення спершу сприймається лідерами думок, а вже через них – ширшою аудиторією [19, с. 144–145; 53, с. 26–27].

Другий, тиражувальний, аспект охоплює масове поширення сформованої ідеї через цифрові платформи, соціальні мережі, месенджери, відеосервіси, онлайн-медіа та алгоритмічні системи рекомендацій. Якщо на попередньому етапі головне значення має смислова конструкція та авторитет джерела, то на цьому етапі визначальною стає швидкість, повторюваність, візуальна привабливість і технічна масштабованість поширення контенту. У цифровому середовищі пропагандистське повідомлення набуває переваги не лише через свій зміст, а й завдяки архітектурі платформи, яка стимулює репости, коментування, лайки, вірусність і повторне включення повідомлення в нові комунікаційні ланцюги. В сучасних дослідженнях наголошується на тому, що в соціальних медіа контент поширюється через мережі користувачів, де саме залученість аудиторії є центральним елементом розповсюдження

пропаганди [102, с. 89]. Тому тиражувальний аспект не варто зводити лише до технічного дублювання повідомлення: він охоплює також алгоритмічне підсилення певних наративів, повторення однакових тез у різних форматах, імітацію масової підтримки, використання ботів, тролів, псевдоакаунтів і прихованих мережевих кампаній для створення враження суспільного консенсусу [147, с. 190]

Третій, поведінковий, аспект виявляється у практичній реалізації нав'язаних сенсів, коли штучно сформована віртуальна реальність поступово набуває ознак суспільної думки, а згодом починає впливати на конкретні рішення, соціальні реакції та колективні форми поведінки. На цьому етапі пропаганда перестає бути лише сферою інформаційного впливу і переходить у площину соціальної дії. Тобто, це означає, що засвоєні в мережевому середовищі наративи починають визначати політичні оцінки, електоральний вибір, ставлення до державних інституцій, готовність до протестної або мобілізаційної активності, рівень суспільної тривожності, а також сприйняття зовнішнього чи внутрішнього ворога. Її наслідком можуть бути зміни поведінки членів спільноти, ослаблення соціальної згуртованості та порушення внутрішніх регулятивних процесів у державі [147, с. 191]. Таким чином, поведінковий аспект є завершальним етапом пропагандистського циклу, на якому інформаційно сконструйоване уявлення про реальність починає функціонувати як підстава для реальних індивідуальних і колективних дій.

Важливо, що між цими трьома аспектами існує не лінійний, а циклічний зв'язок. Успішна поведінкова реалізація нав'язаних сенсів, своєю чергою, стає підставою для подальшого зміцнення первинної ідеї, оскільки вже сам факт її зовнішнього прийняття частиною аудиторії може використовуватися як доказ її «правдивості», «природності» або «суспільної підтримки». У результаті проєктивний, тиражувальний і поведінковий аспекти постійно взаємно підсилюють один одного. До речі, саме в цьому і полягає одна з основних відмінностей сучасної цифрової пропаганди від традиційних форм агітації:

вона не лише поширює повідомлення, а й створює середовище, у якому користувачі самі стають співучасниками його відтворення, нормалізації та соціального закріплення.

Таким чином, методи пропаганди, що застосовувалися раніше, зберігають актуальність і нині, однак у зв’язку з розвитком інформаційних технологій вони істотно модернізувалися, адаптувалися до сучасних умов і набули здатності впливати на масову свідомість навіть за наявності альтернативних джерел інформації та формально вільного доступу до них. У цьому й полягає феномен сучасних методів пропаганди: що вищим є рівень розвитку суспільства та інформаційних технологій, то більш різноманітними, гнучкими й технологічно вдосконаленими стають засоби інформаційного впливу.

Отже, сучасні методи пропаганди не лише зберігають спадковість із традиційними формами інформаційного впливу, а й зазнають суттєвої трансформації під впливом цифровізації, розвитку соціальних мереж, алгоритмічних систем поширення контенту та нових комунікаційних платформ. Їх особливістю є здатність діяти приховано, адаптивно та персоналізовано, використовуючи когнітивні, емоційні й поведінкові механізми впливу, що дозволяє ефективно маніпулювати суспільною свідомістю навіть в умовах формального плюралізму інформаційних джерел і свободи доступу до інформації. Феномен сучасної пропаганди полягає в тому, що зростання рівня інформаційної відкритості суспільства не зменшує її вплив, а, навпаки, створює сприятливе середовище для поширення дезінформації, викривлених наративів і цілеспрямованих інформаційно-психологічних операцій. У зв’язку з цим сучасні методи пропаганди слід розглядати не як суто комунікаційне явище, а як один із визначальних чинників загроз національній інформаційній безпеці держави. Зазначене зумовлює необхідність формування та реалізації комплексної державної стратегії протидії інформаційній війні, яка поєднувала б правові, організаційні, технологічні та освітні інструменти, спрямовані на своєчасне

виявлення пропагандистських впливів, нейтралізацію їх наслідків і підвищення стійкості суспільства до маніпулятивних інформаційних практик.

1.3. Державна інформаційна політика як інструмент протидії пропаганді та інформаційній війні

У загальнотеоретичному розумінні політику розглядають як особливу сферу суспільної діяльності, пов'язану з управлінням державою і суспільством, узгодженням інтересів, виробленням обов'язкових рішень та впливом на основні напрями суспільного розвитку [23, с. 12]. Водночас у сучасній науці дедалі частіше наголошується на необхідності відмежування політики як politics від політики як policy. Як слушно зазначає В. Тертичка, у першому значенні йдеться про сферу взаємовідносин соціальних груп та індивідів щодо влади, тоді як у другому – про план, курс дій або напрям діяльності, що приймається і реалізується владою, політичною партією чи іншим уповноваженим суб'єктом [175, с. 5]. Для цілей дослідження інформаційної політики продуктивним є саме другий підхід, оскільки він дає змогу розглядати її як цілеспрямований і системно організований напрям державної діяльності.

З огляду на це інформаційну політику доцільно аналізувати не лише як сукупність окремих рішень у сфері обігу інформації, а як відносно самостійний напрям державного впливу на інформаційну сферу. О. Токар пропонує виходити з того, що політика загалом є сукупністю намірів і засобів їх здійснення, які формує суб'єкт управління щодо певної сфери життєдіяльності суспільства; відповідно щодо інформаційної політики її об'єктом є національна інформаційна сфера з усіма її компонентами [176, с. 132]. Такий підхід видається методологічно виправданим, оскільки дозволяє поєднати цільову, інституційну та функціональну характеристики відповідного явища. При цьому за наведеним узагальненням зазначеного науковця одні дослідники тлумачать її у вузькому значенні як сукупність

напрямів і способів діяльності держави щодо одержання, використання, поширення та зберігання інформації; інші – у широкому значенні, як багатокомпонентне явище, що охоплює організацію функціонування всієї інформаційної сфери, взаємодію держави, суспільства і засобів масової комунікації, а також питання інформаційної безпеки [176, с. 132–133]. На наш погляд, широкий підхід сьогодні має більшу евристичну цінність, оскільки інформаційні процеси вже давно вийшли за межі суто технічного обігу відомостей і безпосередньо впливають на політичну стабільність, суспільну довіру, стан правопорядку та національну безпеку [56, с. 127–131].

Вартують уваги й підходи, узагальнені Т. Савосько на підставі праць українських учених. Дослідниця звертає на позицію В. Дзюндзюка, який визначає інформаційну політику як особливу сферу життєдіяльності людей, пов’язану з відтворенням і поширенням інформації, що задовольняє інтереси соціальних груп та суспільних інститутів, і наголошує на міждисциплінарному характері цього явища [151, с. 30]. Окрім того, у межах сучасної наукової думки виокремлюють владний, психологічний і цільовий підходи до визначення державної інформаційної політики, що свідчить про складність її змісту та неможливість зведення цього поняття лише до діяльності держави у сфері засобів масової інформації [151, с. 31].

Важливе значення має і те, що в сучасних дослідженнях інформаційна політика дедалі тісніше пов’язується з проблематикою інформаційної безпеки. У науковому середовищі обґрунтовується думка, що вона не може обмежуватися лише регулюванням інформаційних потоків або гарантуванням доступу до інформації. Її зміст охоплює також створення умов для захисту інформаційного простору держави, забезпечення стійкості суспільства до деструктивних комунікативних впливів, формування належного рівня інформаційної культури та критичного сприйняття повідомлень [151, с. 30–311; 76, с. 133]. Тому інформаційна політика у сучасній державі повинна розглядатися одночасно як напрям публічного управління, інструмент

забезпечення інформаційного суверенітету та засіб протидії маніпулятивним інформаційним практикам.

У такому контексті протидія пропаганді постає одним із сегментів державної інформаційної політики. Звернемо увагу на те, що сучасний етап розвитку української держави супроводжується істотним зростанням значення інформаційного простору як середовища реалізації національних інтересів і водночас як сфери виникнення системних загроз для інформаційної безпеки. За нинішніх умов інформація вже не виконує лише комунікативну чи пізнавальну функцію, а дедалі більше використовується як засіб політичного, ідеологічного, психологічного та організаційного впливу на суспільство. Небезпека полягає й у тому, що такий вплив часто маскується під журналістську діяльність, аналітичні оцінки, експертні коментарі або альтернативну точку зору, що ускладнює його своєчасне виявлення та належну правову оцінку [151, с. 31; 176, с. 133].

Практика останніх років переконливо засвідчує, що окремі медіа та цифрові комунікаційні майданчики можуть використовуватися як інструменти поширення дезінформації, політично заангажованих інтерпретацій і відверто маніпулятивних наративів. Наслідком такого впливу стає не лише викривлення суспільної думки, а й ускладнення реалізації завдань публічного управління, зниження рівня довіри до рішень органів державної влади, послаблення внутрішньої єдності суспільства та створення додаткових ризиків для обороноздатності держави. У зв’язку з цим, вкотре зазначимо, що державна реакція на пропагандистські впливи має розглядатися як складова послідовної політики захисту національного інформаційного простору.

Нагадаємо, що початок формування системного підходу до протидії інформаційним загрозам в Україні пов’язується з подіями після 2014 року, коли проблема інформаційної безпеки набула особливої гостроти у зв’язку з агресивним зовнішнім інформаційним впливом, активним використанням дезінформації та спробами дестабілізації внутрішньополітичної ситуації. Одним із перших кроків у цьому напрямі стало Рішення Ради національної

безпеки і оборони України «Про заходи щодо вдосконалення формування та реалізації державної політики у сфері інформаційної безпеки України», введене в дію Указом Президента України від 1 травня 2014 року № 449/2014. У зазначеному рішенні було зафіксовано необхідність розроблення комплексу організаційних і правових заходів, спрямованих на вдосконалення нормативно-правового забезпечення та запобігання реальним і потенційним загрозам національній безпеці в інформаційній сфері [127].

Зміст цього рішення дає підстави стверджувати, що вже на початковому етапі загострення безпекової ситуації держава усвідомила не локальний, а системний характер інформаційних загроз. Ідеться не лише про наявність окремих випадків дезінформації чи ворожої агітації, а про потребу у виробленні узгодженої державної політики, здатної поєднати правові, організаційні, інституційні та комунікаційні засоби протидії. У документі було визначено завдання щодо підвищення ефективності діяльності органів державної влади у сфері захисту інформаційного простору, удосконалення міжвідомчої взаємодії, посилення нормативного регулювання, а також створення дієвих механізмів реагування на дезінформаційні кампанії та пропагандистські впливи. Окремого значення набув курс на приведення національного законодавства у відповідність до актуальних викликів інформаційної сфери та підходів, вироблених міжнародною практикою [181].

Поряд із цим уже на стадії реалізації положень зазначеного рішення виявилися й суттєві проблеми. Насамперед ішлося про відсутність цілісного концептуального бачення державної інформаційної політики, яке б визначало її засадничі орієнтири, довгострокові пріоритети, принципи реалізації та критерії результативності. Передбачені заходи мали переважно загальний характер і не завжди супроводжувалися конкретними механізмами виконання, чітким розподілом повноважень між уповноваженими суб’єктами, належним ресурсним забезпеченням та зрозумілими показниками оцінки ефективності. Через це практичне втілення окремих положень виявилося нерівномірним, а

сама державна реакція на інформаційні загрози в окремих випадках мала радше реактивний, ніж послідовний і випереджальний характер.

Крім того, початковий етап інституційного оформлення державної політики у сфері інформаційної безпеки продемонстрував, що ефективна протидія пропаганді не може обмежуватися лише правовими заборонами або точковими управлінськими рішеннями. Належного результату можна досягти лише за умови поєднання нормативного регулювання із діяльністю у сфері стратегічних комунікацій, офіційного інформування, розвитку медіаграмотності, підтримання суспільної довіри до державних інституцій та налагодження постійної координації між органами влади. За відсутності такої узгодженості навіть формально правильні рішення не завжди забезпечують потрібний рівень захисту інформаційного простору.

Отже, ухвалення Рішення РНБО України у 2014 році стало важливим етапом у становленні державної реакції на інформаційні загрози та засвідчило перехід до більш впорядкованого підходу у сфері захисту інформаційної безпеки. Водночас зазначений акт виявив і низку концептуальних та організаційних прогалин, що зумовили потребу у подальшому розвитку стратегічного підходу до формування та реалізації загальнодержавної інформаційної політики.

Значущим складником державної реакції на інформаційні загрози стали також рішення Національної ради України з питань телебачення і радіомовлення, а також судові акти, якими було обмежено ретрансляцію окремих російських телеканалів, у змісті яких виявлялися заклики до агресивних дій проти України, посягання на її суверенітет і територіальну цілісність, а також матеріали з ознаками системного пропагандистського впливу [122]. Практичне значення таких заходів зумовлюється тим, що телерадіомовлення тривалий час залишалося одним із найбільш потужних каналів масового інформаційного впливу, здатним забезпечувати швидке охоплення значної аудиторії та закріплення потрібних інформаційних настанов у суспільній свідомості. Унаслідок цього поширення через

телемовлення деструктивного контенту створювало реальні ризики для стабільності суспільних настроїв, рівня довіри до державних інституцій та стану внутрішньої консолідації суспільства.

З адміністративно-правового погляду рішення Національної ради у зазначеній сфері слід розглядати як одну з форм реалізації державного регулювання в галузі телерадіомовлення, що здійснюється через нагляд за дотриманням вимог законодавства суб'єктами медіасфери, ухвалення регуляторних актів, застосування передбачених законом засобів реагування та забезпечення виконання встановлених обмежень провайдерами програмної послуги. Правовий статус Національної ради як спеціального конституційного регулятора у сфері телебачення і радіомовлення зумовлює її повноваження щодо здійснення моніторингу програмного продукту, фіксації порушень, аналізу змісту поширюваних матеріалів і прийняття рішень про необхідність припинення чи обмеження ретрансляції. У практичному вимірі така діяльність охоплювала виявлення у змісті програм ознак виправдання агресії, посягання на територіальну цілісність України, розпалювання національної, політичної чи соціальної ворожнечі, а також поширення маніпулятивних повідомлень, зміст яких був спрямований на викривлення реальної картини подій та нав'язування ворожих інтерпретацій [89].

Важливо враховувати, що відповідні обмежувальні заходи у переважній більшості випадків не належать до сфери кримінально-правового реагування, а функціонують у площині адміністративно-правових інструментів захисту інформаційного простору. Їх призначення полягає не у покаранні суб'єкта за вчинене порушення як самоцілі, а у припиненні подальшого поширення інформаційного продукту, здатного завдати шкоди публічним інтересам, та у зменшенні ризиків для національної безпеки. Отже, ідеться про реалізацію превентивно-обмежувальної функції держави у сфері медіарегулювання, що має спиратися на принципи законності, належного обґрунтування, співмірності втручання та його фактичної необхідності за конкретних умов [104]. У цьому аспекті адміністративно-правове реагування на пропаганду

постає не як виняткова дія, а як різновид державного захисту суспільно значущих інтересів у сфері інформаційної безпеки.

Окремого значення набуває судовий контроль за такими рішеннями. Судові акти, якими перевірялася правомірність дій уповноважених суб'єктів, мають подвійне значення. З одного боку, вони забезпечують дотримання процесуальних гарантій, оскільки перевіряють компетенцію органу, належність доказової бази, повноту мотивування рішення, дотримання встановленої законом процедури та меж дискреційних повноважень [110]. З іншого боку, судовий контроль створює правові передумови для дотримання балансу між публічним інтересом у захисті інформаційної безпеки та гарантіями свободи вираження поглядів і права на доступ до інформації. За відсутності такого балансу будь-які обмежувальні заходи ризикують бути сприйнятими як надмірне втручання держави у сферу медіа. Судова практика у зазначеній площині виконує функцію правової легітимації обмежень лише за умови, що вони мають законну мету, спираються на належні підстави та відповідають критерію необхідності у демократичному суспільстві.

Поряд із позитивним значенням відповідних рішень практика їх застосування виявила й низку проблем. Насамперед слід зважати на те, що телерадіомовлення вже не є єдиним або навіть основним каналом поширення пропагандистського впливу. Цифрові платформи, соціальні мережі, месенджери, відеохостинги та стримінгові сервіси істотно розширили можливості дистрибуції деструктивного контенту, причому нерідко поза межами національної юрисдикції або з використанням механізмів, які ускладнюють оперативне регуляторне реагування [100]. За таких умов обмеження ретрансляції окремих телеканалів хоча й зберігає значення, однак не здатне самостійно забезпечити належний рівень протидії сучасній пропаганді. Крім того, будь-які заборонні рішення в цій сфері потребують особливо ретельного обґрунтування, оскільки недостатня визначеність критеріїв, за якими контент визнається пропагандистським, створює ризики

неоднакового правозастосування і може викликати сумніви щодо правомірності втручання.

Належна результативність таких заходів залежить також від узгодженості дій між регулятором, провайдерами програмної послуги, судовими інституціями, правоохоронними органами та іншими суб'єктами сектору безпеки і оборони [51]. За відсутності належної координації навіть обґрунтовані рішення можуть втрачати ефективність або реалізовуватися із запізненням, коли деструктивний інформаційний вплив уже набув значного поширення. У зв'язку з цим адміністративно-правові засоби протидії пропаганді потребують інституційної узгодженості, єдності критеріїв оцінювання контенту та належного процедурного супроводу.

У підсумку рішення Національної ради України з питань телебачення і радіомовлення та відповідні судові акти доцільно оцінювати як важливий адміністративно-правовий інструмент реагування держави на інформаційні загрози, що має превентивно-обмежувальне спрямування та орієнтований на захист публічних інтересів. Разом із тим їх застосування виявило потребу у ширшому підході, за якого регуляторні механізми не функціонують відокремлено, а інтегруються у загальну систему державної інформаційної політики. Ідеться про необхідність поєднання точкових обмежувальних рішень із програмними та концептуальними засадами державної діяльності у сфері протидії пропаганді, включаючи визначення принципів, інституційних повноважень, стандартів прозорості медіавласності, процедур координації та гарантій редакційної незалежності.

Подальшим кроком у напрямі правового забезпечення захисту інформаційного простору стало прийняття Закону України «Про внесення змін до деяких законів України щодо захисту інформаційного телерадіопростору України», яким було встановлено заборону трансляції аудіовізуальних творів, вироблених суб'єктами держави-агресора після 1 січня 2014 року [118]. У системі заходів протидії пропаганді зазначений нормативно-правовий акт мав превентивний характер і був орієнтований на недопущення поширення

контенту, здатного містити виправдання агресивних дій, викривлене висвітлення суспільно-політичних процесів або інші смислові конструкції, що негативно впливають на національні інтереси України.

З адміністративно-правового погляду встановлена заборона є формою спеціального регуляторного обмеження у сфері телерадіомовлення, що реалізується через діяльність уповноважених органів у галузі медіа та кінематографії, а також через процедури контролю за програмною політикою мовників. Законодавець використав відносно чіткі часові та суб'єктні критерії застосування заборони, що дало змогу відмежувати дозволений контент від такого, який розглядався як потенційно небезпечний для публічних інтересів і національної безпеки. У цьому можна вбачати прагнення забезпечити правову визначеність регуляторного впливу та уникнути надмірно широкого тлумачення підстав для обмеження поширення інформаційного продукту.

Водночас аналіз практики застосування цього Закону засвідчує, що його ефективність у площині комплексної протидії пропаганді є відносною. Передусім обмеження орієнтовані головно на традиційні канали телерадіомовлення і не охоплюють значну частину сучасних способів поширення аудіовізуального контенту, зокрема інтернет-платформи, соціальні мережі, відеохостинги та цифрові сервіси на замовлення. Унаслідок цього контент, обмежений у телерадіоефірі, міг залишатися доступним для широкої аудиторії в інших сегментах інформаційного простору [87]. За сучасних умов така прогалина має принципове значення, оскільки пропагандистський вплив дедалі частіше реалізується не через класичне мовлення, а через розгалужені цифрові канали, де національні механізми контролю є менш дієвими.

Крім того, вибірковий характер відповідних законодавчих обмежень не забезпечує повного нейтралізування пропагандистського впливу, оскільки значна частина сучасного інформаційного тиску реалізується у завуальованій формі, без прямої вказівки на країну походження контенту або через транснаціональні медіасередовища, які складно піддаються однозначній ідентифікації. У таких випадках формальний критерій походження

аудіовізуального продукту не завжди збігається з його фактичним змістом, смисловим навантаженням та реальною здатністю впливати на інформаційну безпеку держави. З огляду на це ефективність правового реагування не може визначатися лише країною виробництва контенту, а потребує врахування його смислового спрямування, способів поширення та фактичних наслідків для суспільної свідомості.

Ще одна проблема полягає в тому, що реалізація заборонних заходів без належного концептуального підґрунтя нерідко призводить до фрагментарності державної інформаційної політики. Окремі нормативні рішення, навіть будучи виправданими в конкретний момент, не завжди інтегруються у цілісну систему довгострокових державних орієнтирів, що ускладнює координацію між уповноваженими суб’єктами, знижує передбачуваність правозастосування та не забезпечує стійкого ефекту у сфері протидії пропаганді [45]. За таких умов правове регулювання набуває реактивного характеру, коли держава відповідає на вже наявні виклики, але не формує упереджувальних механізмів їх нейтралізації.

Отже, Закон України «Про внесення змін до деяких законів України щодо захисту інформаційного телерадіопростору України» слід оцінювати як важливий, але обмежений за своїм регуляторним потенціалом інструмент державної реакції на інформаційні загрози. Його ухвалення підтвердило готовність держави застосовувати правові механізми захисту інформаційного простору, однак водночас виявило необхідність переходу від окремих заборонних рішень до вироблення цілісної загальнодержавної інформаційної політики.

Подальший розвиток державної політики у сфері протидії інформаційним загрозам пов’язаний із початком повномасштабної збройної агресії рф проти України у 2022 році, що спричинило істотне розширення змісту, форм і засобів забезпечення інформаційної безпеки. За нових безпекових обставин інформаційна сфера остаточно набула значення одного з базових напрямів захисту національних інтересів, оскільки інформаційні

атаки, дезінформація та інші форми ворожого інформаційного впливу безпосередньо позначаються на стані національної безпеки, суспільній стабільності та спроможності держави протидіяти зовнішній агресії [69, с. 141–142; 73, с. 127; 149, с. 172]. Через інформаційну сферу здійснювався потужний інформаційно-психологічний тиск, спрямований на дестабілізацію держави, підрив її суверенітету, послаблення довіри до державних інституцій та деформацію суспільного сприйняття подій війни. Поширення дезінформації, фейкових повідомлень, маніпулятивних інтерпретацій воєнних подій, а також навмисне нагнітання панічних настроїв поставили перед державою завдання не лише оперативного реагування на окремі інформаційні інциденти, а й вироблення більш жорсткого, скоординованого та функціонально узгодженого підходу до захисту національного інформаційного простору [25, с. 305–309; 69, с. 142].

У період 2022–2023 років відбулося посилення координації між суб’єктами сектору безпеки і оборони, органами виконавчої влади, правоохоронними структурами, регуляторами у сфері медіа, а також іншими інституціями, діяльність яких була пов’язана із виявленням, оцінкою та нейтралізацією інформаційних загроз. Така координація була обумовлена тим, що в умовах повномасштабної війни стратегічні комунікації набули значення одного з ключових інструментів забезпечення національної безпеки, а слабка міжвідомча взаємодія істотно знижувала ефективність реагування на інформаційні виклики [72, с. 22–23]. Поряд із цим у науковій літературі обґрунтовано, що в умовах воєнного стану комунікативна стратегія держави повинна спиратися на узгоджені, достовірні та емоційно збалансовані повідомлення, оскільки саме забезпечення довіри до офіційної інформації, запобігання паніці та підтримка морального духу населення стають її першочерговими завданнями. Таке посилення координації мало не декларативний, а прикладний характер, оскільки в умовах війни будь-яке запізнення у спростуванні дезінформації, неналежна узгодженість офіційних повідомлень або відсутність єдиного підходу до кризової комунікації могли

безпосередньо впливати на стан громадського порядку, рівень довіри до влади та готовність населення до виконання заходів правового режиму воєнного стану [25, с. 305–315]. Показово, що навіть у практиці медіарегулятора протидія дезінформації та інформаційній агресії рф реалізовувалася через постійний моніторинг пропагандистського контенту, обмін інформацією з Центром протидії дезінформації при РНБО України, підготовку аналітичних матеріалів щодо наративів російської пропаганди та їх подальше використання для інформування партнерів і стримування деструктивного інформаційного впливу [48, с. 131–132]. У зв'язку з цим адміністративно-правові засоби забезпечення інформаційної безпеки почали застосовуватися в більш тісному зв'язку з оборонними, управлінськими та комунікаційними потребами держави [73, с. 127].

Поряд із цим після 2022 року активізувалася діяльність Національної ради України з питань телебачення і радіомовлення щодо моніторингу контенту, виявлення ознак поширення дезінформації та координації дій з провайдерами медіапослуг. Розширено практику застосування регуляторних заходів реагування, спрямованих на припинення трансляції матеріалів, що містять ознаки виправдання збройної агресії, посягання на територіальну цілісність України або маніпулятивного впливу на суспільну свідомість в умовах воєнного стану. Зазначені обмеження не мали характеру довільного звуження інформаційних прав, а були обумовлені необхідністю недопущення використання відкритих даних противником у воєнних цілях. В адміністративно-правовому вимірі вони виступали як тимчасові, правомірно встановлені та функціонально виправдані обмеження, спрямовані на охорону публічних інтересів у сфері оборони та безпеки [104].

Водночас, суттєвого значення набула і централізація офіційних комунікацій. В умовах широкомасштабної війни множинність неузгоджених повідомлень від різних органів влади, посадових осіб чи коментаторів могла породжувати інформаційний хаос, суперечливе сприйняття подій і втрату довіри до державної позиції. Саме з огляду на це було посилено значення

єдиних підходів до офіційного інформування населення, погодженості публічних повідомлень і концентрації базових комунікаційних потоків навколо визначених державою джерел. Такий підхід мав на меті не лише забезпечення громадян перевіреною інформацією, а й запобігання використанню інформаційної невизначеності як інструменту ворожого впливу [93, с. 447–449].

Важливим складником державної інформаційної політики стало також запровадження механізмів єдиної державної комунікації у сфері телемовлення, спрямованих на забезпечення безперервного інформування населення в умовах воєнного стану та нейтралізацію дезінформаційного впливу. У правовому й організаційному сенсі такі заходи мали адміністративно-правовий характер, оскільки реалізовувалися через відповідні управлінські рішення, координацію діяльності мовників, визначення порядку інформаційної взаємодії та встановлення особливостей функціонування телемарафону як форми консолідованого поширення суспільно важливої інформації. Основне призначення цього інструменту полягало у тому, щоб забезпечити стабільний доступ населення до перевірених відомостей, зменшити вплив панічних повідомлень, чуток і ворожих фейків, а також підтримати суспільну стійкість в умовах надзвичайно інтенсивного психологічного тиску [6, с. 139].

Наукове осмислення таких заходів дає підстави стверджувати, що в умовах війни державна інформаційна політика неминуче набуває більш концентрованого і функціонально підпорядкованого безпековим цілям характеру. У працях, присвячених проблемам інформаційної безпеки та стратегічних комунікацій, підкреслюється, що під час збройного конфлікту ефективність державної комунікації визначається не лише швидкістю поширення офіційної інформації, а й її узгодженістю, достовірністю, регулярністю та здатністю запобігати ворожим інформаційним вкидам. За таких умов публічна комунікація держави виконує не лише інформативну, а й стабілізаційну, організаційну та захисну функції. Через неї забезпечується

підтримання належного рівня довіри до органів влади, формування зрозумілих орієнтирів суспільної поведінки та збереження внутрішньої керованості в умовах воєнної загрози [82, с. 181–184].

Разом із тим застосування механізмів єдиної державної комунікації не позбавлене дискусійності. У науковій літературі та експертному середовищі порушується питання про межі допустимого втручання держави у медіасферу, співвідношення інтересів безпеки і свободи слова, а також про ризики надмірної концентрації інформаційних потоків. Вказані застереження мають принципове значення, оскільки навіть за умов воєнного стану діяльність держави у сфері інформаційної політики не може бути виведена за межі конституційних орієнтирів, принципу пропорційності та вимоги тимчасового характеру обмежувальних заходів. У цьому аспекті особливої ваги набуває не лише саме рішення про централізацію комунікації, а й належне правове обґрунтування його запровадження, визначеність процедур реалізації, відкритість мотивів та наявність зрозумілих критеріїв припинення таких режимів після усунення надзвичайних обставин [93, с. 449–450].

Отже, після початку повномасштабної збройної агресії рф проти України державна політика у сфері протидії інформаційним загрозам набула значно більш інтенсивного, скоординованого та безпеково орієнтованого характеру. Запровадження в умовах воєнного стану спеціальних режимів функціонування інформаційного простору, встановлення обмежень на поширення відомостей, здатних зашкодити оборонним інтересам держави, а також посилення ролі офіційних комунікацій засвідчили прагнення держави адаптувати адміністративно-правові засоби до нових умов широкомасштабної війни. За таких обставин інформаційна політика вже не могла обмежуватися лише загальними напрямами розвитку інформаційної сфери, а мала забезпечувати оперативне реагування на дезінформаційні кампанії, нейтралізацію пропагандистських впливів, підтримання довіри до органів державної влади та збереження внутрішньої стійкості суспільства. Поряд із цим значна частина рішень у зазначеній сфері ухвалювалася під впливом

конкретних обставин і була спрямована насамперед на негайне усунення поточних загроз. Такий підхід був об’єктивно зумовлений динамікою воєнних подій, однак він одночасно продемонстрував і певні межі державного реагування. За відсутності повною мірою сформованої довгострокової стратегії окремі правові та організаційні заходи нерідко функціонували як самостійні рішення, недостатньо пов’язані між собою спільною логікою, єдиними критеріями оцінювання результативності та прогнозуванням подальших наслідків. Унаслідок цього державні заходи у сфері протидії пропаганді не завжди утворювали внутрішньо узгоджену систему, здатну забезпечити не лише реагування на вже наявні інформаційні загрози, а й їх упередження. Окремої уваги потребує й те, що низка ініціатив у цій сфері не отримала належного законодавчого закріплення або зберегла переважно програмний чи декларативний характер. За таких умов навіть суспільно виправдані та практично необхідні рішення не завжди мають достатньо стійке нормативне підґрунтя, що негативно позначається на їх послідовній реалізації, правовій визначеності та інституційній стабільності. Через це ефективність державної інформаційної політики знижується не лише внаслідок зовнішнього інформаційного тиску, а й у зв’язку з внутрішніми організаційно-правовими недоліками, які перешкоджають формуванню цілісного механізму протидії.

Аналіз сучасного стану державної інформаційної політики дає підстави виокремити чимало проблем, що потребують системного вирішення. До них належать неузгодженість і розпорошеність норм інформаційного законодавства, недостатня міжнародна інформаційна присутність України, технічна застарілість частини державного телерадіомовного сектору, незадовільний стан мережі проводового радіомовлення, а також обмеженість державних програм розвитку інформаційного суспільства. Сукупність зазначених чинників істотно послаблює можливості держави у сфері захисту національного інформаційного простору, ускладнює оперативне донесення офіційної позиції до внутрішньої та зовнішньої аудиторії, а також знижує

здатність своєчасно й результативно протидіяти пропагандистським впливам [39].

Не менш важливим є і питання стану самих засобів масової інформації, оскільки саме вони посідають провідне місце у формуванні суспільної свідомості, поширенні суспільно значущої інформації та забезпеченні демократичних засад функціонування держави. У науковій літературі обґрунтовується, що журналістика і медіа в демократичному суспільстві покликані не лише інформувати, а й забезпечувати публічну сферу, виступати майданчиком для обміну думками, сприяти контролю за діяльністю влади та підтримувати суспільний діалог [15, с. 40–42; 94, с. 12–14]. Рівень незалежності медіа, прозорість їхньої діяльності, редакційна самостійність та відсутність прихованого політичного чи економічного впливу безпосередньо пов’язані із якістю публічного інформаційного середовища, оскільки саме за таких умов медіа здатні виконувати своє демократичне призначення без деформації змісту суспільно значущої інформації [177, с. 305–307].

У демократичній державі засоби масової інформації мають виконувати не лише інформативну, а й контрольну, просвітницьку та суспільно-орієнтуючу функції. У сучасних дослідженнях наголошується, що медіа виступають посередником між владою і суспільством, забезпечують зворотний зв’язок, сприяють підзвітності органів публічної влади, а в умовах гібридних загроз і війни також виконують важливу безпекову функцію [94, с. 12–13]. Водночас збереження їхньої суспільної ролі безпосередньо залежить від реального захисту редакційної незалежності від політичних та економічних впливів, а також від наявності належних гарантій плюралізму думок.

За наявності ж фінансової залежності редакцій, надмірної концентрації медіавласності або впливу окремих політичних і бізнесових груп виникають передумови для викривлення інформаційного порядку денного, нав’язування суспільству вигідних інтерпретацій та прихованого маніпулятивного впливу. У наукових працях підкреслюється, що концентрація медіавласності,

залежність від політичних та економічних інтересів, а також недостатня інституційна стійкість професійних стандартів істотно знижують об’єктивність і неупередженість медіа. Крім того, у правничих дослідженнях слушно акцентується, що одним із пріоритетних завдань розвитку плюралістичного медіапростору є запровадження обґрунтованих обмежень щодо концентрації медіавласності, паралельно із захистом редакційної автономії та підтримкою некомерційних інформаційних платформ [177, с. 305–306].

У цьому контексті відсутність належних і результативних механізмів контролю за концентрацією медіавласності, джерелами фінансування медіа та реальним впливом власників на редакційну політику створює додаткові ризики для інформаційної безпеки держави. Ідеться не лише про можливість прямого поширення пропагандистських матеріалів, а й про більш складні форми викривлення інформаційного простору, коли суспільно значущі події висвітлюються вибірково, однобічно або з наперед заданими акцентами. Як слушно зазначається у сучасних правових дослідженнях, чинні вимоги щодо розкриття структури власності медіа потребують подальшого вдосконалення, а прозорість медіавласності має розглядатися як один із базових запобіжників проти прихованого впливу на редакційну політику та проти зловживань в інформаційній сфері. У такій ситуації загроза полягає не тільки у ворожих зовнішніх інформаційних впливах, а й у внутрішній вразливості медіасередовища, яке за відсутності належних правових і організаційних запобіжників може використовуватися як канал тиску на суспільну думку [65, с. 191].

З огляду на викладене, доцільно дійти висновку, що ефективна протидія пропаганді не може забезпечуватися лише поодинокими заборонними, обмежувальними або ситуативними управлінськими рішеннями. Такі заходи, хоча й мають прикладне значення в умовах виникнення конкретних інформаційних загроз, самі по собі не здатні забезпечити стійкий і довгостроковий результат (стратегічне планування). Належний рівень захисту

національного інформаційного простору можливий лише за умови формування цілісної, внутрішньо узгодженої та стратегічно орієнтованої загальнодержавної інформаційної політики, яка спиратиметься на єдність правових, організаційних, інституційних, комунікаційних та технічних засобів впливу. Зміст такої політики має виходити з того, що пропаганда в сучасних умовах, як вже було зазначено, є не лише інформаційним явищем, а й одним із засобів впливу на суспільну свідомість, публічне управління, оборонну стійкість, громадську стабільність та міжнародний авторитет держави. У зв'язку з цим протидія пропаганді повинна розглядатися як самостійний напрям державної діяльності, який потребує чітко визначених стратегічних орієнтирів, належного нормативного підґрунтя, розподілу компетенції між уповноваженими суб'єктами та процедурної впорядкованості управлінських дій. Саме з цих міркувань обґрунтованою є необхідність затвердження авторської *Концепції національної інформаційної політики України* як базового стратегічного документа, покликаного визначити цілі, принципи, напрями, суб'єктний склад і механізми реалізації державної політики у сфері інформаційної безпеки та протидії пропаганді (Рис. 2. Додатки).

Наукова доцільність розроблення цієї Концепції полягає в тому, що на сьогодні державна політика у відповідній сфері реалізується через значну кількість нормативно-правових та підзаконних нормативно-правових актів, які не завжди утворюють завершену та впорядковану систему. Унаслідок цього окремі напрями державного реагування розвиваються нерівномірно, правове регулювання залишається фрагментарним, а координація між суб'єктами публічної влади значною мірою залежить від поточної безпекової ситуації. Запропонована Концепція (Рис. 2) покликана усунути зазначені недоліки шляхом формування єдиної методологічної, правової та організаційної основи державної інформаційної політики.

У структурному аспекті Концепція національної інформаційної політики України, на нашу думку, має складатися з низки взаємопов'язаних

розділів, кожен із яких виконує окреме функціональне призначення [26, с. 3005–3015].

Перший розділ доцільно присвятити *загальним положенням*, у межах яких необхідно визначити мету Концепції, її місце у системі документів стратегічного планування, нормативну основу, сферу дії, а також базові терміни. В цьому розділі доцільно закріпити авторське розуміння національної інформаційної політики як *цілеспрямованої, нормативно забезпеченої та інституційно організованої діяльності держави, спрямованої на розвиток і захист національного інформаційного простору, гарантування інформаційних прав, зміцнення інформаційної стійкості суспільства, забезпечення незалежності медіасередовища та нейтралізацію зовнішніх і внутрішніх деструктивних інформаційних впливів*.

Другий розділ має містити *характеристику сучасного стану інформаційної сфери України та основних проблем державної політики у цій сфері*. Тут доцільно відобразити основні виклики: фрагментарність інформаційного законодавства, недостатню узгодженість діяльності суб’єктів публічної влади, вразливість віртуального середовища до дезінформаційних впливів, концентрацію медіавласності, фінансову залежність частини медіа, недостатній рівень міжнародної інформаційної присутності України, технічну нерівномірність функціонування комунікаційної інфраструктури, а також обмеженість програм підвищення медіаграмотності населення. Значення цього розділу полягає в тому, що він має зафіксувати не лише перелік недоліків, а їх системний взаємозв’язок, показавши, що слабкість інформаційної політики зумовлюється не одним чинником, а сукупністю проблем.

Третій розділ доцільно присвятити *завданням національної інформаційної політики.* На наш погляд, такими завданнями мають бути: захист національного інформаційного простору від пропаганди, дезінформації та інших деструктивних впливів; забезпечення права громадян на достовірну та повну інформацію; зміцнення незалежності та прозорості медіа; розвиток

стратегічних комунікацій держави; створення механізмів координації між суб'єктами інформаційної політики; підтримка інформаційної присутності України у світі; підвищення медіаграмотності населення; удосконалення системи правового регулювання інформаційних відносин [29, с. 14–18].

Четвертий розділ має закріплювати *принципи реалізації національної інформаційної політики*. До них доцільно віднести: верховенство права; законність; пропорційність втручання держави в інформаційну сферу; пріоритет захисту національних інтересів; повагу до свободи слова та права на інформацію; достовірність офіційної комунікації; відкритість публічної влади; інституційну узгодженість; своєчасність реагування на інформаційні загрози; поєднання превентивних і реагувальних заходів; відповідальність суб'єктів інформаційної політики за результати своєї діяльності.

П'ятий розділ доцільно побудувати навколо *основних напрямів реалізації національної інформаційної політики.* На нашу думку, до таких напрямів мають належати: нормотворчий; інституційно-координаційний; безпековий; медійний; комунікаційний; міжнародний; технологічний; освітньо-просвітницький. Нормотворчий напрям має передбачати систематизацію інформаційного законодавства, усунення прогалин і колізій, а також визначення правових критеріїв оцінки деструктивного контенту. Інституційно-координаційний напрям покликаний забезпечити узгодженість діяльності органів державної влади, регуляторів, правоохоронних органів і суб'єктів сектору безпеки і оборони. Безпековий напрям охоплює виявлення, попередження та припинення пропагандистських, дезінформаційних і психологічних впливів, що завдають шкоди національним інтересам. Медійний напрям пов'язаний із підтримкою незалежності медіа, прозорості медіавласності та зменшенням політичного й економічного впливу на редакційну політику. Комунікаційний напрям має охоплювати розвиток офіційних комунікацій, кризового інформування та стратегічних комунікацій. Міжнародний напрям спрямований на посилення інформаційної присутності України за кордоном, донесення державної позиції до міжнародної аудиторії

та протидію зовнішній дискредитації. Технологічний напрям передбачає розвиток інфраструктури мовлення, цифрових платформ державної комунікації та засобів моніторингу інформаційного простору. Освітньо-просвітницький напрям має забезпечувати розвиток медіаграмотності, критичного мислення та навичок інформаційної самооборони населення [27, с. 18–23].

Шостий розділ доцільно присвятити *системі суб'єктів реалізації Концепції та розподілу їх компетенції.* У ньому слід чітко визначити повноваження Верховної Ради України, Президента України, Кабінету Міністрів України, Ради національної безпеки і оборони України, центральних органів виконавчої влади, Національної ради України з питань телебачення і радіомовлення, правоохоронних органів, суб'єктів сектору безпеки і оборони, органів місцевого самоврядування, державних і комунальних медіа, а також інститутів громадянського суспільства. При цьому, варто наголосити на тому, що наша пропозиція полягає в тому, щоб не просто перерахувати суб'єктів, а визначити три рівні їх участі: перший – суб'єкти стратегічного формування політики; другий – суб'єкти безпосередньої реалізації та координації;
третій – суб'єкти суспільної підтримки, громадського контролю та інформаційного партнерства.

Сьомий розділ має визначати *механізми реалізації Концепції*. До них слід віднести правовий (має охоплювати ухвалення та оновлення нормативно-правових актів), організаційний (побудову процедур взаємодії та координації між суб'єктами), інформаційно-аналітичний (постійний моніторинг інформаційного простору, виявлення загроз, аналітичне узагальнення тенденцій і вироблення прогнозів), фінансовий (ресурсне забезпечення державних програм і відповідних інституцій), кадровий (підготовку фахівців у сфері стратегічних комунікацій, медіарегулювання), технологічний (модернізацію засобів мовлення, цифрових платформ, систем кіберзахисту та моніторингу) і контрольний механізми (оцінювання результативності заходів, звітування та перегляд пріоритетів залежно від змін інформаційної ситуації).

Восьмий розділ повинен містити *етапи реалізації Концепції та очікувані результати*. Доцільно передбачити короткостроковий, середньостроковий і довгостроковий етапи. На короткостроковому етапі слід зосередитися на інвентаризації законодавства, аудиті інституційних повноважень, створенні координаційних процедур та розробленні підзаконних актів. На середньостроковому – на модернізації технічної бази, запровадженні програм підвищення медіаграмотності, посиленні міжнародної комунікації України, удосконаленні регуляторних і моніторингових практик. На довгостроковому – на формуванні стійкого, збалансованого та демократично впорядкованого інформаційного середовища, в якому пропагандистські впливи втрачатимуть ефективність через поєднання правового захисту, інституційної злагодженості та суспільної стійкості.

Дев'ятий розділ доцільно присвятити *показникам результативності реалізації Концепції.* Саме цей компонент найчастіше відсутній у програмних документах, що істотно знижує їх практичну цінність. У зв'язку з цим доцільно запропонувати систему критеріїв оцінювання, яка охоплюватиме: стан узгодженості інформаційного законодавства; рівень координації між суб'єктами інформаційної політики; ступінь прозорості медіавласності; рівень довіри населення до офіційних джерел інформації; охоплення програмами медіаграмотності; оперативність державного реагування на дезінформаційні кампанії; рівень міжнародної інформаційної присутності України; технічну спроможність державної комунікаційної інфраструктури. Запровадження таких індикаторів дало б змогу перевести Концепцію з площини загальних намірів у площину реального управлінського інструмента.

Отже, забезпечення інформаційної безпеки України об'єктивно зумовлює формування цілісної та ефективної загальнодержавної інформаційної політики, здатної забезпечувати не лише реагування на інформаційні загрози, а й їх своєчасне запобігання. Протидія пропаганді має розглядатися як системний напрям державної політики, спрямований на захист національних інтересів, інформаційної стійкості суспільства та належне

функціонування демократичних інститутів. У межах загальнодержавної інформаційної політики у протидії пропаганді виокремлено два взаємопов'язані напрями: розвиток інституцій громадських медіа та забезпечення фінансової, організаційної й редакційної незалежності державних і комерційних засобів масової інформації. Реалізація цих напрямів потребує вдосконалення нормативно-правового регулювання, зокрема шляхом впровадження Концепції національної інформаційної політики, кодифікації інформаційного законодавства та запровадження механізмів прозорості медіавласності й захисту редакційної автономії. Наголошено на тому, що Концепція має розглядатися не як формальний політико-декларативний документ, а як основа державної діяльності у сфері захисту інформаційного простору та протидії пропаганді. В цілому ж підвищення ефективності загальнодержавної інформаційної політики у протидії пропаганді можливе за умови комплексного поєднання правових, організаційних та інституційних заходів, спрямованих на розвиток єдиного інформаційного простору та зміцнення інформаційної безпеки держави.

Висновки до розділу 1

1. Встановлено, що інформаційна війна, особливо в умовах воєнного стану є не периферійним, а одним із базових різновидів загроз інформаційній безпеці держави, оскільки її вплив спрямований не лише на дезорієнтацію населення, а й на підрив довіри до органів публічної влади, послаблення національної стійкості, викривлення історичної пам'яті, дестабілізацію суспільних відносин і створення сприятливого середовища для зовнішнього воєнно-політичного та інформаційного впливу. Для сфери публічного управління та адміністрування інформаційна війна є загрозою, що потребує не епізодичного реагування, а системної, інституційно забезпеченої та науково обґрунтованої державної політики, зорієнтованої на захист інформаційного суверенітету, посилення стратегічних комунікацій, своєчасне спростування

дезінформації та зміцнення суспільної згуртованості. Результати проведених опитувань підтвердили, що особливо небезпечними каналами інформаційного впливу респонденти вважають історичні фальсифікації та маніпуляції щодо минулого України, а також наголошують на потребі ширшого використання державою науково обґрунтованих інформаційних продуктів для спростування ворожих наративів. Водночас оцінки працівників сфери публічного управління, науково-педагогічних працівників і здобувачів вищої освіти засвідчили вагоме значення незалежних фактчекінгових ініціатив і громадських інформаційно-аналітичних платформ у протидії пропаганді. З огляду на це доведено, що ефективна протидія інформаційній війні можлива лише за умови поєднання державних і громадських зусиль, налагодження сталої взаємодії між органами влади, науковим середовищем та інститутами громадянського суспільства, а також включення протидії дезінформації до числа пріоритетних напрямів публічного управління у сфері забезпечення інформаційної безпеки держави.

2. Виокремлено історичний аспект пропагандистського впливу та показано, що одним із найбільш дієвих інструментів сучасної інформаційної агресії є історичні фальсифікації, маніпулювання колективною пам’яттю, нав’язування псевдоісторичних наративів, міфологізація минулого та викривлення фактів, пов’язаних із державотворенням України. Встановлено, що через такі підходи пропаганда впливає не лише на оцінку минулого, а й на сучасну політичну позицію суспільства, формує сумніви щодо легітимності української державності та створює підґрунтя для виправдання зовнішнього інформаційного й політичного втручання.

3. До найбільш поширених сучасних пропагандистських технологій і методів віднесено масове поширення фейкових повідомлень, маніпулятивне конструювання інформаційного порядку денного, повторюване відтворення необхідних наративів, селективний добір і замовчування фактів, використання емоційного тиску, мови ворожнечі, псевдоекспертного середовища, анонімних телеграм-каналів, бот-мереж, цифрових платформ, візуальних маніпуляцій і

прихованих форм інформаційного впливу. Доведено, що небезпека цих технологій полягає у їх комплексному характері, високій швидкості адаптації до нових умов та здатності поєднуватися з кіберзагрозами і психологічними методами. Обґрунтовано, що протидія сучасним пропагандистським технологіям має бути одним із пріоритетів державної політики у сфері інформаційної безпеки та передбачати системне виявлення ворожих наративів, своєчасне спростування маніпулятивного контенту, зміцнення стратегічних комунікацій і підвищення рівня медіаграмотності населення.

4. Доведено, що державна інформаційна політика є головним інструментом протидії пропаганді, від ефективності якого залежить стан інформаційної безпеки держави, рівень суспільної стійкості та здатність органів влади своєчасно реагувати на деструктивні інформаційні впливи. Встановлено, що наявні проблеми у цій сфері мають системний характер і проявляються у фрагментарності інформаційного законодавства, недостатній узгодженості дій суб’єктів публічної влади та певній вразливості віртуального середовища до дезінформаційних кампаній. Обґрунтовано, що подальший розвиток державної інформаційної політики потребує переходу від розрізнених заходів реагування до цілісної стратегічного планування, у межах якого будуть поєднані правові, організаційні, безпекові, медійні, технологічні та просвітницькі засоби.

5. Розроблено авторську Концепцію національної інформаційної політики України як програмний документ, покликаний визначити мету, принципи, завдання, напрями, суб’єктний склад і механізми реалізації державної політики у сфері інформаційної безпеки та протидії пропаганді. Запропоновано її змістову структуру, яка охоплює: загальні положення; характеристику сучасного стану інформаційної сфери; завдання національної інформаційної політики; принципи її реалізації; основні напрями реалізації; систему суб’єктів та розподіл їх компетенції; механізми реалізації; етапи впровадження та очікувані результати; показники результативності. Окремо запропоновано поділ суб’єктів реалізації Концепції на три рівні участі: 1)

суб’єкти стратегічного формування політики, 2) суб’єкти безпосередньої реалізації та координації, а також суб’єкти суспільної підтримки, громадського контролю й інформаційного партнерства. Визначено систему механізмів реалізації Концепції (правовий, організаційний, інформаційно-аналітичний, фінансовий, кадровий, технологічний, контрольний) та обґрунтовано доцільність запровадження конкретних індикаторів оцінювання її результативності. Запропонована нами Концепція може бути використана як методологічна й прикладна основа для вдосконалення державної інформаційної політики України в умовах пропагандистських та інформаційно-воєнних загроз.

РОЗДІЛ 2.
МЕХАНІЗМ ФОРМУВАННЯ ДЕРЖАВНОЇ СТРАТЕГІЇ ПРОТИДІЇ ІНФОРМАЦІЙНІЙ ВІЙНІ

2.1. Зарубіжний досвід формування державної стратегії протидії інформаційній війні

Дослідження зарубіжного досвіду формування державної стратегії протидії інформаційній війні має важливе теоретичне і прикладне значення для України, оскільки дає змогу не лише простежити напрями розвитку відповідної державної політики у провідних демократичних країнах, а й виявити найбільш результативні організаційні, правові, комунікаційні та технологічні засоби захисту інформаційного простору. Для української держави таке звернення до досвіду інших країн має особливу вагу, оскільки повномасштабна агресія російської федерації супроводжується масовим використанням дезінформації, різного роду маніпулятивних наративів, інформаційно-психологічного впливу, спроб дискредитації державних інституцій, підриву міжнародної підтримки України та розхитування суспільної єдності. У зв'язку з цим аналіз підходів, що були вироблені, зокрема, у Європейському Союзі та Сполучених Штатах Америки, дозволяє окреслити основні перспективні напрями вдосконалення національної стратегії у сфері протидії інформаційній війні.

Зростання уваги до проблеми дезінформації та інформаційного впливу з боку міжнародних інституцій зумовлене усвідомленням того, що інформаційне середовище дедалі частіше використовується як простір політичного тиску, маніпулювання суспільною свідомістю та втручання у внутрішні справи держав. На Всесвітньому економічному форумі (WEF), що проходив 15–19 січня 2024 року в Давосі, Президентка Європейської Комісії Урсула фон дер Ляєн у своїй промові наголосила, що «головними ризиками наступних двох років є не конфлікт чи клімат. Це дезінформація та неправдива

інформація, за якою слідує поляризація суспільств. Такі ризики є серйозними, оскільки вони обмежують здатність долати великі глобальні виклики, з якими ми стикаємося, а саме: зміни природнього клімату, геополітичні, технологічні зміни» [47]. Наведена оцінка відображає зміну міжнародного сприйняття інформаційних загроз, які дедалі частіше розглядаються як окремий чинник дестабілізації демократичних інститутів і суспільної єдності. У подальших виступах Урсула фон дер Ляєн неодноразово зверталася до цієї проблематики, окремо акцентуючи увагу на Україні та підкреслюючи, що навколо нашої держави розгортається один із найбільш показових прикладів масштабного дезінформаційного впливу у світовому просторі. Характеризуючи дезінформацію як «проблему № 1 серед глобальних ризиків», вона також наголосила, що «цінності, які ми цінуємо офлайн, повинні також бути захищені онлайн» [47].

Підґрунтям таких оцінок став Звіт про глобальні ризики 2024 року, у якому серед основних короткострокових загроз особливе місце посідають дезінформація, неправдива інформація та зумовлена ними поляризація суспільств. Однією з центральних тез цього Звіту є те, що 2024–2025 роки характеризуються участю майже 4 мільярдів людей у національних та муніципальних виборах, у тому числі у США, Мексиці, Індії, Пакистані, Індонезії. За такого масштабу виборчих процесів дезінформаційні кампанії можуть істотно впливати на сприйняття політичної реальності, підривати легітимність новообраних урядів, руйнувати довіру до виборчих процедур та сприяти дестабілізації демократичного устрою. У Звіті цілком слушно підкреслюється, що «поляризовані суспільства можуть стати поляризованими не лише за своїми політичними пристрастями, але й за сприйняттям реальності. Фальсифікована інформація також може розпалити ворожість до певних груп, від упередженості та дискримінації на робочому місці до насильства та злочинів на ґрунті ненависті» [211].

У межах аналізованої проблематики особливий інтерес становить досвід Європейського Союзу та Сполучених Штатів Америки як стратегічних

партнерів України. Звернення до практики саме цих суб'єктів зумовлено не лише їхнім впливом на міжнародну політику, а й тим, що російська пропаганда та дезінформація вже тривалий час виступають одним із пріоритетних інструментів зовнішнього впливу російської федерації на демократичні суспільства. У війні проти України інформаційний компонент агресії має системний характер: через мережі поширення неправдивих наративів, маніпулювання новинним порядком денним, перекручення фактів про воєнні події, дискредитацію української влади та партнерів росія прагне знизити рівень міжнародної підтримки України, підірвати політичний консенсус серед союзників, послабити санкційний тиск і виправдати власну агресію. Проте спрямованість російської інформаційної війни не обмежується лише українським напрямом. Під загрозою перебувають і країни Європейського Союзу, і Сполучені Штати Америки, і будь-які інші демократичні держави, оскільки російський дезінформаційний вплив має глобальну мету – дискредитацію демократичних інституцій, посилення суспільних розколів, легітимацію антидемократичних сил та послаблення стійкості держав.

У Європейському Союзі протидія інформаційним загрозам вже давно набула системного характеру. Початковим поштовхом до розроблення більш цілісної політики у цій сфері стала російська анексія Криму у 2014 році. Саме після неї у структурах ЄС відбулося усвідомлення того, що інформаційна війна з боку російської федерації становить суттєву загрозу політичній стабільності, безпеці та демократичним процесам. У 2015 році Європейською комісією була створена і розпочала діяльність оперативна робоча група зі стратегічних комунікацій Європейського Союзу – East StratCom Task Force (ESTF). Робота цієї групи була зорієнтована передусім на підвищення обізнаності щодо прокремлівської дезінформації, інформаційних маніпуляцій, координацію комунікації інституцій Європейського Союзу та зміцнення стійкості до дезінформаційного впливу. Водночас діяльність ESTF не зводилася лише до викриття окремих фейків. Важливу частину її роботи становили заходи із підтримки стійкого медіасередовища у Східному сусідстві та сприяння

підтримці незалежних засобів масової інформації. З 2015 року ESTF реалізує кампанію EUvsDisinfo, спрямовану на моніторинг, аналіз та реагування на дезінформацію і маніпулювання інформацією [213]. Саме цей ресурс перетворився на один із найбільш упізнаваних елементів європейської політики у сфері протидії дезінформації.

Функціонування EUvsDisinfo дало змогу на практиці накопичити значний масив даних про характер і способи проведення дезінформаційних кампаній. Узагальнення відповідних матеріалів дозволяє виокремити кілька найбільш поширених напрямів таких кампаній: створення конфліктогенного контенту з метою розпалювання суспільної ворожнечі, міжрасової та міжетнічної нетерпимості; вплив на політичні дебати через соціальні мережі та засоби масової інформації; втручання у демократичні процеси, насамперед у виборчу сферу; поєднання інформаційних операцій із кібератаками на критичну інфраструктуру та мережі. У такий спосіб у межах Європейського Союзу поступово сформувалося розуміння того, що інформаційна війна є багатовимірним явищем, яке потребує не лише медійної відповіді, а й адміністративного, правового, технологічного й аналітичного супроводу.

Важливе місце у європейській політиці протидії дезінформації посідає Посилений кодекс практики щодо дезінформації, який було підписано і опубліковано Європейською комісією 16 червня 2022 року. Його значення полягає у тому, що він закріпив комплекс зобов’язань для великих онлайн-платформ, соціальних мереж, суб’єктів рекламної індустрії, фактчекерських організацій, дослідницьких центрів та інших учасників цифрового середовища. Документ містить 44 зобов’язання та 128 конкретних заходів, спрямованих на підвищення прозорості й підзвітності платформ у питаннях поширення дезінформації в мережі Інтернет [196; 232]. Йдеться не про декларативний акт політичного характеру, а про інструмент, за допомогою якого Європейський Союз прагне пов’язати саморегуляцію цифрових сервісів із публічними інтересами захисту демократії, виборчих процесів, інформаційної безпеки та прав користувачів. Додаткового значення Кодексу

надає та обставина, що 13 лютого 2025 року Європейська комісія та Європейська рада з цифрових послуг підтримали його інтеграцію у форматі Code of Conduct on Disinformation у правову рамку Digital Services Act, що посилило його зв'язок із загальною системою цифрового регулювання Європейського Союзу [228].

Звернемо увагу на те, що Кодекс не обмежується загальними деклараціями. Його конструкція передбачає періодичну та систематичну звітність компаній щодо заходів, яких вони вживають для виявлення, обмеження і попередження поширення дезінформації. У цьому аспекті показовими є окремі зобов'язання, які демонструють глибоке розуміння новітніх ризиків інформаційної війни. Так, зобов'язання 15 адресоване тим підписантам, які розробляють або використовують системи штучного інтелекту і поширюють AI-згенерований чи змінений контент, зокрема deepfake-матеріали. У межах цього зобов'язання наголошено на необхідності враховувати вимоги прозорості та протидіяти маніпулятивним практикам, у тому числі шляхом попередження користувачів і проактивного виявлення такого контенту [198]. Зобов'язання 18 закликає підписантів мінімізувати ризик вірусного поширення дезінформації через запровадження безпечних практик ще на етапі проєктування систем, політик і функцій сервісів [199]. Значення такого підходу полягає в тому, що відповідальність покладається не лише на стадії реагування після поширення шкідливого контенту, а ще на рівні побудови алгоритмів рекомендацій, механізмів поширення, ранжування та підсилення інформації. Не менш важливим є зобов'язання 29, відповідно до якого підписанти повинні проводити дослідження на основі прозорої методології та етичних стандартів, а також обмінюватися наборами даних, результатами досліджень і методиками з релевантною аудиторією [222].

Такий підхід засвідчує, що боротьба з дезінформацією в Європейському Союзі спирається не лише на управлінські приписи та технічні засоби модерації контенту, а й на дослідницьке підґрунтя, без якого неможливо ані виявити закономірності інформаційного впливу, ані оцінити ефективність

ужитих заходів. Необхідно окремо вказати і на склад учасників цього Кодексу. На момент його представлення у 2022 році до процесу перегляду приєдналися 34 підписанти, а надалі коло учасників істотно розширилося. Станом на лютий 2026 року на офіційному ресурсі Європейської комісії серед чинних підписантів зазначено 44 суб'єкти, серед яких Adobe, Google, Meta, Microsoft Advertising, Microsoft Bing, Microsoft LinkedIn, TikTok, Twitch, NewsGuard, European Factchecking Standards Network, Democracy Reporting International, VOST Europe, Maldita.es, PagellaPolitica та інші організації, що представляють платформи, рекламну сферу, фактчекінг, дослідницьке та громадянське середовище [228].

Перелічений склад учасників має суттєве значення, оскільки свідчить про намагання Європейського Союзу вибудувати багаторівневу систему співпраці, у якій протидія дезінформації не зводиться виключно до державного примусу або до внутрішньої політики окремих платформ. Натомість формується простір узгоджених дій між основними інституціями ЄС, технологічними компаніями, аналітичними центрами, незалежними фактчекерами та громадянським суспільством. У вересні 2023 року Європейська комісія окремо повідомила, що Google, Meta, Microsoft і TikTok подали другий комплект звітів про виконання Кодексу, а у березні 2024 року було підкреслено, що перші звіти опубліковано у лютому 2023 року. У межах прийнятих зобов'язань підписанти мають вживати заходів у низці сфер: демонетизація поширення дезінформації, забезпечення прозорості політичної реклами, посилення співпраці з фактчекерами, розширення прав та можливостей користувачів завдяки інструментам розпізнавання маніпулятивного контенту, а також надання дослідникам кращого доступу до даних [232].

Практичне значення Кодексу можна простежити на прикладі окремих держав Європейського Союзу, де наднаціональні підходи поєднуються з національними механізмами реагування на інформаційні загрози. Наприклад, у Франції у 2021 році було створено службу VIGINUM, підпорядковану

Генеральному секретаріату з оборони і національної безпеки (SGDSN). На офіційному рівні визначено, що VIGINUM покликана захищати Францію та її інтереси від іноземного цифрового втручання, а її роль полягає у виявленні та характеристиці кампаній інформаційної маніпуляції за участю іноземних акторів, які можуть завдавати шкоди фундаментальним інтересам держави [217]. Така інституція становить приклад того, як принципи, закладені у європейських документах, реалізуються через спеціалізований національний орган, здатний поєднувати моніторинг, аналітику та оперативне інформування держави про іноземні інформаційні операції.

У Німеччині федеральний уряд сформував окремі підходи до протидії російським дезінформаційним наративам, зосередивши увагу на виявленні таких наративів, посиленні комунікації, заснованої на перевірених фактах, і підвищенні суспільної стійкості [230]. Німецький підхід показує, що ефективність наднаціональних ініціатив значною мірою залежить від того, наскільки вони підкріплені на рівні держав-членів інституційною координацією та політикою публічної комунікації.

У Швеції діяльність Агентства психологічного захисту спрямована на координацію, розвиток і зміцнення психологічної оборони держави; до його завдань віднесено попередження, виявлення, аналіз і протидію зловмисному інформаційному впливу, дезінформації та пропаганді [200]. Натомість у Фінляндії протидія дезінформації спирається на високий рівень суспільної довіри до інституцій і медіа, а також на системне впровадження медіаграмотності як елемента розвитку критичного мислення; у документах уряду та OECP такий підхід характеризується як складова ширшої суспільної стійкості до дезінформації [218].

Отже, європейський підхід поєднує два рівні: наднаціональний (через Кодекс, DSA, EDMO та інші механізми ЄС), і національний (через спеціалізовані служби, урядові координаційні підрозділи, системи публічної комунікації та освітні програми в окремих державах-членах).

Подальша еволюція цього підходу знайшла вияв в механізмах моніторингу виконання взятих зобов'язань. Постійна робоча група покликана переглядати й адаптувати зобов'язання з урахуванням технологічних, соціальних, ринкових та законодавчих змін. До її складу входять представники підписантів, регуляторних органів, Європейської обсерваторії цифрових медіа та Європейської служби зовнішніх справ. Значення такого формату полягає у тому, що протидія дезінформації не замикається на діяльності одного органу, а організовується як постійна взаємодія державних інституцій, приватного сектору та незалежної експертної спільноти. У поєднанні з доступом дослідників до даних, що передбачається статтею 40 Закону про цифрові послуги (DSA), формується правове й організаційне підґрунтя для тривалих досліджень впливу онлайн-діяльності на реальне суспільне життя [226]. Отже, для Європейського Союзу характерний системний підхід, спрямований, з одного боку, на виявлення неправдивих повідомлень, способів їх поширення та суб'єктів такого впливу, а з другого – на недопущення надмірного обмеження прав громадян на доступ до інформації.

Одним із центральних нормативно-правових актів у цифровій політиці Європейського Союзу став Закон про цифрові послуги (Digital Services Act, DSA), ухвалений 19 жовтня 2022 року. Його поява була зумовлена тим, що попереднє регулювання електронної комерції вже не забезпечувало належної відповіді на нові виклики, пов'язані з масовим поширенням незаконного контенту, недостатньою прозорістю алгоритмів, фрагментарністю національних підходів до нагляду за платформами та зростанням впливу великих цифрових посередників на інформаційний простір [4, с. 45–46]. Значення DSA виходить далеко за межі технічного впорядкування діяльності соціальних мереж або маркетплейсів, оскільки йдеться про формування цілісного правового механізму, спрямованого на забезпечення безпечного цифрового середовища, захист основних прав користувачів, підвищення підзвітності платформ та вироблення єдиних правил функціонування цифрових сервісів на внутрішньому ринку ЄС [203]. У науковій літературі

підкреслюється, що DSA запровадив диференційоване регулювання для кількох категорій постачальників цифрових послуг, закріпив вимоги до прозорості алгоритмів, модерації контенту, функціонування механізмів скарг та захисту прав одержувачів послуг. Для України такий досвід є особливо цінним, оскільки дозволяє простежити, яким чином у праві ЄС поєднуються захист користувача, інституційний контроль і вимоги до платформ, що фактично стали ключовими інфраструктурними елементами сучасного інформаційного середовища [190, с. 3–4].

Важливо й те, що дія DSA поширюється на постачальників послуг, які працюють на ринку Європейського Союзу, незалежно від місця їх державної реєстрації, а тому цей акт набув екстериторіального значення та перетворився на інструмент не лише внутрішнього, а й зовнішнього нормативного впливу ЄС на цифрові платформи [4, с. 49]. Особливого значення в контексті протидії інформаційним загрозам набувають положення DSA, які спрямовані не просто на видалення незаконного контенту, а на попередження системних ризиків, що виникають унаслідок функціонування самих платформ. У фахових публікаціях справедливо зазначається, що Закон окремо виділяє дуже великі онлайн-платформи та дуже великі онлайн-пошукові системи, тобто сервіси, які мають щонайменше 45 мільйонів активних користувачів у ЄС щомісяця; саме для таких суб’єктів запроваджено спеціальні обов’язки щодо регулярної оцінки системних ризиків, зокрема ризиків, пов’язаних із роботою рекомендаційних і рекламних систем [67, с. 579–580]. Вказаний підхід має безпосередній стосунок до протидії інформаційній війні, адже дозволяє розглядати дезінформацію не як випадковий наслідок активності окремих користувачів, а як явище, інтенсивність якого може посилюватися самою архітектурою цифрового сервісу, способами ранжування інформації, механізмами персоналізації та рекламного таргетингу. Не менш показовим є й те, що DSA забороняє оманливі та маніпулятивні інтерфейсні практики, відомі як «темні шаблони», які спонукають користувача до рішень, яких він спочатку не мав наміру приймати. Аналітичні матеріали українських експертів

додатково акцентують, що в межах DSA забороняються окремі форми реклами, орієнтованої на дітей, а також практики, пов’язані з використанням чутливих даних; у частині правозастосування Європейська комісія наділена повноваженнями накладати штрафи до 6% від загального обороту компанії у разі недотримання вимог Регламенту. Наведені положення свідчать про прагнення Європейського Союзу надати боротьбі з інформаційними загрозами не лише політичного, а передусім нормативно-правового характеру, за якого відповідальність за цифрову безпеку покладається не тільки на державу чи користувача, а й на самі платформи як впливових учасників інформаційного простору [190, с. 27; 203].

Втім, важливе місце у формуванні та розвитку європейської стратегії протидії дезінформації посіли ті програмні документи, які були ухвалені ще до запровадження Закону про цифрові послуги та Посиленого кодексу практики щодо дезінформації. Одним із базових актів у цьому напрямі стало Повідомлення Європейської Комісії від 26 квітня 2018 року «Боротьба з дезінформацією в Інтернеті: європейський підхід», у якому дезінформацію було визнано не просто медійною проблемою, а явищем, здатним негативно впливати на демократичні процеси, вибори, формування державної політики та рівень суспільної довіри до інституцій [107, с. 5–7; 206, p. 6–7]. У межах цього документа Європейська Комісія запропонувала комплексне бачення протидії дезінформації, що поєднувало нормативні, інституційні, освітні та комунікаційні засоби, а також наголосила на необхідності вироблення збалансованого підходу, який би не руйнував свободу вираження поглядів і водночас давав змогу обмежувати шкідливі інформаційні впливи. Цей підхід засвідчив відхід ЄС від спрощеного розуміння дезінформації як суто неправдивого контенту та орієнтацію на ширшу модель суспільної стійкості до маніпулятивних інформаційних практик [157, с. 155–157].

Зміст названого Повідомлення дає підстави стверджувати, що Європейська Комісія заклала ті концептуальні орієнтири, які в подальшому були розвинуті у спеціальних кодексах, планах дій та законодавчих актах ЄС.

Передусім ішлося про підвищення прозорості цифрового середовища, посилення відповідальності онлайн-платформ, розвиток механізмів виявлення й спростування дезінформаційних кампаній, а також формування стійкості суспільства до інформаційних маніпуляцій. Особливий акцент зроблено на медіаграмотності, оскільки саме вона розглядалась як один із найбільш ефективних довгострокових засобів нейтралізації дезінформаційного впливу. У цьому контексті ЄС виходив із того, що громадяни повинні не лише отримувати інформацію, а й володіти навичками критичного осмислення медіаконтенту, розрізнення фактів, оцінювання джерел та виявлення маніпулятивних повідомлень [50, с. 157–158]. Не менш важливо, що серед пріоритетів було визначено підтримку якісної журналістики та незалежних медіа, оскільки без функціонування професійного інформаційного середовища неможливо забезпечити належний рівень демократичної дискусії та захисту суспільства від масового поширення недостовірних відомостей [206, с. 7].

Самостійного значення набув і безпековий вимір цього документа. У Повідомленні наголошувалося, що дезінформація здатна використовуватися як інструмент зовнішнього втручання, політичного тиску та дестабілізації, особливо в періоди виборчих кампаній і суспільно криз [231]. Тому Європейська Комісія запропонувала не обмежуватися реакцією на окремі інформаційні вкиди, а розвивати постійний діалог із державами-членами щодо зміцнення стійкості виборчих процесів до кіберзагроз, координації стратегічних комунікацій та формування спільної відповіді на внутрішні й зовнішні інформаційні загрози. Надалі ці положенні були покладені в основу Плану дій ЄС проти дезінформації, в якому вже більш предметно були визначені чотири пріоритетні напрями: посилення інституційних можливостей ЄС, зміцнення координації та спільної відповіді, мобілізація приватного сектору та підвищення суспільної обізнаності й стійкості [231].

У цьому документі підкреслено, що найбільшу загрозу для Європейського Союзу становить дезінформація, здійснювана з боку російської федерації. Серед нагальних кроків було передбачено створення і запуск

спеціальної системи швидкого сповіщення – Rapid Alert System (RAS). Важливість цієї системи полягає у тому, що вона забезпечує оперативний обмін інформацією між державами-членами та інституціями ЄС щодо виявлених дезінформаційних загроз, сприяючи швидкому узгодженню реагування. Подальше посилення політики ЄС у цій сфері відбулося у грудні 2020 року, коли Європейська комісія представила План дій щодо європейської демократії. Документ передбачав посилення рамки політики ЄС за трьома основними напрямами: сприяння вільним і чесним виборам та активній демократичній участі; підтримка вільних і незалежних засобів масової інформації; протидія дезінформації [221].

Щодо останнього напряму Комісія наголосила на необхідності розширення співпраці з Агентством з кібербезпеки (ENISA), Європейською обсерваторією цифрових медіа (EDMO), а також з Групою експертів із медіаграмотності. Досить показово, що Європейський Союз у протидії інформаційним загрозам значну увагу приділяє не лише діяльності інституцій, а й розширенню можливостей самих громадян, оскільки цифрова грамотність дає змогу людині безпечніше орієнтуватися в онлайн-середовищі і критичніше сприймати інформаційний контент.

Надалі, у грудні 2022 року Європейський парламент, Рада Європейського Союзу та Європейська комісія спільно проголосили Європейську декларацію про цифрові права та принципи для цифрового десятиліття, яка стала політико-правовим орієнтиром для подальшого розвитку цифрової політики ЄС [207]. На офіційному рівні цей документ позиціонується як такий, що відображає бачення Союзу щодо безпечної, захищеної та сталої цифрової трансформації, у центрі якої перебуває людина, її гідність, права і свободи. Декларація не створює нових суб’єктивних прав у формально-юридичному розумінні, однак виконує роль узагальненого нормативно-ціннісного орієнтира для інституцій ЄС, держав-членів, бізнесу та інших суб’єктів, які беруть участь у формуванні цифрового середовища [2; 197, с. 1; 207].

Структурно Декларація передбачає шість розділів, які охоплюють: 1) людиноцентричний характер цифрової трансформації; 2) солідарність та інклюзію; 3) свободу вибору в цифровому середовищі; 4) участь у цифровому публічному просторі; 5) безпеку, захищеність і розширення можливостей людини; 6) сталість цифрового майбутнього. У науковій літературі слушно підкреслюється, що така структура відображає прагнення Європейського Союзу не зводити цифровізацію лише до технічного прогресу чи ринкової ефективності, а пов'язати її з вимогами демократії, верховенства права, соціальної справедливості та поваги до фундаментальних прав [12, с. 34; 188, с. 25].

Для тематики протидії дезінформації та інформаційній війні значення цього документа полягає насамперед у тому, що він закріплює загальні засади організації цифрового простору, в межах якого мають забезпечуватися безпечне онлайн-середовище, захист від незаконного і шкідливого контенту, прозорість використання алгоритмів, належний рівень захисту персональних даних, а також реальна можливість участі громадян у цифровому публічному просторі. Йдеться не про вузькоспеціальний акт у сфері боротьби з дезінформацією, а про ширшу нормативну основу, що визначає, яким саме має бути європейський цифровий порядок: демократичним, відкритим, підзвітним і таким, що не допускає підриву прав людини під приводом технологічного розвитку. У цьому аспекті Декларація формує ціннісну базу для подальших спеціальних актів ЄС, зокрема у сфері цифрових послуг, платформної відповідальності, кібербезпеки та протидії маніпулятивним інформаційним впливам [21, с. 95–96; 188, с. 25–26; 205, с. 1]. Також особливої уваги заслуговує те, що в тексті Декларації прямо наголошено на потребі забезпечення справедливого цифрового середовища, в якому люди мають бути поінформовані про взаємодію з алгоритмічними системами та системами штучного інтелекту, а діти й молодь повинні бути захищені від шкідливого й незаконного контенту, маніпулювання, експлуатації та зловживань онлайн.

Водночас, на відміну від Європейського Союзу, у Сполучених Штатах Америки підхід до протидії інформаційній війні має дещо іншу внутрішню логіку. Якщо в ЄС акцент робиться на поєднанні регуляторних, комунікаційних, освітніх та платформених механізмів, то американський підхід більш тяжіє до безпекового, розвідувального, аналітичного й міжвідомчого виміру. Інформаційна війна між росією і США не є новим явищем, однак особливої інтенсивності вона набула після повномасштабного вторгнення росії в Україну. Для американської влади це означало потребу не лише відстежувати кремлівські інформаційні кампанії, а й виробляти нові інструменти їхнього виявлення, публічного викриття та нейтралізації. Російська федерація прагне підірвати позиції США всередині країни, в Європі та у світі загалом, виходячи з власного уявлення про необхідність протидії американському впливу. Через дезінформаційні кампанії вона намагається дискредитувати демократичні інститути, посилювати поляризацію в американському суспільстві та формувати недовіру до державної політики.

Активізація дезінформаційних операцій з боку авторитарних режимів спонукала США до поступового вибудовування загальнодержавного підходу у цій сфері. Ще за адміністрації Б. Обами було зроблено кроки до посилення координації у протидії зовнішній пропаганді та інформаційному впливу. У 2016 році президентом Б. Обамою було підписано указ про офіційне створення Глобального центру взаємодії (Global Engagement Center, GEC), завданням якого стало викриття різних форм пропаганди та протидія дезінформаційним зусиллям, спрямованим на підрив або вплив на політику, безпеку чи стабільність Сполучених Штатів Америки, їхніх союзників та країн-партнерів [208]. Значення GEC полягало в тому, що він став майданчиком акумуляції та поширення аналітичної інформації щодо іноземної пропаганди, у тому числі російської. Попри те, що діяльність цього центру піддавалася критиці з боку окремих представників свободи ЗМІ, він систематично публікував матеріали, присвячені тактиці поширення дезінформації у світі. У межах протидії кремлівським інформаційним кампаніям щодо вторгнення в Україну GEC

розпочав випуск «Бюлетенів кремлівської дезінформації» (Kremlin Disinformation Bulletins), які виконували функцію публічного аналітичного інформування.

Поряд із цим у США розвивалися й міжвідомчі форми координації. У 2018 році Міністерство внутрішньої безпеки і Міністерство юстиції створили міжвідомчу робочу групу з протидії російській дезінформації. До її складу були включені Цільова група з протидії іноземному впливу Міністерства національної безпеки та Цільова група з кіберцифрових технологій Міністерства юстиції. Такий формат співпраці дає підстави стверджувати, що американський підхід поступово відходив від вузького сприйняття дезінформації як виключно зовнішньополітичної чи медійної проблеми. Вона стала розглядатися як багатокомпонентна загроза, що перетинається з проблемами виборчої безпеки, кіберзахисту, контррозвідувальної діяльності та стійкості державних інституцій. Ще одним важливим кроком було «заснування при офісі Директора Національної розвідки США у 2021 році Центру протидії деструктивному іноземному впливу» [9, с. 96]. У наведеному випадку чітко простежується інтеграція аналітичного та безпекового компонентів у межах єдиної державної політики реагування на інформаційні загрози.

Особливу роль у США відіграють розвідувальні органи, які застосовують тактику розкриття розвідувальної інформації щодо російських кампаній інформаційної війни, попереджаючи як державний, так і приватний сектори про характер і спрямованість таких операцій. Так, у період підготовки до виборів 2020 року представники ФБР і ЦРУ попереджали, що Росія знову спробує посилити поляризацію американського суспільства і втрутитися у виборчий процес. Крім того, розвідувальне співтовариство та адміністрація Байдена в режимі реального часу повідомляли про спроби дезінформації щодо COVID-19 та вторгнення в Україну. Такі кроки мають важливе значення, оскільки вони дозволяють не лише інформувати суспільство про наявні загрози, а й завчасно формувати сприйняття інформаційних операцій як

інструменту зовнішнього впливу. З метою громадського контролю та нагляду «директору Національної розвідки США у координації з міністром оборони було доручено створити в червні 2021 року Центр з аналізу загроз і даних соціальних медіа (Social Media Data and Threat Analysis Center)» [9, с. 96]. Вказаний напрям діяльності підтверджує, що в США значну увагу приділяють дослідженню зв'язку між активністю в соціальних мережах, зовнішнім втручанням і виникненням реальних політичних та безпекових ризиків.

Поза межами розвідувальних й інших органів виконавчої влади проблему інформаційної війни активно розглядав і Конгрес США. Через профільні комітети Сенату він проводив відкриті слухання щодо використання соціальних медіа у межах іноземних операцій впливу, акцентуючи увагу на тому, що йдеться не лише про окремі епізоди дезінформації, а про загрозу демократичним інститутам і виборчим процесам. Законодавчі ініціативи у цій сфері стосувалися насамперед підвищення прозорості джерел політичної реклами в мережі, удосконалення механізмів розкриття відомостей про замовників і поширювачів рекламних повідомлень, а також посилення підзвітності цифрових платформ у разі використання їхніх сервісів для іноземного втручання. Показовим у цьому відношенні є повторне внесення до Сенату законопроєкту Honest Ads Act, метою якого прямо визначено посилення прозорості й підзвітності онлайн-політичної реклами в інтересах захисту американської демократії та національної безпеки [210, с. 1–2].

Водночас у матеріалах американських аналітичних центрів і фахових доповідях наголошується, що протидія іноземному інформаційному впливу в США потребує широкої міжпартійної та міжінституційної взаємодії, однак така взаємодія ускладнюється високим рівнем внутрішньо-політичної поляризації. У цьому зв'язку цілком обґрунтованим є висновок, що навіть за відсутності повної нормативної завершеності відповідних рішень самі конгресові дискусії та слухання показали важливу особливість американського підходу: протидія інформаційній війні розглядається не лише

як завдання спеціалізованих органів, а і як питання широкої міжінституційної та суспільної відповідальності [223, с. 67].

Під тиском уряду, експертного середовища та громадськості приватні компанії США також поступово активізували свої зусилля у боротьбі з іноземними дезінформаційними кампаніями. Так, у своїх офіційних поясненнях до Сенату компанія Facebook прямо визнала, що діяла недостатньо швидко, і повідомила про посилення інвестицій у технологічні засоби виявлення шкідливого контенту, закриття фальшивих акаунтів, зменшення поширення неправдивих новин, а також запровадження нових правил прозорості реклами, обмежень на зміст рекламних матеріалів і додаткових вимог до покупців політичної реклами [227, с. 1]. Компанія Twitter, зі свого боку, інформувала Сенат про оновлення правил платформи, посилення виявлення та припинення координованої неавтентичної поведінки, видалення облікових записів, пов’язаних із зовнішніми інформаційними операціями, а також про запуск спеціального маркування акаунтів кандидатів на виборні посади і відкриття масивів даних для незалежних дослідників. У письмових свідченнях Google наголошувалося, що боротьба з дезінформацією у США неминуче пов’язана з необхідністю збереження балансу між захистом виборчого процесу, безпекою користувачів і свободою вираження поглядів [233, с. 1–2]. Саме в цьому виявляється одна з основних відмінностей між американським і європейським підходами: якщо в Європейському Союзі більш переважає регуляторний інструментарій, то у США держава значною мірою спирається на координацію, інформування, аналітичний супровід, співпрацю з приватним сектором та точкові механізми впливу, не виходячи за межі конституційно чутливої сфери свободи слова [214, с. 5; 224, с. 34].

Окремого висвітлення потребує роль кібербезпекового компонента у державній стратегії США щодо протидії інформаційній війні. Використання кіберзасобів для захисту критичної інфраструктури, інформаційних мереж, фінансового сектору, а також для протидії викраденню конфіденційної інформації здійснюється, зокрема, через діяльність U.S. Cyber Command

(USCYBERCOM). У звіті Government Accountability Office зазначено, що Cyber Mission Force становить операційну основу кіберсил, організованих під егідою USCYBERCOM, а її перша хвиля охоплювала 133 команди, які досягли повної оперативної готовності у травні 2018 року. У цьому ж звіті вказано, що команди CMF мають різне функціональне призначення: Combat Mission Teams і пов'язані з ними Combat Support Teams підтримують бойові командування й забезпечують наступальні кіберспроможності; National Mission Teams та Mission Support Teams захищають Сполучені Штати й їхні інтереси від кібератак значного масштабу; Cyber Protection Teams посилюють традиційні оборонні заходи й захищають пріоритетні мережі та системи Міністерства оборони США [204, с. 5]. Про певну стратегічну вагу цього напряму свідчить і бюджетування: обсяг cyber investments у складі бюджету становив 10,7468 млрд дол. США у FY2022, 11,6699 млрд дол. США у FY2023 та 13,452 млрд дол. США у FY2024 [209, с. 6].

Отже, узагальнення досвіду Європейського Союзу та Сполучених Штатів Америки має значення не лише для порівняльної характеристики підходів до протидії інформаційній війні, а й для виявлення тих організаційно-правових, інституційних та комунікаційних рішень, які можуть бути враховані під час вдосконалення державної стратегії України у цій сфері. Звернення до практики зарубіжних країн дає змогу окреслити, які механізми виявилися дієвими в умовах зростання дезінформаційного впливу, посилення зовнішнього втручання в інформаційний простір та ускладнення цифрових загроз. По-перше, в обох випадках інформаційна війна розглядається як самостійний і системний виклик державній безпеці, демократії, суспільній довірі та політичній стабільності. По-друге, результативна протидія їй неможлива лише шляхом спростування окремих неправдивих повідомлень. Необхідною є цілісна сукупність заходів, яка охоплює інституційну координацію, аналітичний моніторинг, правове регулювання, технологічну безпеку, взаємодію з цифровими платформами, підтримку незалежних медіа, фактчекінг і розвиток медіаграмотності. По-третє, європейський і

американський підходи мають спільну мету, проте відрізняються за своїми пріоритетами. Для Європейського Союзу більш характерною є опора на правове регулювання цифрового простору, підзвітність платформ, створення наднаціональних координаційних механізмів і посилення ролі фактчекерської та дослідницької спільноти. Для Сполучених Штатів Америки більш притаманний підхід, заснований на аналітичній діяльності, роботі розвідувального співтовариства, міжвідомчій взаємодії, співпраці з приватним сектором та використанні кібербезпекових інструментів.

2.2. Принципи та стратегічні засади формування державної стратегії протидії інформаційній війні

Формування державної стратегії протидії інформаційній війні має спиратися не на сукупність ситуативних рішень, а на цілісну систему принципів і стратегічних засад, що визначають зміст, межі, інструменти та порядок державної діяльності у відповідній сфері. Такий підхід випливає з конституційного статусу інформаційної безпеки: Основний Закон прямо відносить забезпечення інформаційної безпеки до найважливіших функцій держави, одночасно закріплюючи ідеологічну багатоманітність, заборону цензури, свободу думки і слова, а також вимогу, щоб органи державної влади діяли лише на підставі, в межах повноважень та у спосіб, передбачені Конституцією і законами України [74]. Отже, державна стратегія у цій сфері повинна поєднувати безпекову спрямованість із конституційними гарантіями свободи та правової визначеності.

Під принципами формування державної стратегії протидії інформаційній війні доцільно розуміти вихідні, нормативно й доктринально обумовлені засади, які визначають спрямованість державної політики, критерії відбору засобів впливу, допустимі межі втручання держави в інформаційну сферу та вимоги до взаємодії суб’єктів, задіяних у її реалізації [97, с. 34]. Їх призначення полягає в тому, щоб надати стратегії внутрішньої цілісності,

убезпечити її від відомчої фрагментарності та не допустити підміни протидії інформаційній агресії надмірними або неправомірними обмеженнями свободи вираження поглядів [96, с. 77]. Саме тому принципи в цій сфері мають бути не декларативними формулами, а реально діючими орієнтирами для нормотворення, стратегічного планування, міжвідомчої координації та практичного реагування на інформаційні загрози [97, с. 35]. Нормативне підґрунтя для такого підходу утворюють Конституція України, Закон України «Про інформацію», Закон України «Про медіа», Закон України «Про доступ до публічної інформації», Закон України «Про національну безпеку України», Стратегія національної безпеки України та Стратегія інформаційної безпеки.

Першим і визначальним принципом формування державної стратегії протидії інформаційній війні слід визнати верховенство права та законність. Значення цього принципу полягає в тому, що він визначає не лише загальну юридичну рамку діяльності держави, а й допустимі межі застосування будь-яких засобів впливу в інформаційній сфері [183, с. 22]. У сучасних умовах саме інформаційний простір є тією сферою, у якій перетинаються інтереси національної безпеки, свободи слова, права на інформацію, права на приватність, діяльності медіа, функціонування цифрових платформ і захисту персональних даних [99, с. 17]. За таких обставин будь-яке стратегічне рішення держави, спрямоване на протидію дезінформації, інформаційним операціям, пропагандистському впливу чи іншим формам інформаційної агресії, повинно бути не лише політично доцільним, а насамперед юридично обґрунтованим [183, с. 24]. Це означає, що засоби протидії інформаційній війні мають спиратися на чітко визначені норми Конституції та законів України, відповідати компетенції уповноважених суб’єктів, бути процедурно врегульованими та допускати перевірку їх законності у встановленому порядку.

Верховенство права у цій сфері передбачає, що держава не може діяти довільно, навіть за умови наявності реальних і масштабних інформаційних загроз. Воно вимагає, щоб будь-які обмежувальні або запобіжні заходи, які

застосовуються у межах державної стратегії, були передбачуваними для суспільства, заснованими на законі, пропорційними легітимній меті та такими, що не виходять за межі необхідного втручання. Інакше протидія інформаційній війні може сама стати джерелом порушення прав людини, зловживань владними повноваженнями або необґрунтованого звуження свободи інформаційної діяльності. Тому конституційна вимога, відповідно до якої органи державної влади та їх посадові особи зобов'язані діяти лише на підставі, у межах повноважень та у спосіб, що передбачені Конституцією і законами України, набуває у цій сфері особливої ваги [74]. У практичному вимірі це означає, що жоден орган не може самостійно розширювати обсяг своїх повноважень, встановлювати додаткові обмеження інформаційної діяльності або вдаватися до заходів реагування, які прямо не передбачені законом.

Поряд із цим принцип верховенства права та законності означає, що державна стратегія протидії інформаційній війні повинна бути внутрішньо узгодженою із загальною системою національного законодавства. Її зміст не може суперечити конституційним приписам щодо свободи думки і слова, заборони цензури, права на доступ до інформації, гарантій невтручання в особисте і сімейне життя чи захисту конфіденційної інформації про особу [120]. Відповідно, під час формування такої стратегії має враховуватися необхідність збалансування двох взаємопов'язаних потреб: з одного боку, потреби ефективного захисту держави, суспільства та громадян від деструктивного інформаційного впливу, а з другого – потреби збереження демократичного характеру правового режиму в інформаційній сфері. У зв'язку з чим, стратегія не може спиратися на позаправові, ситуативні або виключно політичні підходи, за яких критерії допустимості державного втручання залишаються нечіткими або визначаються довільно [96, с. 80]. Навпаки, вона повинна мати чітко окреслений нормативний фундамент, спиратися на визначені процедури ухвалення та реалізації рішень, а також передбачати механізми контролю, оскарження і перегляду дій держави.

Особливого значення цей принцип набуває також через те, що інформаційна війна часто спонукає державу діяти в умовах терміновості, високої суспільної напруги та підвищеного безпекового ризику. У таких умовах зростає небезпека підміни правових підходів логікою виключної доцільності, коли швидкість реагування починає сприйматися як достатня підстава для відступу від усталених юридичних вимог. Проте саме за обставин кризи верховенство права повинно зберігати своє визначальне значення, оскільки воно виконує стримувальну функцію щодо можливого надмірного втручання держави та водночас забезпечує довіру суспільства до законності відповідних заходів. Якщо дії держави у сфері протидії інформаційній війні є правово визначеними, прозорими за своїми підставами та здійснюються компетентними суб'єктами, це не лише підвищує їх легітимність, а й зміцнює авторитет державних інституцій у цілому [183, с. 29].

Другим базовим принципом формування державної стратегії протидії інформаційній війні є пріоритет прав і свобод людини. Його зміст полягає в тому, що будь-яка діяльність держави в інформаційній сфері має орієнтуватися не лише на захист публічних інтересів, а й на недопущення невиправданого звуження конституційних прав особи. Конституція України гарантує кожному право на свободу думки і слова, на вільне вираження своїх поглядів і переконань, а також право вільно збирати, зберігати, використовувати і поширювати інформацію. У зв'язку з цим державна стратегія протидії інформаційній війні не може будуватися на логіці безумовного пріоритету безпекових міркувань, оскільки інформаційна сфера є простором реалізації фундаментальних прав людини, а будь-яке надмірне втручання держави в цю сферу здатне поставити під загрозу самі засади демократичного ладу.

Разом із тим конституційне закріплення свободи інформаційної діяльності не означає її абсолютного характеру. Основний Закон допускає обмеження відповідних прав, але лише законом і лише в чітко визначених випадках, зокрема в інтересах національної безпеки, територіальної цілісності, громадського порядку, охорони здоров'я, захисту репутації чи прав інших

осіб, запобігання розголошенню конфіденційної інформації або для підтримання авторитету правосуддя [74]. Отже, під час формування державної стратегії протидії інформаційній війні визначальним є не механічне розширення інструментів обмеження, а пошук правомірного балансу між захистом держави від деструктивного інформаційного впливу та забезпеченням реального змісту прав і свобод людини. За такого підходу кожне можливе обмеження повинно бути законним, об'єктивно необхідним, пропорційним поставленій меті та належно мотивованим.

Важливим орієнтиром у цьому аспекті виступають і положення спеціального інформаційного законодавства. Закон України «Про інформацію» [128] та Закон України «Про медіа» закріплюють принципи гарантованості права на інформацію, відкритості, достовірності, свободи вираження поглядів і свободи поширення інформації, що має враховуватися під час вироблення стратегічних рішень у досліджуваній сфері [129]. Це означає, що державна стратегія протидії інформаційній війні повинна не лише містити механізми виявлення та нейтралізації інформаційних загроз, а й водночас забезпечувати збереження правового режиму, за якого особа не втрачає можливості вільно одержувати інформацію, формувати власну позицію та брати участь у суспільному обговоренні.

Третім принципом формування державної стратегії протидії інформаційній війні слід визнати ідеологічну багатоманітність і недопустимість цензури. Конституція України визначає, що суспільне життя ґрунтується на засадах політичної, економічної та ідеологічної багатоманітності, жодна ідеологія не може встановлюватися державою як обов'язкова, а цензура не допускається [74]. У площині досліджуваної проблематики такий конституційний припис має не декларативне, а безпосередньо прикладне значення, оскільки окреслює межі державного впливу на інформаційну сферу навіть за умов наявності реальних і масштабних інформаційних загроз.

За таких умов протидія ворожій пропаганді не може зводитися до нав'язування єдино допустимого способу сприйняття суспільно-політичних процесів або до звуження простору легальної публічної дискусії. Орієнтиром для держави має бути не придушення різноманітності думок, а захист національного інформаційного простору від деструктивного, маніпулятивного та підривного впливу, що спрямований на послаблення суверенітету, суспільної стійкості та довіри до інституцій влади [137]. Межа між правомірною протидією інформаційній агресії та надмірним адміністративним втручанням у сферу свободи слова є доволі тонкою, а тому потребує особливо виваженого нормативного й стратегічного підходу.

Зміст майбутньої державної стратегії повинен формуватися так, щоб охорона інформаційної безпеки не підміняла собою принципи демократичного устрою. Збереження конкурентності поглядів, можливості відкритого суспільного обговорення, права на критику влади та на висловлення альтернативної позиції має залишатися невід'ємною умовою функціонування правової держави навіть у період посилення інформаційного протиборства [1]. У цьому й полягає одна з найбільш складних вимог до державної стратегії протидії інформаційній війні: поєднати належний захист від ворожого інформаційного впливу з непорушністю конституційних засад ідеологічної багатоманітності та свободи публічного слова.

Четвертим принципом формування державної стратегії протидії інформаційній війні слід визнати достовірність, повноту та своєчасність офіційної інформації. Закон України «Про інформацію» відносить до основних принципів інформаційних відносин гарантованість права на інформацію, відкритість, доступність, свободу обміну інформацією, а також її достовірність і повноту [128]. Закон України «Про доступ до публічної інформації», у свою чергу, спрямований на забезпечення прозорості діяльності суб'єктів владних повноважень і створення належних правових механізмів реалізації права кожного на доступ до публічної інформації [120].

За умов інформаційного протиборства недостатньо лише реагувати на вже поширені фейки, маніпуляції чи дезінформаційні вкиди. Належний рівень інформаційної безпеки передбачає, що держава сама виступає постійним, авторитетним і зрозумілим джерелом перевіреної інформації, здатним оперативно пояснювати події, коментувати кризові ситуації та надавати суспільству орієнтири для правильного сприйняття обставин [137]. У випадку, коли офіційна інформація подається із запізненням, є неповною, суперечливою або надмірно формалізованою, у суспільстві виникає інформаційна невизначеність. Такий стан, як правило, швидко заповнюється чутками, емоційно забарвленими припущеннями, спекулятивними оцінками та ворожими наративами, що істотно послаблює стійкість інформаційного простору.

У зв’язку з цим достовірність, повнота та своєчасність офіційної інформації слід розглядати не як допоміжні характеристики державної комунікації, а як одну з базових опор усієї стратегії протидії інформаційній війні [128]. Значення має не лише сам факт поширення державою певних відомостей, а й рівень суспільної довіри до них, логічність їх викладу, внутрішня узгодженість та доступність для різних аудиторій [137].

П’ятим принципом слід визнати системність і міжвідомчу координацію. Стратегія інформаційної безпеки визначає своєю метою посилення спроможностей держави у сфері інформаційної безпеки, підтримку соціальної та політичної стабільності, оборони держави, захисту суверенітету та прав людини [137]. Досягнення цієї мети, відповідно до Стратегії, має здійснюватися, зокрема, шляхом створення ефективної системи взаємодії між органами державної влади, органами місцевого самоврядування та суспільством, а реалізація Стратегії забезпечується згідно з планом заходів, який затверджується Кабінетом Міністрів України [137]. Такий підхід свідчить, що формування державної стратегії не може відбуватися у межах одного відомства або одного функціонального блоку. Інформаційна війна охоплює безпековий, медійний, цифровий, дипломатичний, освітній та

регіональний напрями, тому системність і координація повинні закладатися у стратегію вже на етапі її підготовки.

Шостим принципом формування державної стратегії протидії інформаційній війні доцільно визначити стійкість та адаптивність держави і суспільства. Стратегія національної безпеки України відносить стійкість до числа базових засад державної політики у сфері безпеки, поряд зі стримуванням і взаємодією [136]. У її змісті стійкість пов'язується зі здатністю держави та суспільства швидко пристосовуватися до змін безпекового середовища, зберігати керованість, інституційну спроможність і належне функціонування навіть за умов посилення зовнішніх та внутрішніх загроз.

У зв'язку з цим державна стратегія не може будуватися лише як сукупність заходів оперативного реагування на окремі випадки дезінформації, інформаційних провокацій чи маніпулятивних кампаній. Її зміст має бути орієнтований на формування довготривалої спроможності державних інституцій, інформаційної інфраструктури та самого суспільства витримувати нові форми ворожого впливу без втрати внутрішньої стабільності [136]. Йдеться про здатність не лише виявляти й нейтралізувати конкретну загрозу, а й зменшувати вразливість до подальших інформаційних втручань, підтримувати довіру до офіційних джерел, забезпечувати безперервність державної комунікації та не допускати руйнування суспільної єдності під тиском зовнішніх інформаційних операцій.

Потреба в такому принципі пояснюється ще й тим, що сучасна інформаційна агресія постійно змінює канали поширення, технологічні засоби, цільові аудиторії та способи впливу на масову свідомість [137]. За відсутності належної адаптивності навіть добре виписана стратегія швидко втрачатиме практичну цінність, оскільки відставатиме від реальної динаміки загроз. З огляду на це стійкість і адаптивність слід розглядати не як бажану характеристику державної політики, а як одну з основних умов її дієвості, що визначає здатність України не лише реагувати на інформаційні виклики, а й

зберігати внутрішню цілісність в умовах тривалого інформаційного протиборства.

Сьомим принципом формування державної стратегії протидії інформаційній війні слід визнати взаємодію з міжнародними партнерами та інтегрованість у ширший безпековий контекст. Стратегія національної безпеки України розглядає взаємодію як одну з базових засад державної політики, пов'язуючи її з розвитком стратегічних відносин із ключовими іноземними партнерами, міжнародними організаціями та безпековими об'єднаннями [136]. Аналогічний підхід закладено і в Стратегії інформаційної безпеки, яка виходить із необхідності розбудови міжнародного співробітництва у сфері інформаційної безпеки на засадах партнерства та взаємної підтримки [137].

За таких умов державна стратегія протидії інформаційній війні не повинна обмежуватися лише внутрішніми механізмами реагування. Її зміст має враховувати міжнародний вимір поширення ворожих наративів, роботу іноземних інформаційних платформ, вплив пропагандистських кампаній на міжнародну громадську думку та потребу в системному донесенні української позиції до зовнішніх аудиторій. Важливого значення набувають обмін аналітичною інформацією з іноземними партнерами, вироблення спільних підходів до виявлення дезінформаційних мереж, координація зусиль у сфері стратегічних комунікацій, кібербезпеки та публічної дипломатії [59, с. 23]. Лише в такому форматі можливо ефективно протидіяти інформаційним впливам, які поширюються одночасно в різних країнах і розраховані не лише на українське, а й на міжнародне сприйняття [174, с. 5].

Міжнародна взаємодія у цій сфері має значення не тільки як зовнішньополітичний ресурс, а і як важлива умова підвищення внутрішньої стійкості держави. Підтримка партнерів, доступ до спільних аналітичних напрацювань, участь у міжнародних ініціативах з протидії дезінформації та узгодження комунікаційних підходів дозволяють Україні діяти в межах ширшої системи безпекової солідарності [78, с. 19]. З огляду на це

інтегрованість у міжнародний безпековий простір слід розглядати як необхідний елемент сучасної державної стратегії протидії інформаційній війні, без якого неможливо повною мірою врахувати реальний масштаб і характер сучасних інформаційних загроз.

Восьмим принципом є поєднання інформаційної та кібернетичної складових безпеки. Стратегія інформаційної безпеки прямо вказує, що питання, пов'язані з кібербезпекою, визначаються Стратегією кібербезпеки України [4]. Отже, вже на рівні чинного стратегічного регулювання закладено підхід, за яким протидія інформаційній війні не відокремлюється від кіберзахисту [6]. Це виправдано, оскільки сучасні інформаційні операції часто супроводжуються кібератаками, втручанням у цифрові канали зв'язку, спробами підриву довіри до державних електронних сервісів або компрометацією офіційних інформаційних ресурсів [92, с. 2]. Відтак, під час формування державної стратегії необхідно передбачати не паралельне, а узгоджене планування інформаційного й кібернетичного напрямів.

Поряд із принципами слід окремо виділити стратегічні засади формування державної стратегії протидії інформаційній війні, оскільки саме вони визначають її загальну логіку, місце у системі національної безпеки, зв'язок із чинним законодавством, порядок підготовки, реалізації та подальшого перегляду. На відміну від принципів, які відображають вихідні нормативні й ціннісні орієнтири державної діяльності, стратегічні засади характеризують уже більш прикладний і організаційний рівень побудови майбутнього документа. Вони дозволяють розкрити, якою саме має бути державна стратегія протидії інформаційній війні за своїм змістом, структурою, інституційним забезпеченням та функціональним призначенням [172, с. 70].

Передусім такою засадою є конституційно-безпекова природа державної стратегії протидії інформаційній війні. Конституція України прямо встановлює, що забезпечення інформаційної безпеки поряд із захистом суверенітету і територіальної цілісності є найважливішою функцією держави та справою всього Українського народу [74]. Водночас Конституція гарантує

свободу думки і слова, право вільно збирати, зберігати, використовувати й поширювати інформацію, а також забороняє цензуру та закріплює ідеологічну багатоманітність. Державна стратегія у цій сфері повинна формуватися як складова політики національної безпеки, але одночасно залишатися узгодженою з конституційними гарантіями свободи, відкритості та правової визначеності.

Другою стратегічною засадою є опора на систему стратегічного планування. У 2025 році Кабінет Міністрів України схвалив Концепцію національної системи стратегічного планування [143]. Для досліджуваної теми це означає, що нова державна стратегія протидії інформаційній війні має розроблятися не як політична декларація чи загальний програмний текст, а як повноцінний стратегічний документ із чітко визначеними цілями, виконавцями, строками, ресурсним забезпеченням, етапністю виконання та критеріями оцінювання результативності.

Третьою стратегічною засадою є спадкоємність і водночас оновлення нормативної рамки. Указ Президента України № 685/2021 затвердив Стратегію інформаційної безпеки, яка була розрахована на період до 2025 року [137]. Надалі Кабінет Міністрів України затвердив план заходів з її реалізації [124]. Отже, формування нової або оновленої державної стратегії повинно спиратися на вже напрацьований нормативний і практичний досвід, але не відтворювати попередні положення механічно [172, с. 71]. Її зміст має враховувати сучасну структуру загроз, досвід повномасштабної війни, розвиток цифрового середовища, роль соціальних платформ та зростання значення кіберскладової.

Четвертою стратегічною засадою слід визнати орієнтацію на чіткий механізм реалізації. Чинна Стратегія інформаційної безпеки закріплює координаційну роль Ради національної безпеки і оборони України, функції Кабінету Міністрів України щодо формування і реалізації державної інформаційної політики, а також участь інших суб’єктів у її виконанні. План заходів з реалізації Стратегії конкретизує цей організаційний вимір. Тому на

нашу думку, майбутня стратегія також повинна мати не лише змістовий, а й організаційно-виконавський характер: із визначенням порядку координації, міжвідомчої комунікації, розподілу функцій, регіональної участі та періодичного перегляду результативності [28].

П’ятою стратегічною засадою є міжсекторальний характер майбутньої стратегії. Інформаційна війна не обмежується медійною сферою, а одночасно впливає на національну безпеку, оборону, кіберзахист, дипломатію, освіту, культуру, діяльність органів державної влади та функціонування місцевого самоврядування.

Шостою стратегічною засадою є стійкість і адаптивність держави та суспільства. Стратегія національної безпеки України визначає стійкість як здатність суспільства і держави швидко адаптуватися до змін безпекового середовища й підтримувати стале функціонування. Для сфери інформаційної війни це означає, що державна стратегія має бути зорієнтована не лише на припинення окремих інформаційних атак, а й на формування довготривалої спроможності суспільства, державних інституцій і національного інформаційного простору протистояти деструктивним впливам. Саме тому в основу стратегії повинні закладатися не лише реактивні інструменти, а й заходи з підвищення суспільної стійкості, довіри до офіційної інформації, розвитку критичного мислення та підтримання сталої роботи державних комунікацій [158, с. 20].

Сьомою стратегічною засадою є поєднання інформаційної та кібернетичної складових безпеки. Під час формування державної стратегії протидії інформаційній війні необхідно виходити з єдності інформаційного та цифрового просторів [92, с. 2]. Сучасні інформаційні операції дедалі частіше поєднуються з кібератаками на державні інформаційні ресурси, втручанням у цифрові сервіси, спробами компрометації офіційних джерел інформації та порушенням роботи електронних комунікацій [174, с. 2].

Восьмою стратегічною засадою є доказовість та аналітична обґрунтованість. Формування державної стратегії протидії інформаційній

війні не може спиратися лише на політичні оцінки, загальні уявлення про загрози або одиничні резонансні випадки. Вона повинна ґрунтуватися на системному моніторингу інформаційного середовища, аналізі дезінформаційних кампаній, оцінюванні вразливостей державних інституцій, дослідженні поведінки цільових аудиторій і прогнозуванні майбутніх ризиків. Отже, майбутня стратегія повинна формуватися на основі перевірених аналітичних даних і допускати періодичне коригування залежно від зміни загрозливого середовища.

Дев'ятою стратегічною засадою є ресурсна забезпеченість. Будь-яка державна стратегія втрачає практичне значення, якщо для її виконання не визначено реальних інституційних, кадрових, фінансових, технологічних та інформаційних ресурсів. У контексті протидії інформаційній війні це має особливе значення, оскільки йдеться про потребу в професійних аналітичних структурах, технічному захисті інформації, сучасних комунікаційних інструментах, освітніх програмах, цифрових засобах моніторингу та належній підготовці персоналу.

Десятою стратегічною засадою є міжнародна взаємодія та зовнішньополітичний вимір. Стратегія національної безпеки України визначає взаємодію як одну з базових засад державної політики безпеки. Стратегія інформаційної безпеки окремо наголошує на розвитку міжнародної співпраці у сфері інформаційної безпеки на засадах партнерства і взаємної підтримки. Це означає, що державна стратегія протидії інформаційній війні не повинна бути орієнтована лише на внутрішнє інформаційне середовище [172, с. 80]. Вона має враховувати й потребу у формуванні позитивного міжнародного образу України, доведенні до іноземних аудиторій достовірної інформації про російську агресію, спільному виявленні та фіксації інформаційних операцій, а також координації дій із міжнародними партнерами у сфері стратегічних комунікацій і кібербезпеки.

Одинадцятою стратегічною засадою доцільно визначити регіональну та суспільну включеність. Чинна Стратегія інформаційної безпеки пов'язує

досягнення її мети зі створенням ефективної системи взаємодії між органами державної влади, органами місцевого самоврядування та суспільством. Тобто, це означає, що формування майбутньої державної стратегії не може відбуватися без урахування регіональних особливостей, місцевих інформаційних вразливостей і ролі громадянського суспільства [78, с. 27]. Оскільки значна частина ворожих інформаційних кампаній спрямовується саме на локальні спільноти, окремі соціальні групи чи суспільно чутливі теми, майбутня стратегія повинна передбачати як загальнодержавну координацію, так і спроможність швидко реагувати на місцевому рівні.

Отже, стратегічні засади формування державної стратегії протидії інформаційній війні мають значно ширший зміст, ніж простий перелік загальних орієнтирів. Вони охоплюють конституційно-безпекову природу такої стратегії, її включеність у систему стратегічного планування, спадкоємність та оновлення нормативної рамки, орієнтацію на чіткий механізм реалізації, міжсекторальність, стійкість і адаптивність, єдність інформаційної та кібернетичної складових, аналітичну обґрунтованість, ресурсну забезпеченість, міжнародну взаємодію та регіонально-суспільну включеність. Саме сукупність цих засад дає підстави розглядати державну стратегію протидії інформаційній війні не як вузький інструмент комунікаційної політики, а як комплексний документ безпекового, правового, управлінського та суспільного значення, покликаний забезпечити довготривалу стійкість держави до інформаційної агресії.

2.3. Інституційний механізм формування та реалізації державної стратегії протидії інформаційній війні

У сучасних умовах інформаційна війна перетворилася на один із основних засобів дестабілізації державності, впливу на суспільну свідомість, підриву легітимності органів влади, деморалізації населення та послаблення здатності держави до організованого опору зовнішнім і внутрішнім загрозам [186, с. 29]. Її специфіка полягає в тому, що руйнівний вплив здійснюється не

лише через поширення неправдивої або маніпулятивної інформації, а й через системне формування недовіри до державних інституцій, знецінення національних інтересів, спотворення фактів, нав’язування вигідних агресору інтерпретацій подій, а також через цілеспрямоване послаблення інформаційного суверенітету держави. За таких умов протидія інформаційній війні не може обмежуватися окремими реактивними заходами, епізодичними комунікаційними кампаніями чи фрагментарними рішеннями окремих органів влади. Вона потребує цілісного, внутрішньо узгодженого та функціонально організованого інституційного механізму, здатного забезпечити формування і подальшу реалізацію державної стратегії у цій сфері [137].

Питання інституційного забезпечення державної політики набуває особливого значення саме тоді, коли йдеться про складні, багаторівневі та міжгалузеві загрози. Інформаційна війна належить саме до таких явищ, оскільки вона одночасно стосується національної безпеки, публічного управління, інформаційної політики, оборонної сфери, освіти, культури, кібербезпеки, міжнародної комунікації та захисту прав людини [154–155]. У цьому випадку потрібна скоординована система суб’єктів, повноважень, форм взаємодії, процедур ухвалення рішень, засобів контролю, способів обміну інформацією та механізмів відповідальності, тобто те, що в науковому значенні доцільно визначати як інституційний механізм [71, с. 52].

Під інституційним механізмом формування та реалізації державної стратегії протидії інформаційній війні доцільно розуміти цілісну, нормативно та організаційно впорядковану систему державних органів, інших уповноважених суб’єктів, процедур, способів взаємодії, управлінських зв’язків і функціональних засобів, за допомогою яких виробляються, узгоджуються, впроваджуються та оцінюються стратегічні рішення держави, спрямовані на запобігання, виявлення, нейтралізацію та мінімізацію наслідків інформаційних загроз [180, с. 61]. Таке визначення дозволяє відійти від надто вузького розуміння цього явища лише як сукупності органів державної влади. Насправді інституційний механізм охоплює не тільки суб’єктний склад, а й

порядок їхньої діяльності, спосіб зв’язку між ними, розподіл компетенції, логіку вироблення рішень і практику їх втілення.

Наукове осмислення інституційного механізму неможливе без розмежування понять «інституція», «механізм», «державна стратегія» та «реалізація». Інституція у даному контексті означає не лише формально створений орган чи установу, а й стале правило організації владної діяльності, закріплений порядок взаємодії, компетенційний центр, на який покладено певний обсяг функцій [170–171]. Відповідно механізм не зводиться до простого переліку структур, а вказує на впорядкованість їх діяльності, взаємообумовленість дій, функціональну єдність і спрямованість на досягнення визначеної мети [180, с. 58].

У сфері протидії інформаційній війні інституційний механізм має декілька взаємопов’язаних вимірів. По-перше, це суб’єктний вимір, тобто коло органів та інших учасників, які наділені відповідними повноваженнями або залучаються до реалізації державної стратегії. По-друге, це функціональний вимір, який охоплює основні напрями їхньої діяльності: аналітичний, нормотворчий, координаційний, комунікаційний, контрольний, освітній, превентивний та міжнародний. По-третє, це процедурний вимір, що включає порядок вироблення рішень, обігу інформації, погодження позицій, реагування на загрози, моніторингу результативності та коригування стратегічних підходів. По-четверте, це ресурсний вимір, у межах якого йдеться про кадрове, інформаційне, технічне, фінансове та організаційне забезпечення функціонування всієї системи. По-п’яте, це ціннісний вимір, оскільки будь-яка державна стратегія протидії інформаційній війні повинна ґрунтуватися не лише на міркуваннях безпеки, а й на засадах верховенства права, поваги до прав людини, законності, пропорційності та недопущення зловживання владними повноваженнями [71, с. 52].

Важливо враховувати, що інституційний механізм не існує відокремлено від загальної системи державного управління. Навпаки, він є її спеціальним складником, пристосованим до розв’язання конкретного комплексу завдань.

Його особливість полягає не в автономності, а в цільовій спрямованості. У сфері протидії інформаційній війні такий механізм повинен забезпечувати безперервний цикл стратегічної діяльності: від виявлення загроз і вироблення державної позиції до практичного впровадження заходів, оцінки їх ефективності та вдосконалення підходів залежно від зміни безпекового середовища. Якщо хоча б одна з цих ланок не функціонує належним чином, уся система втрачає внутрішню цілісність, а стратегія набуває декларативного характеру [18, с. 76].

Для глибшого розуміння архітектоніки зазначених процесів та забезпечення системності державного управління у цій сфері нами розроблено структурно-функціональну модель формування та реалізації державної стратегії протидії інформаційній війні (Рис. 1, додатки).

Запропонована модель базується на інтеграції трьох взаємопов'язаних рівнів, що дозволяє подолати традиційну фрагментарність безпекових заходів.

Інституційний рівень (суб'єктна вертикаль) — визначає ієрархію та межі відповідальності органів публічної влади: від стратегічного (Президент, РНБО) до виконавчого (МКСК, ЦПД) та партнерського (громадянське суспільство) секторів.

Функціонально-процесуальний рівень (динамічний алгоритм) — відображає послідовність управлінських дій: від предиктивного моніторингу семантичного простору із застосуванням Big Data до активної нейтралізації загрози та контрпропаганди.

Організаційно-управлінський рівень (цикл резильєнтності) — забезпечує безперервність процесу через постійний контроль KPI, оцінювання результативності та корекцію стратегічних цілей залежно від зміни характеру гібридних загроз.

Така тривимірна архітектура моделі забезпечує перехід від лінійного адміністрування до екосистемного захисту інформаційного суверенітету, де кожен елемент підсилює загальну стійкість (резильєнтність) держави.

Необхідність саме інституційного підходу до аналізу державної стратегії протидії інформаційній війні обумовлена тим, що інформаційна загроза має не разовий, а тривалий, адаптивний і багатоканальний характер [186, с. 32]. Агресор здатний змінювати форми подання дезінформації, комбінувати медійні, цифрові, психологічні та політичні засоби впливу, використовувати внутрішні суперечності суспільства, експлуатувати чутливі теми та впроваджувати потрібні йому наративи через різні інформаційні платформи [137]. За таких умов держава не може діяти виключно ситуативно. Вона повинна мати наперед визначену стратегічну лінію, а її реалізація має забезпечуватися не тимчасовими рішеннями, а стійкою системою владно-організаційних зв'язків, яка не втрачає своєї дієздатності залежно від кадрових змін, політичної кон'юнктури чи окремих кризових обставин.

У цьому зв'язку доцільно підкреслити, що інституційний механізм формування державної стратегії і інституційний механізм її реалізації хоча й становлять єдиний процес, однак не є тотожними. Формування стратегії передбачає насамперед аналітичне виявлення загроз, прогнозування ризиків, визначення цілей, завдань, принципів, пріоритетів і засобів державної дії [148, с. 53–54]. Реалізація стратегії пов'язана вже з практичним втіленням визначених рішень, координацією виконавців, розподілом ресурсів, організацією комунікації, здійсненням контролю та оцінюванням результатів [70]. Отже, інституційний механізм має забезпечувати обидва напрями: стратегічне вироблення рішень і їх послідовне втілення. Якщо держава спроможна сформулювати стратегічні цілі, але не здатна створити належну систему їх реалізації, така стратегія не виконує свого призначення. Водночас практична діяльність без чітко окресленої стратегії породжує хаотичність, дублювання повноважень, конкуренцію між інституціями та зниження загальної результативності.

Сутність інституційного механізму виявляється також через його ознаки. По-перше, він має системний характер, тобто складається із взаємозалежних елементів, що діють у межах спільного функціонального поля

[108, с. 69–70]. По-друге, він має владно-організаційну природу, оскільки пов’язаний із реалізацією компетенції уповноважених суб’єктів і прийняттям обов’язкових для виконання рішень [130]. По-третє, для нього характерна нормативна визначеність, адже функціонування інституційного механізму повинно спиратися на норми права, які встановлюють повноваження, процедури, межі втручання та гарантії законності. По-четверте, він є цільовим, оскільки спрямований на досягнення конкретного публічного результату – захист національного інформаційного простору та забезпечення стійкості держави до інформаційних впливів [137]. По-п’яте, він має динамічний характер, бо повинен адаптуватися до зміни загроз, способів інформаційного впливу та технологічного середовища [111, с. 117–118].

Окремої уваги потребує питання співвідношення інституційного механізму з правовим, організаційним та функціональним механізмами. У науковій літературі ці категорії часто використовуються паралельно, проте між ними існують певні відмінності [14; 33; 63; 216]. Правовий механізм відображає передусім сукупність нормативних засобів регулювання суспільних відносин; організаційний (побудову структур, розподіл компетенції та порядок здійснення управлінської діяльності); функціональний напрями та способи практичного впливу на відповідну сферу [64]. Інституційний механізм є ширшим поняттям, оскільки поєднує ці складники через діяльність конкретних суб’єктів та усталені правила їх взаємодії. Саме тому в межах дослідження державної стратегії протидії інформаційній війні доцільно оперувати саме категорією інституційного механізму, яка дозволяє охопити і суб’єктний склад, і компетенційний розподіл, і процедурну сторону, і фактичну практику реалізації владних рішень [108, с. 70].

Зміст інституційного механізму у досліджуваній сфері розкривається через сукупність його основних елементів. Першим елементом є інституційна основа, тобто сукупність органів державної влади та інших уповноважених суб’єктів, які беруть участь у формуванні та реалізації державної стратегії. Другим – компетенційна основа, що визначає межі, обсяг і характер

повноважень кожного з них [130]. Третім – комунікаційна основа, яка охоплює порядок міжвідомчої взаємодії, обміну даними, узгодження спільних рішень і доведення інформації до населення. Четвертим – аналітична основа, що забезпечує виявлення інформаційних загроз, оцінювання ризиків і вироблення рішень на основі достовірних даних [70]. П’ятим – контрольна основа, яка включає моніторинг виконання стратегії, оцінювання результативності та реагування на виявлені недоліки [137]. Шостим – кадрова основа, оскільки жоден інституційний механізм не може бути дієздатним без належно підготовлених фахівців, здатних працювати у сфері стратегічних комунікацій, інформаційної безпеки, аналітики, публічного управління та правового забезпечення.

Особливо важливим є те, що інституційний механізм формування та реалізації державної стратегії протидії інформаційній війні повинен мати не лише вертикальний, а й горизонтальний вимір [66]. Вертикальний вимір виражається у підпорядкованості, розмежуванні рівнів управління, прийнятті політичних і управлінських рішень, а також у забезпеченні їх виконання [130]. Горизонтальний вимір пов’язаний із міжвідомчою взаємодією, координацією діяльності різних органів, обміном інформацією, узгодженням підходів і залученням недержавних учасників до спільного виконання стратегічних завдань [137]. У сфері протидії інформаційній війні саме горизонтальні зв’язки набувають особливої ваги, оскільки жоден орган не володіє повним обсягом інструментів для нейтралізації всіх видів інформаційних загроз [108, с. 70–71]. Відтак недостатність координації, розірваність інформаційних потоків, дублювання функцій або відсутність єдиної стратегічної позиції суттєво послаблюють спроможність держави до ефективної протидії.

При цьому не слід ототожнювати інституційний механізм лише з системою державних органів. Для його належного функціонування важливе значення можуть мати й інші учасники: наукові установи, експертні центри, суб’єкти у сфері медіа, заклади освіти, структури громадянського суспільства, платформи фактчекінгу, професійні об’єднання та інші інституції, діяльність

яких здатна посилювати державну спроможність у цій сфері [70]. Однак їх участь не змінює того, що саме держава повинна залишатися організуючим центром такої діяльності, оскільки лише вона наділена владними повноваженнями щодо формування стратегії, офіційного визначення пріоритетів, координації суб'єктів і забезпечення загальнообов'язкового виконання відповідних рішень.

Отже, інституційний механізм формування та реалізації державної стратегії протидії інформаційній війні слід розглядати як одну з передумов результативної державної політики у сфері інформаційної безпеки [108, с. 69]. Його значення полягає в тому, що він забезпечує перехід від загальних декларацій до впорядкованої системи практичної дії, у межах якої кожен суб'єкт має визначене місце, функції, обсяг повноважень і відповідальності. Завдяки цьому стає можливим не лише формулювання державної стратегії, а й її послідовне впровадження, коригування та оцінювання в умовах постійної зміни інформаційних загроз. Відтак подальший науковий аналіз цієї проблематики доцільно спрямувати на з'ясування того, які саме суб'єкти утворюють зазначений інституційний механізм, яким є характер їхньої взаємодії та які структурні недоліки перешкоджають формуванню цілісної та дієвої державної стратегії протидії інформаційній війні.

З'ясування кола суб'єктів інституційного механізму формування та реалізації державної стратегії протидії інформаційній війні має не лише теоретичне, а й прикладне значення. Без чіткого визначення того, хто саме виробляє стратегічні рішення, хто забезпечує їх нормативне оформлення, хто координує їх виконання, хто здійснює моніторинг загроз, а хто безпосередньо втілює відповідні заходи у практичній площині, державна стратегія неминуче залишається декларативною. Стратегія інформаційної безпеки України прямо виходить із того, що забезпечення інформаційної безпеки є однією з найважливіших функцій держави, а досягнення її мети пов'язується зі створенням ефективної системи взаємодії між органами державної влади, органами місцевого самоврядування та суспільством. Водночас чинна

Стратегія інформаційної безпеки була розрахована на період до 2025 року, що додатково актуалізує питання переосмислення суб'єктного складу майбутнього стратегічного документа та уточнення ролі кожного учасника відповідного механізму.

На нашу думку, суб'єкти інституційного механізму у досліджуваній сфері доцільно поділяти не лише за формальною належністю до певної гілки влади, а передусім за їх функціональним призначенням [30]. У такому разі можна виокремити суб'єктів стратегічно-політичного рівня, які визначають основні орієнтири державної політики та забезпечують її легітимацію; суб'єктів координаційно-управлінського рівня, що перетворюють політичні рішення на систему виконавських заходів; суб'єктів спеціального та безпекового рівня, які виявляють, аналізують і нейтралізують загрози; суб'єктів регуляторно-комунікаційного рівня, що забезпечують стійкість інформаційного простору, офіційні комунікації держави та протидію дезінформації; а також допоміжних суб'єктів, участь яких не має владного характеру, однак є важливою для результативності всієї системи [108, с. 70–71].

Першою та визначальною групою є суб'єкти стратегічно-політичного рівня. До них насамперед належать Верховна Рада України, Президент України та Рада національної безпеки і оборони України. Їх роль є фундаментальною, оскільки саме на цьому рівні закладаються нормативні, політичні та інституційні рамки державної відповіді на інформаційну агресію. Верховна Рада України формує законодавче підґрунтя для реалізації стратегії, приймаючи акти, що стосуються національної безпеки, медіарегулювання, кібербезпеки, захисту інформації та функціонування інформаційної сфери. Саме парламент ухвалив, зокрема, Закон України «Про національну безпеку України» та Закон України «Про медіа», без яких будь-яка державна стратегія протидії інформаційній війні не мала б належної правової основи. Разом із тим Верховна Рада не повинна розглядатися лише як орган, що ухвалює закони. У межах інституційного механізму вона виконує значно ширшу роль, оскільки

забезпечує демократичну легітимацію державної політики, здійснює контроль за діяльністю виконавчих органів та визначає бюджетні пріоритети у відповідній сфері.

Центральне місце у формуванні державної стратегії посідає Президент України як глава держави та Голова Ради національної безпеки і оборони України. Указ Президента України від 28 грудня 2021 року № 685/2021 увів у дію рішення РНБО від 15 жовтня 2021 року «Про Стратегію інформаційної безпеки» і одночасно затвердив саму Стратегію. У цьому ж акті контроль за виконанням рішення було покладено на Секретаря Ради національної безпеки і оборони України [137]. Отже, Президент у даному механізмі виступає не лише суб'єктом формального затвердження стратегічного документа, а й конституційним центром, через який стратегічне рішення набуває загальнообов'язкового характеру для всієї системи публічної влади. Через Президента стратегія переходить із площини міжвідомчого погодження у площину загальнодержавного курсу [40, с. 12].

Рада національної безпеки і оборони України є основним координаційно-стратегічним суб'єктом у межах досліджуваного механізму. По суті, саме РНБО виступає інституцією, де відбувається узгодження безпекового, політичного, інформаційного та управлінського вимірів державної політики. Не випадково Стратегія інформаційної безпеки була затверджена саме через рішення цього органу [137]. Значення РНБО полягає в тому, що вона забезпечує концентрацію аналітичної інформації, міжвідомчу координацію, вироблення комплексних рішень і можливість пов'язати питання інформаційної війни із загальною системою національної безпеки [105, с. 68]. Інформаційні загрози у сучасних умовах майже ніколи не існують окремо від кіберзагроз, розвідувальної активності, санкційної політики, дипломатичного протистояння та внутрішньої політичної стабільності [194, с. 409].

Наступну групу становлять суб'єкти координаційно-управлінського рівня, насамперед Кабінет Міністрів України. Особливість уряду полягає в

тому, що він займає проміжне, але визначальне місце між стратегічним задумом і його практичним втіленням [112, с. 27]. Із тексту рішення про Стратегію інформаційної безпеки випливає, що проект цього документа був внесений Кабінетом Міністрів України. Це означає, що саме уряд виступає базовим суб'єктом підготовки змісту стратегічних рішень, їх міжвідомчого узгодження та подальшого виконавського забезпечення. Крім того, уряд у 2025 році схвалив Концепцію національної системи стратегічного планування, що засвідчує його провідну роль у побудові загальної логіки формування, моніторингу та коригування державних стратегій. У контексті протидії інформаційній війні Кабінет Міністрів має значення як центр розподілу виконавчих завдань, затвердження операційних планів, визначення відповідальних органів і ресурсного забезпечення їх діяльності.

Слід підкреслити, що урядова ланка у цій сфері не зводиться до технічного адміністрування. Саме Кабінет Міністрів спроможний перетворити загальну політичну тезу про необхідність протидії інформаційній війні на послідовну систему виконавських дій: від розподілу компетенції між центральними органами виконавчої влади до запровадження конкретних комунікаційних, освітніх, цифрових, аналітичних і безпекових заходів. Без урядової координації навіть найбільш якісно сформульована стратегія залишатиметься нормативною декларацією [40, с. 19]. Тому Кабінет Міністрів є головним суб'єктом операціоналізації державної стратегії у досліджуваній сфері.

Особливе місце в урядовому блоці посідає Міністерство культури та стратегічних комунікацій України. На момент функціонування цього найменування воно визначалося урядом як центральний орган виконавчої влади у відповідній сфері, а його інституційна присутність у проблематиці інформаційної війни підсилювалася саме напрямом стратегічних комунікацій. У жовтні 2025 року це міністерство було перейменоване на Міністерство культури України [133]. В умовах російської інформаційної агресії значення цього органу виходило далеко за межі традиційного гуманітарного

адміністрування. Його компетенція у практичній площині охоплювала державні комунікації, смислову консолідацію, просування українського наративу, протидію дезінформації, підтримку стійкості суспільства до маніпулятивних впливів та взаємодію з міжнародними партнерами у сфері інформаційної безпеки [106, с. 70].

У структурі цього напряму особливої уваги заслуговує Центр стратегічних комунікацій та інформаційної безпеки. На урядовому рівні повідомлялося, що у січні 2025 року було завершено його державну реєстрацію як державної установи [91]. У матеріалах, пов'язаних із діяльністю цього напряму та порталу SPRAVDI, наголошувалося на комунікаційній протидії зовнішнім загрозам, насамперед інформаційним атакам Російської Федерації, а також на розбудові сталих державних комунікацій і стійкості суспільства до дезінформації. Це дає підстави відносити Центр не до периферійних комунікаційних структур, а до окремого спеціалізованого суб'єкта інституційного механізму. Його місія полягає не у виробленні політичних рішень найвищого рівня, а у щоденній аналітичній, просвітницькій, роз'яснювальній та контрпропагандистській роботі, без якої неможлива реалізація будь-якої державної стратегії протидії інформаційній війні [22, с. 139].

До суб'єктів спеціального і безпекового рівня слід віднести насамперед Службу безпеки України, розвідувальне співтовариство, Державну службу спеціального зв'язку та захисту інформації України, а також створений при РНБО Центр протидії дезінформації. Роль Служби безпеки України у цій системі обумовлена її призначенням щодо захисту державного суверенітету, конституційного ладу та інших життєво важливих інтересів держави [141]. У сучасних умовах інформаційна війна майже завжди супроводжується елементами підривної діяльності, спеціальними інформаційними операціями, кібератаками, спробами впливу на критичну інфраструктуру та використанням ворожих мереж для дестабілізації внутрішньої ситуації. СБУ у межах цього механізму виконує не стільки комунікаційну, скільки

контррозвідувальну, безпекову та захисну функцію. Законодавство у сфері кібербезпеки також прямо пов’язує систему реагування на кіберзагрози із безпековими та контррозвідувальними суб’єктами.

Не менш важливою є роль розвідувального співтовариства. Закон України «Про розвідку» визначає, що в Україні функціонує розвідувальне співтовариство, до суб’єктів якого належать координаційний орган з питань розвідки, розвідувальні органи, Служба безпеки України та інші складові сектору безпеки і оборони, визначені РНБО [140]. У цьому ж законі передбачено, що загальна координація діяльності суб’єктів розвідувального співтовариства здійснюється РНБО. Для теми інформаційної війни це має принципове значення, оскільки ефективна стратегія неможлива без розвідувальної інформації про наміри, інструменти, наративи, канали поширення дезінформації та вразливості, які використовує противник. Розвідка в цій площині забезпечує не публічну комунікацію, а своєчасне попередження, аналітичне передбачення та інформаційну основу для ухвалення стратегічних рішень.

У сфері цифрової безпеки одним із основних суб’єктів є Державна служба спеціального зв’язку та захисту інформації України. Законодавство у сфері кібербезпеки прямо пов’язує з нею діяльність CERT-UA як національної команди реагування на кіберінциденти, кібератаки та кіберзагрози. Після змін 2025 року роль Держспецзв’язку була ще чіткіше окреслена у сфері формування та реалізації державної політики з кіберзахисту державних інформаційних ресурсів і критичної інфраструктури [119]. У листопаді 2025 року уряд затвердив спеціальний порядок взаємодії суб’єктів національної системи реагування на кіберінциденти із правоохоронними, контррозвідувальними та розвідувальними органами [125]. Це свідчить, що у сучасних умовах Держспецзв’язку є одним із центральних суб’єктів тієї частини інституційного механізму, яка відповідає за технічну стійкість держави до інформаційних і кібернетичних атак.

Поряд із Держспецзв'язку важливим виконавцем цифрового напряму виступає Міністерство цифрової трансформації України. Його положення затверджене постановою Кабінету Міністрів України у 2019 році [113]. У контексті протидії інформаційній війні значення Мінцифри полягає в забезпеченні цифрової стійкості державних сервісів, електронних реєстрів, хмарної інфраструктури, електронної ідентифікації, безпеки електронних довірчих послуг та захисту державних даних від кібернетичного впливу. Хоча Міністерство цифрової трансформації не є органом, що самостійно формує політичний зміст інформаційної стратегії, воно створює критично важливі технічні умови для її реалізації, а відтак має розглядатися як один із базових суб'єктів виконавського блоку [40, с. 20].

Окремим спеціалізованим суб'єктом є Центр протидії дезінформації при РНБО. Рішення про його створення було ухвалене Радою національної безпеки і оборони України у березні 2021 року, а вже 19 березня 2021 року Указом Президента України № 106/2021 це рішення було введене в дію. На офіційному ресурсі Центру зазначено, що до його основних завдань належать аналіз і моніторинг подій та явищ в інформаційному просторі України, стану інформаційної безпеки, виявлення та протидія дезінформації, а також підготовка пропозицій щодо забезпечення інформаційної безпеки України [145]. Наявність цього органу засвідчує інституційне визнання того, що дезінформація є не побічним комунікаційним явищем, а самостійною безпековою загрозою, яка потребує окремого центру аналізу, оцінювання, реагування та міжвідомчої координації. На відміну від Центру стратегічних комунікацій та інформаційної безпеки, який виконує передусім урядово-комунікаційну і просвітницьку функцію, Центр протидії дезінформації має значно виразніший безпеково-аналітичний характер.

Суттєве значення у структурі інституційного механізму має і регуляторно-медійний блок. Його ядро становлять Національна рада України з питань телебачення і радіомовлення та Суспільне медіа України. Закон України «Про медіа» закріплює сучасне правове підґрунтя регулювання

відповідної сфери. Закон України «Про суспільні медіа України» визначає правові основи діяльності Національної суспільної телерадіокомпанії України [142]. У контексті протидії інформаційній війні ці суб'єкти мають подвійну роль. З одного боку, вони забезпечують підтримання належного правового порядку в медіасфері, стримування порушень законодавства та підвищення стандартів відповідального мовлення. З другого боку, вони формують частину національної інформаційної стійкості, оскільки наявність професійного, незалежного й довіреного медійного середовища є однією з передумов зменшення ефективності ворожої дезінформації [22, с. 141].

У ширшому інституційному розумінні до системи суб'єктів слід віднести також зовнішньополітичний і міжнародний напрям держави. Стратегія інформаційної безпеки прямо вказує на розвиток міжнародної співпраці у сфері інформаційної безпеки на засадах партнерства та взаємної підтримки як один із шляхів досягнення її мети. Звідси випливає, що зовнішньополітичний блок держави, дипломатичні представництва, органи, відповідальні за комунікацію з міжнародними партнерами, а також суб'єкти, що представляють Україну у міжнародних форматах зі стратегічних комунікацій, не можуть залишатися поза межами інституційного механізму [46, с. 22]. Хоча їх функція має іншу природу, ніж у національних безпекових чи регуляторних органів, вона є надзвичайно важливою для доведення української позиції на зовнішню аудиторію, нейтралізації ворожих наративів за кордоном та формування міжнародної підтримки державної політики у сфері протидії інформаційній агресії [105, с. 72]. Тут ми маємо справу з органічним продовженням внутрішньої стратегії на зовнішньому рівні.

Не менш важливо, що Стратегія інформаційної безпеки прямо пов'язує досягнення її мети зі створенням ефективної системи взаємодії між органами державної влади, органами місцевого самоврядування та суспільством. Отже, органи місцевого самоврядування, регіональні комунікаційні структури, місцеві центри реагування на кризові інформаційні ситуації, а також інститути громадянського суспільства не можуть розглядатися як зовнішні щодо цього

механізму. Їх участь є допоміжною за правовою природою, але в багатьох випадках критично важливою за практичним значенням [20, с. 14]. Російська інформаційна агресія часто спрямовується на локальні спільноти, прикордонні регіони, окремі соціальні групи і теми місцевого життя [46, с. 23]. За таких умов централізованої державної комунікації недостатньо. Необхідні розгалужені канали доведення перевіреної інформації, зворотного зв'язку та швидкого спростування маніпуляцій на місцях [20, с. 15]. Саме тому місцевий та суспільний рівні повинні інтегруватися в єдину логіку державної стратегії, а не залишатися поза нею.

Водночас участь недержавних суб'єктів (наукових установ, експертних центрів, професійних медійних об'єднань, закладів освіти, аналітичних спільнот) не повинна тлумачитися як розмивання ролі держави. Навпаки, саме наявність у держави координаційного та стратегічного центру дозволяє ефективно залучати їх потенціал [77, с. 151]. Досвід діяльності Центру стратегічних комунікацій та інформаційної безпеки, який декларує співпрацю з громадським сектором, показує, що сучасна протидія дезінформації потребує поєднання владних рішень, професійної аналітики, наукового супроводу, громадської довіри та освітньої роботи [178]. Однак інтеграція таких суб'єктів повинна відбуватися не стихійно, а через чіткі процедури взаємодії, зрозумілі критерії відповідальності та узгодженість із державними стратегічними цілями.

Отже, інституційний механізм формування та реалізації державної стратегії протидії інформаційній війні в Україні має багаторівневий і поліцентричний характер. Його ядро становлять Верховна Рада України, Президент України та РНБО як суб'єкти політичного, нормативного й стратегічного спрямування; Кабінет Міністрів України – як основний суб'єкт перетворення стратегічних рішень на систему виконавських заходів; Міністерство культури та стратегічних комунікацій України, Центр стратегічних комунікацій та інформаційної безпеки, Міністерство цифрової трансформації України, Держспецзв'язку, Служба безпеки України, суб'єкти

розвідувального співтовариства та Центр протидії дезінформації – як виконавці спеціальних, аналітичних, комунікаційних, технічних і безпекових функцій; Національна рада України з питань телебачення і радіомовлення та Суспільне медіа України – як суб'єкти регуляторно-медійного впливу; органи місцевого самоврядування, наукові інституції та громадянське суспільство – як допоміжний, але необхідний елемент практичної стійкості системи [20, с. 13]. Недоліки у взаємодії між цими суб'єктами, нечіткість розмежування їх повноважень або відсутність єдиного центру координації неминуче послаблюють державну здатність до протидії інформаційній війні. Відповідно наступним кроком дослідження має бути аналіз повноважень, форм взаємодії та проблем функціонування цієї системи з метою обґрунтування напрямів її вдосконалення.

Після визначення кола суб'єктів інституційного механізму формування та реалізації державної стратегії протидії інформаційній війні закономірно постає питання про зміст їхніх повноважень, способи взаємодії між ними та ті організаційно-правові ускладнення, які знижують результативність усієї системи. У цьому контексті важливо виходити з того, що Стратегія інформаційної безпеки України не обмежується констатацією загроз, а прямо визначає стратегічні цілі та завдання, спрямовані на протидію таким загрозам, захист прав осіб на інформацію та захист персональних даних. Отже, інституційний механізм у цій сфері має оцінюватися не лише за наявністю відповідних органів, а передусім за їх спроможністю забезпечити реальний рух від стратегічного рішення до практичного результату.

На стратегічно-політичному рівні повноваження основних суб'єктів мають установчий і спрямовуючий характер. Верховна Рада України забезпечує законодавче підґрунтя державної політики у сфері національної, інформаційної та кібернетичної безпеки через ухвалення законів, які визначають правові й організаційні засади відповідної діяльності Президент України, увівши в дію рішення РНБО про Стратегію інформаційної безпеки, фактично надав відповідному документу статус загальнообов'язкового

стратегічного орієнтира для всієї системи публічної влади. Рада національної безпеки і оборони України, своєю чергою, виступає центром міжвідомчого стратегічного узгодження, у межах якого проблематика інформаційної війни інтегрується до загальної системи національної безпеки [130]. Кабінет Міністрів України посідає проміжне, але основне місце між стратегічним рішенням і його практичним виконанням, оскільки саме уряд вносив проект Стратегії інформаційної безпеки та забезпечує виконавське наповнення стратегічних документів через систему центральних органів виконавчої влади.

На координаційно-виконавчому рівні особливе значення мають повноваження Міністерства культури та стратегічних комунікацій України. Положення про це міністерство закріплює, що воно є головним органом у системі центральних органів виконавчої влади, який забезпечує формування та реалізує державну політику, зокрема, у сферах інформаційної безпеки, популяризації України у світі, державного іномовлення та стратегічних комунікацій. Окрім цього, у положенні окремо вказано на повноваження МКСК у сфері міжнародного співробітництва з питань інформаційної безпеки та стратегічних комунікацій, а також на здійснення заходів, спрямованих на захист національного інформаційного простору. У межах досліджуваного механізму це дозволяє розглядати МКСК як головного суб’єкта державної комунікаційної політики, відповідального за вироблення офіційних наративів, їх системне поширення та координацію публічних комунікацій у безпековому вимірі [105, с. 74].

Функціонально близьким, але не тотожним за призначенням є Центр протидії дезінформації при РНБО. Згідно з положенням про нього, Центр забезпечує здійснення заходів щодо протидії поточним і прогнозованим загрозам національній безпеці та національним інтересам України в інформаційній сфері, забезпечення інформаційної безпеки України, виявлення і протидії дезінформації, пропаганді, деструктивним інформаційним впливам і спробам маніпулювання громадською думкою [114]. Серед його основних завдань прямо названо аналіз і моніторинг подій в інформаційному просторі,

виявлення та вивчення поточних і прогнозованих загроз інформаційній безпеці, а також оцінку їх наслідків для національних інтересів. Це означає, що ЦПД у межах інституційного механізму виконує насамперед аналітичну, попереджувальну та координаційно-безпекову функцію, тоді як МКСК більшою мірою відповідає за формування й проведення державної політики у комунікаційній площині [77, с. 152].

Важливий блок повноважень пов'язаний із безпековою, розвідувальною та кібернетичною складовими. Закон України «Про розвідку» визначає правові та організаційні засади функціонування розвідки та порядок здійснення контролю за нею, що створює нормативну основу для залучення розвідувального співтовариства до виявлення зовнішніх інформаційних загроз, джерел їх походження, каналів поширення та намірів противника [140]. Закон України «Про основні засади забезпечення кібербезпеки України» встановлює правові й організаційні основи захисту національних інтересів у кіберпросторі, повноваження державних органів і засади координації їхньої діяльності [132]. Через це безпековий сегмент протидії інформаційній війні охоплює не лише боротьбу з пропагандою у медійному полі, а й захист державних інформаційних ресурсів, критичної інфраструктури, електронних комунікацій та цифрових систем, які можуть бути об'єктом одночасного інформаційного і кібернетичного впливу [105, с. 78].

У цьому ж контексті особливе місце посідає Державна служба спеціального зв'язку та захисту інформації України разом із CERT-UA та суміжними елементами національної системи реагування на кіберінциденти. У 2025 році уряд затвердив окремий порядок взаємодії у сфері кіберзахисту між CERT-UA, галузевими й регіональними командами реагування, а також правоохоронними, контррозвідувальними і розвідувальними структурами. Для досліджуваної теми це має принципове значення, оскільки свідчить про поступове інституційне оформлення не лише окремих суб'єктів, а й процедур їх взаємодії [38]. Звідси випливає, що сучасний механізм протидії інформаційній війні вже не може обмежуватися лише гуманітарно-

комунікаційними заходами, а повинен охоплювати й скоординовані дії у кіберпросторі.

Окремий сегмент становлять суб'єкти медійно-регуляторного та суспільно-комунікаційного рівня. Закон України «Про медіа» створює сучасні правові рамки функціонування медійної сфери, а Закон України «Про суспільні медіа України» визначає правові основи діяльності Суспільного медіа. У досліджуваному механізмі значення цих суб'єктів полягає в тому, що протидія інформаційній війні не може зводитися лише до заборонних або силових інструментів. Вона потребує одночасного підтримання законного, стійкого та професійного медійного середовища, здатного бути джерелом перевіреної інформації, зменшувати простір для маніпуляції та забезпечувати суспільству доступ до достовірного контенту [105, с. 77]. У цьому аспекті регуляторний і суспільний медійний блоки виконують запобіжну та стабілізуючу функції.

Форми взаємодії між суб'єктами інституційного механізму мають як вертикальний, так і горизонтальний характер. Вертикальна взаємодія полягає у русі стратегічних рішень від рівня політичного визначення пріоритетів до рівня їх виконавського забезпечення. Горизонтальна взаємодія проявляється в координації між органами, які належать до різних функціональних блоків: безпекового, цифрового, медійного, дипломатичного, гуманітарного, аналітичного. Стратегія інформаційної безпеки прямо вказує, що досягнення її мети пов'язується зі створенням ефективної системи взаємодії між органами державної влади, органами місцевого самоврядування та суспільством, а також із розвитком міжнародної співпраці у сфері інформаційної безпеки. Більше того, у Стратегії окремо визначено стратегічну ціль щодо створення ефективної системи стратегічних комунікацій і наголошено на необхідності визначення системи взаємодії з питань реагування на кризову ситуацію та післякризову комунікацію.

Практичною формою такої взаємодії є міжвідомче погодження стратегічних документів, обмін аналітичною інформацією, координація

офіційних комунікацій, спільне реагування на кризові інформаційні ситуації та розмежування сфер відповідальності між основними суб'єктами [109, с. 118].

Ще однією формою взаємодії виступає координація у сфері кіберзахисту та реагування на інциденти. Закон про кібербезпеку прямо вказує на координаційний характер державної політики в цій сфері [132], а нові урядові рішення 2025 року деталізують механізм взаємодії між CERT-UA, галузевими й регіональними командами реагування та силовими структурами [125]. Для теми протидії інформаційній війні це особливо важливо, оскільки ворожі інформаційні кампанії дедалі частіше поєднуються з кібератаками на державні сайти, реєстри, медійні платформи або канали комунікації [173, с. 202]. Тому взаємодія у цій площині повинна будуватися не постфактум, а як заздалегідь визначений алгоритм спільних дій, у якому інформаційний і кібернетичний напрями не розриваються, а взаємно доповнюють один одного.

Окрему увагу слід звернути на взаємодію держави з місцевим самоврядуванням і суспільством. Стратегія інформаційної безпеки прямо вказує на необхідність саме такої взаємодії, а не лише на внутрішньодержавну координацію між центральними органами. Це має глибокий практичний зміст, оскільки значна частина інформаційних впливів спрямовується на локальні спільноти, окремі соціальні групи або регіональні інформаційні поля. Без участі місцевого рівня, без доведення офіційної позиції до конкретних громад і без зворотного зв'язку від суспільства державна стратегія ризикує залишитися надмірно централізованою і недостатньо гнучкою [148, с. 57]. Звідси випливає, що до дієвих форм взаємодії належать не лише службові координаційні процедури, а й просвітницькі кампанії, інформаційні роз'яснення, кризові комунікації, партнерські формати з громадянським суспільством та залучення недержавних експертних спільнот [153, с. 192].

Проблеми функціонування досліджуваного інституційного механізму насамперед пов'язані з розпорошеністю компетенції. Аналіз чинної нормативної бази дає підстави для висновку, що у сфері протидії

інформаційній війні одночасно діють суб’єкти з різною правовою природою, різними каналами підпорядкування та різними інструментами впливу: стратегічно-політичні, урядово-комунікаційні, аналітично-безпекові, кібернетичні, медійно-регуляторні. Така багатосуб’єктність сама по собі не є негативною, однак за відсутності чітких процедур постійної координації вона може породжувати дублювання функцій, конкуренцію за інформаційне лідерство, різночитання у публічних меседжах і затримки у реагуванні на загрози [106, с. 182].

Друга системна проблема полягає в тому, що реалізація чинної Стратегії інформаційної безпеки була розрахована на період до 2025 року. Ця обставина має важливе значення для оцінки сучасного стану інституційного механізму, оскільки стратегічні документи такого рівня не повинні втрачати часову визначеність без одночасного оновлення цілей, інструментів та системи координації [143]. З урахуванням того, що за останні роки інституційна структура у сфері стратегічних комунікацій, кіберзахисту та державної комунікації була змінена і розширена, актуальним постає завдання або оновлення, або прийняття нового стратегічного документа, який би врахував сучасний розподіл повноважень, нові інструменти реагування та досвід повномасштабної війни.

Третя проблема пов’язана з необхідністю зберігати баланс між безпекою та демократичними стандартами. Стратегія інформаційної безпеки одночасно орієнтує державу на протидію загрозам і на захист прав осіб на інформацію та захист персональних даних. Отже, держава не може будувати протидію інформаційній війні виключно на логіці заборон, блокувань і обмежень. Кожне посилення безпекового реагування має супроводжуватися правовими гарантіями, прозорістю процедур і чітким розмежуванням повноважень. У протилежному випадку виникає ризик того, що боротьба з інформаційною агресією почне вступати в суперечність із принципами правової держави, а це, своєю чергою, послаблюватиме легітимність самої державної стратегії [153, с. 193].

Четверта проблема стосується нерівномірності інституційної спроможності суб’єктів. Нормативне закріплення широких повноважень ще не означає однакового рівня кадрового, технічного, аналітичного й комунікаційного забезпечення всіх учасників системи [106, с. 183]. Уже сам факт того, що законодавець і уряд у 2025 році були змушені додатково врегульовувати порядок взаємодії у сфері кіберзахисту, свідчить про поступове дооформлення відповідних процедур, а не про їх остаточну завершеність [125]. З цього випливає, що частина ускладнень у функціонуванні інституційного механізму зумовлена не браком суб’єктів, а недостатнім рівнем інституційної злагодженості, стандартизації процедур та інтеграції інформаційного, безпекового й кібернетичного компонентів у єдину логіку дії.

Отже, аналіз повноважень, форм взаємодії та проблем функціонування суб’єктів інституційного механізму протидії інформаційній війні дає підстави для кількох узагальнень. По-перше, сучасна українська система має вже сформоване багаторівневе інституційне ядро, яке охоплює стратегічний, урядово-комунікаційний, безпеково-аналітичний, кібернетичний і медійний блоки. По-друге, визначальною умовою її результативності є не механічне розширення кола суб’єктів, а чітка координація між ними, узгодженість повноважень і своєчасне оновлення стратегічних орієнтирів. По-третє, основні труднощі пов’язані не стільки з відсутністю правових інструментів, скільки з ризиком фрагментації, дублювання функцій, несинхронності комунікаційних та безпекових дій і потребою оновлення стратегічної рамки після завершення періоду дії чинної Стратегії. Усе це створює підстави для наступного етапу дослідження – формулювання конкретних напрямів удосконалення інституційного механізму формування та реалізації державної стратегії протидії інформаційній війні [143].

Удосконалення інституційного механізму формування та реалізації державної стратегії протидії інформаційній війні має розглядатися не як локальне коригування окремих управлінських рішень, а як послідовне

впорядкування всієї системи суб’єктів, повноважень, процедур взаємодії та засобів реагування. Така потреба зумовлена як динамічним характером самої інформаційної агресії, так і тим, що чинна Стратегія інформаційної безпеки визначала цілі та завдання держави на період до 2025 року, а отже нині об’єктивно постає питання про оновлення з урахуванням досвіду повномасштабної війни, змін у структурі центральних органів виконавчої влади, розвитку кіберзагроз та накопиченої практики реагування на дезінформацію. Водночас уряд у 2025 році схвалив Концепцію національної системи стратегічного планування, що додатково підкреслює потребу в більш системному підході до підготовки нових стратегічних документів і до узгодження їх із загальною логікою державного планування.

Першочерговим напрямом удосконалення є підготовка нового стратегічного документа або ґрунтовне оновлення чинної Стратегії інформаційної безпеки. Йдеться не лише про зміну строків її дії, а про перегляд самого змісту стратегічних пріоритетів, переліку загроз, механізмів реагування та системи відповідальних суб’єктів. Після 2021 року інституційна архітектура у цій сфері істотно змінилася: посилився напрям стратегічних комунікацій [153, с. 191], більш чітко окреслилися функції Центру протидії дезінформації при РНБО, зросло значення кіберзахисту державних ресурсів, набув нової ваги Закон України «Про медіа», а також сформувалася ширша практика державно-суспільної співпраці у протидії ворожим інформаційним впливам. За таких умов новий стратегічний документ має не повторювати загальні положення попереднього, а відобразити реальну картину сучасного інституційного середовища, визначити чіткі напрями дії, часові межі, критерії оцінювання та співвідношення між безпековим, комунікаційним, медійним і кібернетичним блоками.

Другим напрямом є чітке нормативне розмежування повноважень між основними суб’єктами інституційного механізму. Нині в цій сфері одночасно діють РНБО, Кабінет Міністрів України, Міністерство культури та стратегічних комунікацій України, Центр протидії дезінформації, Центр

стратегічних комунікацій та інформаційної безпеки, Держспецзв'язку, Міністерство цифрової трансформації, медійний регулятор та інші суб'єкти. Формально таке багаторівневе коло учасників є виправданим, однак без достатньо чіткого розмежування компетенції воно може породжувати дублювання дій, паралельне продукування схожих інформаційних продуктів, конкуренцію за комунікаційний простір і розмивання відповідальності.

Третім напрямом слід визнати посилення координаційного центру всієї системи. На нашу думку, удосконалення інституційного механізму неможливе без закріплення стабільного порядку міжвідомчої взаємодії, який не залежав би від ситуативних рішень чи особистої управлінської активності окремих посадових осіб [31, с. 1150–1162]. РНБО вже виконує стратегічно-узгоджувальну функцію, а Центр протидії дезінформації створений саме при цьому органі, що свідчить про безпековий характер координації у сфері інформаційної протидії. Водночас державна практика показує, що для повноцінної дії механізму потрібні не лише загальні координаційні повноваження, а й постійні регламенти обміну аналітичною інформацією, узгодження кризових комунікацій, спільного вироблення позицій та швидкого доведення рішень до виконавців.

Четвертий напрям пов'язаний із поєднанням інформаційної безпеки та кіберзахисту в межах єдиної логіки державної дії. Закон України «Про основні засади забезпечення кібербезпеки України» прямо визначає правові й організаційні основи захисту національних інтересів у кіберпросторі та засади координації діяльності державних органів у цій сфері. CERT-UA як урядова команда реагування на комп'ютерні надзвичайні події функціонує при Держспецзв'язку, а урядові акти 2025 року деталізували порядок реагування на кіберінциденти, кібератаки та кіберзагрози. За сучасних умов російські інформаційні операції все частіше супроводжуються кібератаками на державні ресурси, офіційні канали комунікації, медійні майданчики, облікові записи посадових осіб і цифрову інфраструктуру. У зв'язку з цим інституційний механізм не повинен розглядати інформаційний і кібернетичний напрями

окремо. Доцільним є закріплення постійної спільної роботи комунікаційного та кібербезпекового блоків, коли спростування дезінформації, технічне блокування шкідливої активності, аналітичне визначення джерела атаки та попередження населення здійснюються як взаємопов'язані елементи єдиного процесу реагування.

П'ятим напрямом є зміцнення державних стратегічних комунікацій як самостійної управлінської підсистеми. Положення про Міністерство культури та стратегічних комунікацій України закріплює його місце як головного органу у системі центральних органів виконавчої влади, який формує та реалізує державну політику, зокрема у сфері стратегічних комунікацій [37]. Разом із тим на практиці стратегічні комунікації ще потребують подальшого інституційного укріплення: від внутрішньої уніфікації державних повідомлень до розбудови мережі комунікаційних підрозділів у різних органах влади. Досвід Центру стратегічних комунікацій та інформаційної безпеки свідчить, що комунікаційна протидія зовнішнім загрозам і розбудова стійкості суспільства до дезінформації вже стали сталими напрямами державної діяльності [123]. Однак для досягнення більшого ефекту необхідно посилити інтеграцію цього напряму в діяльність не лише профільного міністерства, а й усіх основних органів державної влади, які повинні працювати у спільній смисловій та процедурній площині.

Шостим напрямом удосконалення є розвиток системи кризових комунікацій. Чинна Стратегія інформаційної безпеки прямо передбачає створення ефективної системи стратегічних комунікацій та визначення системи взаємодії з питань реагування на кризову ситуацію та післякризову комунікацію. Це означає, що держава вже на рівні стратегічного документа визнала потребу не лише в загальній комунікаційній політиці, а й у спеціально організованому реагуванні на гострі фази інформаційної агресії. Проте практична реалізація цього напряму повинна бути поглиблена шляхом запровадження постійних кризових комунікаційних груп, типових алгоритмів публічного інформування, резервних каналів зв'язку, порядку взаємодії з

місцевими органами влади та єдиних вимог до змісту державних повідомлень у перші години після масштабних інформаційних атак [109, с. 119]. Саме швидкість, узгодженість і переконливість первинної реакції держави часто визначають, чи набуде ворожий наратив масового поширення.

Сьомим напрямом є поглиблення регуляторної та суспільно-запобіжної складової. Закон України «Про медіа» створив сучасні рамки для правового упорядкування медійного простору, а існування Суспільного медіа України закріплює інституційну основу для поширення перевіреної, професійної та суспільно значущої інформації. Однак стійкість до інформаційної війни не досягається лише контролем чи наглядом за дотриманням законодавства. Вона значною мірою залежить від якості національного медійного середовища, довіри до офіційних і суспільних джерел, наявності прозорих правил для ринку медіа та спроможності держави діяти в межах права, не підриваючи демократичних свобод.

Восьмим напрямом доцільно визначити розширення регіонального та місцевого виміру інституційного механізму. Стратегія інформаційної безпеки орієнтує державу на ефективну взаємодію не лише між центральними органами влади, а й з органами місцевого самоврядування та суспільством. Це положення має бути наповнене більш чітким організаційним змістом. У практичній площині це означає потребу створення або посилення регіональних осередків комунікаційної та аналітичної роботи, швидкого доведення спростувань до громад, підготовки посадових осіб місцевого рівня до дій в умовах інформаційних криз і встановлення постійного зворотного зв’язку між центром та територіями. Ворожі інформаційні кампанії нерідко будуються на місцевих проблемах, побутових конфліктах, регіональних особливостях або чутках, які не завжди помітні на центральному рівні.

Дев’ятим напрямом є кадрове та освітнє забезпечення відповідної системи. Жоден інституційний механізм не може бути результативним без належно підготовлених фахівців, здатних працювати на стику права, національної безпеки, інформаційної аналітики, стратегічних комунікацій,

цифрової безпеки, медійного права та кризового управління [106, с. 183]. Окремі державні інституції вже накопичили значний практичний досвід, однак ця спроможність має бути переведена на системний рівень через спеціалізовані програми навчання, міжвідомчі тренінги, підготовку кадрів для комунікаційних підрозділів, вироблення спільної термінологічної бази та підвищення кваліфікації державних службовців, що працюють у сфері інформаційної безпеки. У цьому аспекті показовим є сам факт існування спеціалізованих державних інституцій, робота яких спрямована на аналітику, спростування, моніторинг і доведення до суспільства перевіреної інформації.

Десятим напрямом є запровадження чіткої системи оцінювання результативності інституційного механізму. Однією з причин недостатньої дієвості багатьох державних стратегій є відсутність зрозумілих критеріїв, за якими можна визначити, чи досягнуто поставлених цілей. Концепція національної системи стратегічного планування, схвалена урядом у 2025 році, якраз указує на потребу цілісного й ефективного підходу до стратегічного планування [143]. Для сфери протидії інформаційній війні це означає, що стратегічний документ повинен містити не лише перелік загроз і бажаних завдань, а й конкретні показники оцінювання: швидкість реагування на дезінформаційні атаки, рівень міжвідомчої узгодженості, охоплення аудиторії державними роз’ясненнями, стан кіберзахисту критичних інформаційних систем, динаміку довіри до офіційних джерел, ступінь проникнення ворожих наративів у публічний простір.

Таким чином, напрями вдосконалення інституційного механізму формування та реалізації державної стратегії протидії інформаційній війні повинні охоплювати не окремі точкові рішення, а взаємопов’язану систему кроків: оновлення стратегічного документа, чіткіше розмежування повноважень, посилення координації, поєднання інформаційного та кібернетичного блоків, укріплення стратегічних комунікацій, розвиток кризових комунікацій, поглиблення медійної та просвітницької складової, розширення місцевого виміру, належне кадрове забезпечення, запровадження

системи оцінювання результативності та посилення міжнародної співпраці. Лише за такої умови держава зможе перейти від реактивного реагування на окремі інформаційні атаки до цілісної, внутрішньо узгодженої та довготривалої системи захисту власного інформаційного простору, суспільної стійкості й національних інтересів.

Висновки до розділу 2

1. Проаналізовано зарубіжний досвід формування державної стратегії протидії інформаційній війні на прикладі провідних європейських країн та США. Встановлено, що найбільш результативні підходи ґрунтуються не на разових інформаційних кампаніях, а на інституційно оформленій системі стратегічних комунікацій, постійному міжвідомчому узгодженні дій, поєднанні безпекових і комунікаційних засобів та широкому залученні суспільства. Швеція демонструє ефективність механізму психологічного самозахисту, де окремий державний орган координує заходи зі зміцнення суспільної стійкості до дезінформації; Фінляндія – дієвість національної політики медіаграмотності, інтегрованої в освітню систему та підтримуваної державними інституціями; Естонія важливість централізованої урядової стратегічної комунікації та узгодженого донесення державної позиції; досвід США підтверджує значення спеціалізованих механізмів виявлення й протидії зовнішній інформаційній маніпуляції та розвитку міжнародного партнерства у цій сфері.

2. З урахуванням опрацьованого матеріалу обґрунтовано, що для України можуть бути адаптовані кілька конкретних елементів зарубіжного досвіду: створення або нормативне посилення постійного координаційного центру протидії інформаційним впливам, зокрема, за зразком шведського механізму; інституціоналізація національної політики медіаграмотності та включення її до системи освіти за фінським підходом; запровадження сталої

системи урядової стратегічної комунікації та єдиного порядку міжвідомчого погодження публічних меседжів, що відповідає естонській практиці; розвиток механізмів міжнародного обміну аналітичною інформацією, координації дій із партнерами та спеціалізованого моніторингу зовнішніх інформаційних операцій, що характерно для американського досвіду. Водночас, наголошено на тому, що практична цінність зарубіжного досвіду полягає не в механічному копіюванні окремих інституцій, а у запозиченні перевірених управлінських рішень, які можуть бути інтегровані в українську систему публічного управління з урахуванням національних безпекових потреб, правового порядку та інституційної структури держави.

3. Аргументовано, що формування державної стратегії протидії інформаційній війні повинно здійснюватися на чітко визначеній системі принципів, які задають межі, зміст і спосіб державного реагування на інформаційні загрози. До таких принципів віднесено: верховенство права та законність; пріоритет прав і свобод людини; ідеологічну багатоманітність і недопустимість цензури; достовірність, повноту та своєчасність офіційної інформації; системність і міжвідомчу координацію; стійкість та адаптивність держави і суспільства; взаємодію з міжнародними партнерами та інтегрованість у ширший безпековий контекст; поєднання інформаційної та кібернетичної складових безпеки. Проведений аналіз дає підстави стверджувати, що без урахування цих принципів державна стратегія втрачає правову визначеність, внутрішню узгодженість і практичну здатність забезпечувати належний захист інформаційного суверенітету держави. Поряд із цим обґрунтовано, що зміст майбутньої державної стратегії повинен будуватися на низці взаємопов’язаних стратегічних засад, до яких віднесено: її конституційно-безпекову складову; опору на систему стратегічного планування; спадкоємність і водночас оновлення нормативно-правової бази; орієнтацію на чіткий механізм реалізації; міжсекторальний характер; стійкість і адаптивність держави та суспільства; поєднання інформаційної та кібернетичної складових безпеки; доказовість та аналітичну обґрунтованість;

ресурсну забезпеченість; міжнародну взаємодію та зовнішньополітичний вимір.

4. Встановлено, що інституційний механізм формування та реалізації державної стратегії протидії інформаційній війні є сукупністю взаємопов’язаних суб’єктів, повноважень, процедур координації та засобів реагування, через які держава забезпечує вироблення, ухвалення і практичне виконання стратегічних рішень у сфері інформаційної безпеки. З’ясовано, що його ефективність залежить не від кількості залучених органів, а від нормативного розмежування компетенції, наявності постійної міжвідомчої взаємодії, узгодженості офіційних комунікацій та здатності поєднувати безпекові, медійні, цифрові й аналітичні засоби в єдиному порядку дій. Водночас доведено, що нинішній стан цього механізму характеризується розпорошенням повноважень, недостатньою процедурною визначеністю взаємодії між основними суб’єктами, неповною інтеграцією інформаційного і кібернетичного напрямів, а також потребою в оновленні стратегічних документів з урахуванням нових загроз і досвіду повномасштабної війни.

5. Вдосконалення інституційного механізму має здійснюватися за кількома взаємопов’язаними напрямами: нормативно-правове закріплення компетенції основних суб’єктів; посилення координаційного центру системи; поєднання інформаційної безпеки і кіберзахисту в межах спільного порядку реагування; зміцнення державних стратегічних комунікацій; розширення регуляторної, просвітницької та регіональної складових; належне кадрове забезпечення; запровадження системи оцінювання результативності; посилення міжнародної взаємодії. Акцентовано увагу на тому, що інституційний механізм формування і реалізації державної стратегії протидії інформаційній війні повинен розглядатися як основний елемент публічного управління у сфері інформаційної безпеки, а його подальше вдосконалення є необхідною умовою підвищення стійкості держави до сучасних інформаційних загроз.

РОЗДІЛ 3.
НАПРЯМИ РЕАЛІЗАЦІЇ ДЕРЖАВНОЇ СТРАТЕГІЇ ПРОТИДІЇ ІНФОРМАЦІЙНІЙ ВІЙНІ В УКРАЇНІ

3.1. Основні проблеми реалізації державної стратегії протидії інформаційній війні

Відповідно до наявних викликів, пов’язаних із розвитком інформаційних технологій, поширенням гібридних загроз, активізацією дезінформаційних кампаній та необхідністю узгодження національного законодавства з європейськими стандартами, реалізація державної стратегії протидії інформаційній війні в Україні спирається на широкий комплекс нормативно-правових актів, організаційних рішень та інституційних механізмів, які визначають засади захисту національного інформаційного простору на загальнодержавному рівні.

Правову основу реалізації такої стратегії становить Конституція України, яка гарантує свободу слова і вираження поглядів, захист приватного життя, а також право громадян на інформацію [74]. Основоположні приписи закладають вихідні засади для побудови державної діяльності, спрямованої, з одного боку, на забезпечення відкритості та доступності інформації, а з іншого – на захист інформаційного простору держави від деструктивного зовнішнього й внутрішнього впливу. На законодавчому рівні важливе значення для реалізації державної стратегії протидії інформаційній війні мають і Закон України «Про інформацію» [128], який визначає загальні засади інформаційної діяльності, види інформації та правові механізми доступу до неї, а також Закон України «Про доступ до публічної інформації» [120], що забезпечує прозорість діяльності органів державної влади та відкритість публічного управління.

У контексті досліджуваної проблематики ці акти мають значення не лише як гарантія інформаційних прав громадян, а і як нормативна база, в

межах якої держава повинна поєднувати принцип відкритості з потребою належного реагування на інформаційні загрози. Окрім цього, вагоме місце у реалізації державної стратегії протидії інформаційній війні посідають і акти, які безпосередньо спрямовані на захист інформаційного простору та запобігання кіберзагрозам. Йдеться про Закон України «Про основні засади забезпечення кібербезпеки України [132] та Закон України «Про захист персональних даних» [126]. Їх призначення полягає у врегулюванні заходів, пов'язаних із захистом державних і приватних інформаційних ресурсів, визначенні правил зберігання та обробки персональних даних, а також створенні правових передумов для протидії кіберінцидентам, які виступають складовою інформаційної війни. У зв'язку з цим посилення вимог до безпеки цифрових систем, оновлення засобів кіберзахисту та наближення національного регулювання до міжнародних стандартів слід розглядати як важливий елемент загальної державної стратегії.

Окремий блок нормативно-правового регулювання стосується медіасфери. Важливим кроком стало набрання чинності Законом України «Про медіа» [129], який оновив національне законодавство, узгодивши його з європейськими підходами, та встановив нові правила функціонування медіаринку, зокрема в частині діяльності цифрових платформ, соціальних мереж та аудіовізуальних сервісів. Для теми дослідження особливе значення має те, що зазначений Закон України створив додаткові правові передумови для протидії дезінформації, поширенню маніпулятивного контенту та іншим проявам інформаційного впливу, які використовуються як інструмент підриву суспільної стійкості в умовах інформаційної війни. Водночас, окремо необхідно виділити проблему фінансування незалежних медіа. В умовах економічної нестабільності значна частина засобів масової інформації перебуває у залежності від приватного капіталу, що створює ризики для об'єктивності інформації, редакційної незалежності та стійкості медійного середовища. У зв'язку з цим одним із проблемних питань реалізації державної стратегії протидії інформаційній війні є відсутність розвинених механізмів

підтримки незалежних журналістських проєктів, прозорого грантового фінансування та належного ресурсного забезпечення суспільного мовлення [11].

Поряд із цим, ще однією складовою реалізації державної стратегії протидії інформаційній війні є правове забезпечення цифровізації публічного управління. Закон України «Про електронні документи та електронний документообіг» [121] закріплює правові засади використання цифрових технологій у діяльності органів державної влади, а Національна програма інформатизації [131] передбачає комплекс заходів щодо впровадження інформаційних технологій у різних сферах суспільного життя.

При цьому серед стратегічних документів, які безпосередньо впливають на реалізацію державної стратегії протидії інформаційній війні в Україні, слід виокремити Стратегію інформаційної безпеки України [165] та Стратегію розвитку кібербезпеки на 2021–2025 роки [166]. У цих актах визначено системні підходи до протидії дезінформації, розвитку національної системи кіберзахисту, посилення інформаційної стійкості держави та суспільства, а також до захисту національних інтересів в інформаційній сфері.

Особливу увагу держава приділяє протидії дезінформації. У розрізі цього, як вже було зазначено у попередніх підрозділах дослідження, важливе значення мало рішення Ради національної безпеки і оборони України «Щодо реалізації єдиної інформаційної політики в умовах воєнного стану» [138], яке передбачало консолідацію медіаресурсів, обмеження діяльності ворожих інформаційних платформ та активізацію заходів з протидії інформаційним атакам. Хоча такі рішення мали практичне значення для оперативного реагування на загрози, вони водночас продемонстрували, що реалізація стратегії протидії інформаційній війні в Україні значною мірою залежить від надзвичайних рішень воєнного періоду, тоді як питання довгострокової

системності й належного нормативного оформлення цієї діяльності все ще потребують подальшого вдосконалення.

Суттєву роль у реалізації державної стратегії протидії інформаційній війні відіграють і спеціалізовані державні органи та інституції, зокрема Міністерство цифрової трансформації України [90], Національна рада України з питань телебачення і радіомовлення, Центр стратегічних комунікацій та інформаційної безпеки [146] та інші суб'єкти, уповноважені здійснювати окремі функції у сфері інформаційної безпеки, цифрового розвитку, медіарегулювання та публічної комунікації. Їх діяльність формує інституційний механізм державної стратегії, однак на практиці ефективність цієї системи залежить від чіткості розмежування повноважень, рівня координації між органами влади та наявності єдиного підходу до визначення цілей і засобів протидії інформаційній війні.

Так, за останні роки державна діяльність у сфері інформаційної безпеки та захисту інформаційного простору зазнала змін, зумовлених поширенням цифрових технологій, посиленням гібридної агресії та потребою адаптувати державні рішення до нових форм зовнішнього інформаційного впливу. Унаслідок оновлення законодавства, розвитку цифрових сервісів і впровадження нових механізмів у сфері інформації Україна досягла певних результатів у побудові системи публічного управління, здатної реагувати на інформаційні загрози. Одним із найбільш помітних результатів стало впровадження цифрових сервісів держави, зокрема проєкту «Держава у смартфоні» та платформи «Дія» [90]. Вони значно спростили доступ громадян до адміністративних послуг, мінімізували бюрократичні процедури та підвищили рівень відкритості державного управління. Разом із тим у межах досліджуваної теми ці здобутки не можна оцінювати виключно позитивно без урахування супутніх ризиків, оскільки розширення цифрових сервісів автоматично збільшує обсяг інформаційних ресурсів і технічних систем, які

можуть ставати об’єктом кібератак, деструктивного інформаційного впливу або використання у межах гібридної агресії.

Створення Центру стратегічних комунікацій та інформаційної безпеки [146], блокування ворожих пропагандистських медіа, а також запровадження єдиної інформаційної політики в умовах воєнного стану [138] дали змогу посилити захист інформаційного простору і знизити вплив російської пропаганди на суспільство. Окремої уваги заслуговує співпраця України з Європейським Союзом у сфері цифрового розвитку, кібербезпеки та інформаційної безпеки [42]. Така взаємодія дає можливість використовувати європейські підходи та поступово наближати національне законодавство до стандартів ЄС. Разом із тим саме у цьому аспекті виявляється одна з основних проблем: процес гармонізації законодавства та управлінських практик із європейськими вимогами ще не завершений, а тому державна стратегія протидії інформаційній війні в Україні поки що реалізується в умовах певної неповноти нормативного та інституційного забезпечення.

Ще однією суттєвою проблемою реалізації державної стратегії протидії інформаційній війні в Україні залишається боротьба з дезінформацією та фейковими повідомленнями. Її актуальність зумовлена не лише масштабом поширення неправдивого контенту, а й тим, що дезінформаційні кампанії дедалі тісніше поєднуються з кібернетичними загрозами, інформаційно-психологічними операціями та спробами підірвати довіру населення до державних інституцій. За офіційними даними, у 2022 році кількість зареєстрованих кіберінцидентів зросла у 2,8 рази порівняно з 2021 роком, а у 2023 році було зафіксовано подальше зростання на 62,5%. Окремо CERT-UA повідомляла, що у 2025 році опрацювала майже 6000 кіберінцидентів, а кількість ворожих атак зросла ще на 37% порівняно з попереднім роком [34; 36; 179].

Зазначена проблема ускладнюється тим, що навіть після блокування окремих проросійських медіа й платформ ворожі інформаційні кампанії не припинилися, а лише змінили форми та канали поширення. Центр протидії

дезінформації наголошує, що одним із найбільш поширених механізмів російського інформаційного впливу є так звана дезінформаційна сітка, основу якої становлять анонімні Telegram-канали, що регулярно цитують один одного, координовано поширюють маніпулятивні повідомлення та формують ілюзію масової підтримки певних тез [192]. Крім того, ЦПД систематично оприлюднює оновлені переліки каналів і ресурсів, які поширюють фейки, маніпуляції та ворожу пропаганду. Це свідчить про те, що сучасні дезінформаційні кампанії пристосовуються до нових умов, переміщуються із заблокованих майданчиків у соціальні мережі, месенджери, закриті спільноти, псевдоекспертне середовище та інші приховані форми інформаційного впливу. За таких умов держава стикається вже не з поодинокими фейковими повідомленнями, а з багаторівневою системою координованого інформаційного впливу, яка швидко змінює канали поширення, цільові аудиторії та тематичні акценти [159; 192].

Проблема дезінформації має не лише технологічний, а й виразний соціально-психологічний вимір. Її небезпека полягає не просто у факті поширення неправдивих повідомлень, а у здатності таких повідомлень формувати викривлене сприйняття подій, провокувати панічні настрої, підривати довіру до офіційних джерел, поглиблювати внутрішні суперечності та послаблювати суспільну згуртованість. Особливо небезпечними є ті інформаційні впливи, які маскуються під «альтернативну аналітику», «інсайдерську інформацію», «експертну думку» або «свідчення очевидців». У такому разі дезінформація сприймається частиною аудиторії не як відверта пропаганда, а як правдоподібне тлумачення подій. Саме тому ворожий інформаційний вплив дедалі рідше має форму прямолінійної агітації, натомість частіше проявляється у вигляді напівправди, емоційно забарвлених тез, провокативних припущень, псевдоаналітичних оцінок чи контенту, який імітує незалежний громадський дискурс [159; 192].

За таких обставин держава повинна не лише обмежувати окремі джерела дезінформації, а й будувати довготривалу систему суспільної стійкості до

маніпулятивного контенту. Одним із основних елементів такої системи мають стати програми медіаграмотності та розвитку критичного мислення. Міністерство культури України у 2023 році прямо наголошувало, що національний тест з медіаграмотності є важливою частиною реалізації Стратегії інформаційної безпеки України, а серед тем, над якими необхідно працювати найбільше, були названі перевірка Telegram-каналів, розпізнавання теорій змов, реагування на контент псевдоекспертів та уникнення фішингу [95; 160].

Важливе місце у загальній характеристиці стану реалізації державної стратегії протидії інформаційній війні займає і розвиток державних онлайн-послуг. Їх значення полягає не лише у спрощенні взаємодії громадян з органами влади, зменшенні бюрократичних бар'єрів та покращенні доступу до адміністративних послуг, а й у формуванні нової архітектури інформаційної взаємодії між державою та суспільством. Україна активно впроваджує електронні сервіси, однак рівень їх використання залишається нерівномірним у різних сферах, що свідчить про збереження проблем як організаційного, так і інформаційно-комунікаційного характеру. Як вже було зазначено, найбільш поширеною онлайн-послугою є мобільний застосунок «Дія» [90], що підтверджує його практичну зручність та інтегрованість у повсякденне життя громадян. Водночас значно нижчий рівень використання окремих спеціалізованих сервісів, зокрема «Електронного суду», може бути пов'язаний зі складністю процедур, недостатньою зручністю користування, а також недостатнім рівнем обізнаності населення. У свою чергу, це свідчить про те, що одним із проблемних аспектів реалізації державної стратегії протидії інформаційній війні є не лише створення цифрових рішень, а й забезпечення їх реальної доступності, зрозумілості та довіри до них з боку громадян. Тобто, у контексті протидії інформаційній війні ці здобутки слід оцінювати не лише як управлінський успіх, а й як чинник нових ризиків. Чим більший обсяг державних послуг переводиться в електронний формат, тим ширшим стає коло цифрових ресурсів, які можуть бути об'єктом кібератак, інформаційного

втручання, технічного блокування або використання для дискредитації державних інституцій. До того ж рівень користування такими сервісами залишається нерівномірним. Якщо застосунок «Дія» охоплює близько 75% користувачів, то «Електронний суд» – лише 40%.

Не менш показовою є ситуація з інформаційною поведінкою населення у соціальних мережах. Facebook використовують для отримання новин близько 60% аудиторії, YouTube – 55%, Telegram – 50%. Такий розподіл демонструє, що основна боротьба за вплив на громадську думку перемістилася в цифровий простір, причому різні платформи охоплюють різні вікові та соціальні групи. Telegram має особливе значення в умовах воєнного стану через швидкість поширення повідомлень, однак саме ця швидкість створює сприятливі умови для дезінформації, емоційних вкидів і неперевірених повідомлень. Водночас популярність TikTok та Instagram серед молоді вказує на ще одну проблему: держава поки що не повною мірою опанувала ті канали комунікації, які безпосередньо формують погляди молодшої аудиторії. Через це одним із недоліків сучасної реалізації державної стратегії є недостатня системність державної присутності в тих сегментах цифрового середовища, де формується повсякденний інформаційний вибір громадян.

У зв’язку з цифровізацією особливого значення набуває також захист персональних даних. Розвиток цифрового середовища, активне впровадження електронних сервісів, функціонування публічних електронних реєстрів, міжвідомчий обмін даними та постійне зростання обсягів інформації, що обробляється в автоматизованих системах, об’єктивно посилюють вимоги до конфіденційності відомостей про особу та до гарантій їх належного правового захисту. Конституція України закріплює, що не допускаються збирання, зберігання, використання і поширення конфіденційної інформації про особу без її згоди, крім випадків, визначених законом, а Закон України «Про захист персональних даних» прямо визначає, що його метою є захист основоположних прав і свобод людини і громадянина, зокрема права на невтручання в особисте життя, у зв’язку з обробкою персональних даних [126].

Додатково законодавство про публічні електронні реєстри окремо підкреслює, що обробка та захист персональних даних у таких реєстрах здійснюються відповідно до спеціального законодавства про захист персональних даних, що свідчить про тісний зв'язок цифрової трансформації держави з необхідністю посилення правових гарантій приватності [135].

У науковій літературі обґрунтовано звертається увага на те, що цифровізація істотно змінює підходи до правового регулювання персональних даних, оскільки сучасні інформаційні технології забезпечують не лише спрощення доступу до послуг та управлінських процедур, а й створюють нові ризики для приватності особи, пов'язані з масовим накопиченням, автоматизованою обробкою, передаванням та повторним використанням персональної інформації [13]. Саме тому одним із напрямів подальшого вдосконалення національного законодавства є його адаптація до європейських вимог, насамперед до стандартів General Data Protection Regulation. GDPR, ухвалений 27 квітня 2016 року і застосовуваний з 25 травня 2018 року, виходить із того, що захист персональних даних є фундаментальним правом, а його призначення полягає у забезпеченні високого, узгодженого та однакового рівня захисту прав і свобод фізичних осіб у зв'язку з обробкою їхніх даних [225]. На відміну від більш фрагментарного підходу, характерного для багатьох національних систем, цей регламент закріплює комплексні стандарти обробки даних, зокрема вимоги щодо законності, прозорості, обмеження мети, мінімізації даних, точності, обмеження строків зберігання, цілісності, конфіденційності та підзвітності контролера. Отже, орієнтація на стандарти GDPR є важливою не лише з позиції європейської інтеграції України, а й з погляду підвищення якості національного механізму захисту персональних даних [13].

Адаптація українського законодавства до європейських стандартів захисту персональних даних повинна охоплювати не лише формальне оновлення нормативних дефініцій, а й глибше переосмислення самого підходу до правового регулювання цифрового середовища. Йдеться, зокрема, про

посилення вимог до згоди суб’єкта персональних даних, підвищення прозорості процедур обробки, розширення обсягу прав особи щодо доступу до своїх даних, їх виправлення, видалення чи обмеження обробки, запровадження більш чітких правил відповідальності володільців і розпорядників даних, а також удосконалення механізмів державного нагляду і контролю [3; 225]. У сучасних умовах така адаптація набуває ще більшого значення, оскільки цифровізація дедалі активніше поєднується з використанням елементів штучного інтелекту, автоматизованого профілювання, алгоритмічного ухвалення рішень і транскордонного переміщення даних. У зв’язку з цим у новітніх наукових дослідженнях справедливо наголошується, що GDPR уже став не лише актом права Європейського Союзу, а й своєрідним еталоном для подальших законодавчих змін у сфері конфіденційності, цифрових прав і захисту персональної інформації [167]. Саме тому вдосконалення національного законодавства у цій сфері має розглядатися як необхідна передумова забезпечення прав людини в цифровій державі та як важливий елемент зміцнення довіри громадян до електронного врядування і цифрових сервісів [13; 42; 167].

Не можна оминути і питання медіаграмотності населення. Блокування ворожих джерел саме по собі не забезпечує належного захисту суспільства, якщо громадяни не вміють критично оцінювати інформацію, відрізняти факт від маніпуляції та перевіряти походження повідомлень. Недостатній рівень медіаосвіти прямо впливає на стійкість суспільства до дезінформації, а отже є не другорядною освітньою проблемою, а складовою національної безпеки. У цьому аспекті державна стратегія протидії інформаційній війні потребує посилення саме через освітні, просвітницькі та комунікаційні заходи, які повинні бути адресовані не лише школярам чи студентам, а всім групам населення.

Підсумовуючи викладене, слід зазначити, що стан реалізації державної стратегії протидії інформаційній війні в Україні є суперечливим. З одного боку, держава вже сформувала значний нормативний масив, створила

спеціалізовані інституції, розвинула цифрові сервіси, посилила правове регулювання медіасфери та кібербезпеки, а також активізувала співпрацю з міжнародними партнерами. З іншого боку, зберігаються суттєві проблеми: недостатня узгодженість між суб'єктами реалізації стратегії, нерівномірність практичного використання цифрових сервісів, посилення кіберзагроз, реактивний характер частини заходів протидії дезінформації, недостатній рівень медіаграмотності населення, фінансова вразливість незалежних медіа та незавершеність узгодження законодавства з європейськими стандартами. За таких умов подальше вдосконалення державної стратегії протидії інформаційній війні в Україні повинно спиратися не на поодинокі ситуативні кроки, а на послідовне поєднання правових, організаційних, технічних, аналітичних і комунікаційних рішень, здатних забезпечити реальну стійкість держави та суспільства до сучасних інформаційних загроз.

3.2. Напрями удосконалення державної стратегії протидії інформаційній війні

На нинішньому етапі забезпечення національної безпеки України, коли інформаційний простір став одним із головних напрямів зовнішнього і внутрішнього протиборства, вдосконалення державної стратегії протидії інформаційній війні має здійснюватися за кількома основними напрямами та передбачати вирішення комплексу взаємопов'язаних завдань [150, с. 89–90; 172, с. 70–72; 189, с. 282–283].

1. *Створення дієвого механізму нормативного та організаційного регулювання державної стратегії протидії інформаційній війні в Україні*.

За цим напрямом необхідно вирішити такі першочергові завдання:

а) осучаснення адміністративно-правового забезпечення державної політики у сфері протидії інформаційній війні, зокрема шляхом вироблення цілісних засад її формування та реалізації;

б) запровадження нових підходів до організації діяльності суб'єктів, уповноважених здійснювати заходи у сфері інформаційної безпеки, стратегічних комунікацій, протидії дезінформації та захисту національного інформаційного простору;

в) проведення детального моніторингу нормативно-правових актів, які регулюють питання інформаційної безпеки, стратегічних комунікацій, кіберзахисту, медіасфери та протидії дезінформації, їх конкретизація та деталізація, максимальне заповнення наявних прогалин, усунення виявлених суперечностей та ліквідація дублювань;

г) систематизація нормативно-правових актів, що регулюють питання протидії інформаційній війні, зокрема шляхом суттєвого скорочення їх кількості; скасування тих, що містять застарілі й суперечливі приписи; покращення їх якості завдяки використанню належних прийомів нормотворчої техніки; об'єднання в єдиному акті кількох суміжних нормативно-правових актів тощо;

ґ) підвищення якості нормотворчої техніки шляхом розроблення та забезпечення впровадження єдиних організаційних і методичних засад її здійснення, в основі яких має лежати суворе дотримання встановлених правил і стандартів;

д) забезпечення оптимального балансу нормативно-правових і морально-етичних норм та регуляторів у структурі державної стратегії протидії інформаційній війні [103, с. 110–111].

Для цього, насамперед, необхідним є закріплення сучасних етичних принципів діяльності посадових осіб та інших суб'єктів, які беруть участь у формуванні й реалізації державної стратегії протидії інформаційній війні, а в разі їх порушення мають застосовуватися належні заходи реагування. До таких принципів доцільно віднести: 1) захист Конституції та законів України, сприяння чіткому й неухильному виконанню їх приписів; 2) прагнення сумлінно й ініціативно виконувати службові обов'язки, застосовуючи найбільш раціональні способи досягнення поставлених завдань;

3) недопущення бюрократизму, формального ставлення до загроз інформаційній безпеці та потреб суспільства; 4) невикористання службової інформації в особистих або корпоративних інтересах; 5) справедливе й обґрунтоване прийняття управлінських рішень, несумісність виконання публічних функцій із будь-якими проявами корисливої заінтересованості; 6) протидію правопорушенням, зловживанням і протекціонізму; 7) досягнення належних результатів у службовій діяльності виключно в межах закону і правомірними засобами [8, с. 241–243; 162, с. 112–114].

Такі принципи формують моральні орієнтири діяльності державного апарату, сприяють утвердженню службової етики та запобігають викривленню змісту публічного управління у сфері інформаційної безпеки. За певних обставин можливе становище, за якого апарат, покликаний забезпечувати захист інформаційного простору та інтересів суспільства, втрачає службове призначення, зосереджується на самозбереженні, відомчій замкненості й використанні наданих повноважень у вузьких інтересах. За таких умов виникають передумови для формування формального стилю реагування на інформаційні загрози, приховування реального стану справ, викривлення звітності, створення штучно позитивної картини виконання завдань та уникнення реальної відповідальності [75, с. 66–68].

Реальні суспільні інтереси та потреби у сфері захисту інформаційного простору за формально-бюрократичного підходу враховуються лише настільки, наскільки вони можуть бути подані у вигляді формального показника, на підставі якого оцінюється діяльність уповноважених суб’єктів. У такому випадку державне управління починає орієнтуватися не на реальне зниження рівня інформаційних загроз, а на досягнення зовнішньо прийнятних індикаторів діяльності. Чим більш централізованою є система ухвалення рішень, тим більшою стає потреба у формальних критеріях вимірювання результатів, що, своєю чергою, спрощує зміст проведеної роботи та створює умови для підміни реальних досягнень звітними показниками [212].

У зв’язку з цим зростають можливості подання за допомогою формальних індикаторів викривленої картини фактично досягнутих результатів. Система оцінювання діяльності у сфері протидії інформаційній війні може бути побудована таким чином, що найбільше значення матимуть кількісні, а не якісні показники: кількість повідомлень, число проведених заходів, обсяг підготовлених інформаційних матеріалів, а не реальна стійкість суспільства до дезінформації, рівень довіри до державних інституцій чи фактичне зниження впливу ворожих інформаційних кампаній. Тому боротьбу з бюрократизмом у цій сфері слід розглядати в ширшому контексті оновлення підходів до публічного управління, зміцнення демократичних засад державної діяльності та підвищення рівня професійної відповідальності [144].

Причинами бюрократизму у сфері реалізації державної стратегії протидії інформаційній війні є недостатня увага до проблеми професіоналізму, підготовки та перепідготовки фахівців, залучених до цієї діяльності, а також відсутність дієвої системи стимулювання результативної службової роботи. Лише окремі групи працівників системно підвищують рівень своєї компетентності, займаються самоосвітою та поглиблюють знання у сфері інформаційної безпеки, кіберзахисту, комунікації та аналітичної діяльності. Низький рівень фахової підготовки та формалізм у роботі значною мірою зумовлюються також недосконалістю організаційного забезпечення, збереженням протекціонізму та відсутністю належного запиту на висококваліфікованих спеціалістів у сфері права, інформаційної безпеки, цифрових комунікацій і стратегічного аналізу [5, с. 82–83; 8, с. 241–243]

2. *Удосконалення системи державного управління у сфері протидії інформаційній війні.*

Зазначений напрям передбачає постановку та вирішення таких завдань:

а) перегляд наявного підходу до управління у сфері протидії інформаційній війні з урахуванням змін у безпековому середовищі, розвитку цифрового простору, активізації дезінформаційних кампаній і потреб міжвідомчої координації;

б) забезпечення подальшого розвитку системи публічного управління у цій сфері з метою підвищення її ефективності, професійності, авторитетності, політичної неупередженості, організаційної стійкості та суспільної довіри;

в) зміщення акцентів від переважно адміністративних способів впливу до комплексного застосування правових, організаційних, інформаційних, аналітичних, соціальних та комунікаційних засобів;

г) узгодження заходів протидії інформаційній війні з вимогами загальнодержавної політики у сфері національної безпеки, інформаційної безпеки, цифрового розвитку та міжнародного співробітництва;

ґ) приведення організаційних засад реалізації державної стратегії у відповідність із європейськими стандартами захисту демократичного інформаційного простору;

д) забезпечення відкритості, прозорості, підзвітності та підконтрольності системи державного управління у сфері протидії інформаційній війні, зміцнення правових, організаційних та матеріально-технічних засад її функціонування;

е) упровадження загальновизнаних європейських і міжнародних стандартів у діяльність суб’єктів, відповідальних за реалізацію державної стратегії протидії інформаційній війні, а також використання кращого зарубіжного досвіду, зокрема шляхом забезпечення постійного обміну знаннями між науковцями, викладачами, аналітиками, представниками державних органів, громадянського суспільства та фахівцями-практиками;

Необхідно ураховувати, що в багатьох державах тривалий час перевага надавалася адміністративній інерції, поступовому службовому просуванню та збереженню усталених підходів до організації публічного управління. Проте в умовах посилення інформаційних загроз та швидкої зміни засобів ведення інформаційного протиборства стаж роботи сам по собі вже не може вважатися головним критерієм під час добору осіб до керівництва відповідними напрямами. Значно вагомішими є високі ділові якості, здатність швидко ухвалювати обґрунтовані рішення, ініціативність, аналітичне мислення,

наполегливість та якість виконаної роботи [201, с. 243–244]. Саме такі критерії доцільно покладати в основу оцінювання діяльності посадових осіб, відповідальних за формування та реалізацію державної стратегії протидії інформаційній війні.

3. *Удосконалення системи та адміністративно-правового статусу суб'єктів реалізації державної стратегії протидії інформаційній війні шляхом*:

а) створення системи вертикальної узгодженості всіх ланок суб'єктів, які забезпечують формування та реалізацію державної стратегії протидії інформаційній війні, на загальнодержавному, регіональному та місцевому рівнях із чітким розмежуванням їхніх повноважень, завдань і функцій та налагодженням координації їхньої діяльності;

б) вдосконалення наявних інституційних структур, відповідальних за окремі напрями протидії інформаційній війні, оптимізація та впорядкування їх діяльності на основі гнучкості організаційної побудови, упровадження сучасних засобів аналітичної, комунікаційної та прогностичної роботи;

в) підвищення професійної компетентності працівників органів державної влади та інших суб'єктів, залучених до реалізації державної стратегії протидії інформаційній війні, удосконалення системи їх професійного навчання, спеціальної підготовки та підвищення кваліфікації.

Варто додати, що під час визначення елементів функціональної структури державної стратегії протидії інформаційній війні та дослідження особливостей кожного з них особливого значення набуває стратегічне планування. Воно дає можливість визначити конкретних виконавців, з'ясувати не лише кількісні, а й якісні потреби у ресурсах, розробити планові заходи для контролю за виконанням визначених завдань, здійснювати нагляд за своєчасністю та якістю їх реалізації, а також готувати рекомендаційні, інформаційні й методичні матеріали, спрямовані на подальше вдосконалення державної діяльності у цій сфері. У зв'язку з чим, планування є однією з базових засад забезпечення результативності державної стратегії, виступає

дієвою управлінською функцією, основою для ухвалення важливих рішень і покликане забезпечувати вищий рівень організації діяльності та її послідовність [58].

Основою такого планування є процес визначення головної мети державної діяльності, встановлення пріоритетів, засобів і способів її досягнення, виявлення комплексу робіт і завдань, а також використання дієвих інструментів, ресурсів і організаційних рішень, необхідних для виконання конкретних завдань у визначені строки. Реалізація загальної стратегії має здійснюватися за окремими видами діяльності. Зокрема, у плануванні слід передбачати належне організаційне й матеріально-технічне забезпечення; використання новітніх інформаційних технологій; чітку спеціалізацію структурних підрозділів, тобто розподіл функцій між ними та посадовими особами за окремими напрямами; належну взаємодію між органами державної влади, інститутами громадянського суспільства, медіа та аналітичними структурами. Під час формування державної стратегії протидії інформаційній війні слід враховувати всі аспекти забезпечення ефективної діяльності відповідальних суб'єктів, аби запобігти дублюванню повноважень, втраті часу на погодження рішень, неузгодженості інформаційних повідомлень та ослабленню загальної результативності [58].

Одним із важливих аспектів стратегічного планування є комплекс заходів, спрямованих на підвищення рівня знань, умінь і практичних навичок осіб, залучених до реалізації державної стратегії протидії інформаційній війні. Необхідно систематично розробляти плани навчальних занять, програми підвищення професійної підготовки, заходи з надання індивідуальної методичної допомоги з різних питань, а їх тематика має формуватися на підставі оцінювання діяльності відповідних суб'єктів, аналізу допущених недоліків, перевірок стану інформаційно-аналітичної роботи, комунікаційної діяльності та ведення службової документації.

Не менш важливим є й планування роботи структурних підрозділів як складова загальної державної стратегії. Належна організація щоденної

діяльності суб’єктів, відповідальних за протидію інформаційній війні, що ґрунтується на оперативному плануванні, дає можливість посилити контроль за виконанням визначених завдань, фіксувати результати роботи на кожному етапі, оцінювати її результативність і якість, з’ясовувати рівень дотримання встановлених вимог до кожного виду діяльності та визначати строки їх виконання. Водночас не можна залишати поза увагою питання кадрового, матеріального, інформаційного та аналітичного забезпечення цієї діяльності [150].

З огляду на це, у межах цього напряму державна стратегія протидії інформаційній війні має передбачати вирішення таких завдань:

а) розроблення та впровадження сучасних способів короткострокового і довгострокового прогнозування розвитку інформаційних загроз на загальнодержавному, регіональному та місцевому рівнях;

б) упровадження системи підготовки фахівців із різним освітнім рівнем, професійними, аналітичними, комунікаційними та соціально-психологічними характеристиками;

в) розроблення державної стратегії протидії інформаційній війні з урахуванням запланованих організаційних змін у структурі органів державної влади, утворення нових або припинення діяльності наявних інституцій, зміни їх компетенції, упровадження нових форм і способів діяльності тощо;

г) проведення постійного моніторингу стану інформаційного простору та суспільних настроїв на основі вивчення громадської думки з метою запровадження дієвих, апробованих організаційних, аналітичних і комунікаційних засобів протидії інформаційній війні.

4. *Розвиток системи професійної орієнтації у сфері реалізації державної стратегії протидії інформаційній війні.*

За цим напрямом необхідно активізувати профорієнтаційну роботу в закладах вищої освіти; розробити й упровадити новітні форми і методи інформування в засобах масової інформації та цифровому середовищі; розширити мережу спеціалізованих освітніх програм, центрів підготовки та

міждисциплінарних курсів, орієнтованих на підготовку фахівців у сфері інформаційної безпеки, стратегічних комунікацій, медіааналітики, кіберзахисту та протидії дезінформації; зміцнити гарантії моральної стійкості, професійної визначеності та належного соціального забезпечення молодих спеціалістів, які залучаються до діяльності у цій сфері [75].

5. *Забезпечення системи реалізації державної стратегії протидії інформаційній війні кваліфікованими та компетентними фахівцями:*

а) оновлення кваліфікаційних характеристик і вимог, наявність яких є необхідною умовою для зайняття відповідних посад у державних органах та інших інституціях, залучених до протидії інформаційній війні, зосередження уваги на оцінці професійної підготовки кандидатів, їх спеціальності, практичного досвіду, рівня освіти, аналітичних здібностей, знань, умінь і навичок, комунікативних, ділових, особистих і моральних якостей, рівня мотивації, самоконтролю, здатності працювати в команді, лідерських якостей, прагнення до професійного зростання та постійного підвищення кваліфікації;

б) розроблення і впровадження науково обґрунтованих методик визначення оптимальної штатної чисельності підрозділів та інституцій, відповідальних за окремі напрями протидії інформаційній війні, з метою забезпечення належного співвідношення між результативністю роботи та фактичним навантаженням на кожного працівника;

в) забезпечення рівних умов професійної діяльності для всіх працівників, які займають рівнозначні посади у сфері реалізації державної стратегії протидії інформаційній війні;

г) вжиття заходів, спрямованих на скорочення відтоку кваліфікованих фахівців із відповідних державних органів та установ, зокрема шляхом встановлення гідного рівня оплати праці, розширення соціальних і правових гарантій, створення належних умов професійної діяльності, оскільки низький рівень матеріального забезпечення істотно знижує престижність такої роботи та не сприяє закріпленню у цій сфері висококваліфікованих кадрів;

ґ) створення умов для професійного просування, підвищення рівня кваліфікації, фахового й особистісного розвитку працівників, залучених до реалізації державної стратегії протидії інформаційній війні [1; 169].

6. *Створення дієвої системи професійного відбору кандидатів для діяльності у сфері реалізації державної стратегії протидії інформаційній війні та формування кадрового резерву.*

Вказаний напрям забезпечується шляхом упровадження сучасних конкурсних процедур і рейтингових систем відбору, які відповідають кращим міжнародним стандартам і практикам; створення дієвих конкурсних та дорадчих комісій із залученням представників наукового середовища, громадянського суспільства, профільних органів державної влади та заінтересованих інституцій; дотримання визначених загальних принципів роботи, зокрема прозорості, гласності, об'єктивності, відкритості та неупередженості.

7. *Упровадження ефективних механізмів адаптації та використання професійного потенціалу у сфері протидії інформаційній війні*.

Серед основних завдань державної стратегії в цьому напрямі можна назвати такі:

а) розстановка, розміщення та ротація фахівців і кадрового резерву на основі комплексної оцінки їх практичної діяльності;

б) плановий і раціональний розподіл працівників за напрямами, структурними підрозділами та посадами з урахуванням організаційних змін, професійних і особистих якостей, рівня підготовки та досвіду роботи;

в) розроблення та практична реалізація методик адаптації працівників до діяльності в умовах підвищеного інформаційного тиску, психологічного напруження, постійної зміни інформаційного середовища, швидкого освоєння необхідних професійних умінь і навичок, а також налагодження належної взаємодії в колективі;

Варто згадати і про удосконалення інституту наставництва. У цьому аспекті окремої уваги заслуговує покращення психологічної підготовки

працівників, залучених до реалізації державної стратегії протидії інформаційній війні. Зазвичай під психологічною підготовкою розуміється комплекс взаємопов'язаних і взаємозумовлених заходів, які спрямовані на формування і розвиток якостей та станів, що забезпечують найбільш ефективне виконання професійних завдань [10]. У практичному вимірі така підготовка має бути орієнтована на врахування соціально-психологічних передумов діяльності, оптимізацію умов роботи фахівців, урахування фізіологічних чинників та підвищення їх готовності діяти в напруженому інформаційному середовищі [162].

Психологічна підготовка здійснюється, як правило, як у процесі навчання, так і безпосередньо під час професійної діяльності та має на меті підвищити функціональні можливості психіки, забезпечити належне виконання службових обов'язків, стійкість до професійного виснаження, зовнішнього тиску, маніпулятивного впливу та конфліктних ситуацій [76]. У межах визначеної проблематики психологічна підготовка працівників, відповідальних за реалізацію державної стратегії протидії інформаційній війні, має включати, по-перше, володіння навичками комунікації з населенням, представниками медіа, інститутів громадянського суспільства та іншими суб'єктами інформаційних відносин, що повинно викликати довіру й відчуття належної державної підтримки; по-друге, готовність адекватно реагувати на конфліктні ситуації, інформаційні провокації, кампанії дискредитації, навмисне поширення неправдивих відомостей та інші деструктивні явища.

8. *Професійний розвиток* фахівців шляхом упровадження сучасних підходів, що ґрунтуються на плануванні професійного просування, супроводженні фахового зростання та постійному моніторингу особистісного розвитку працівників; формування дієвого та ефективного кадрового резерву кандидатів на посади керівників усіх ланок управління; розроблення і впровадження нормативно-правових, організаційно-методичних, матеріально-технічних та інших засад роботи з таким резервом; забезпечення постійного

навчання та підвищення кваліфікації працівників, включених до нього [103, с. 110].

9. *Удосконалення системи професійної підготовки фахівців для реалізації державної стратегії протидії інформаційній війні в Україні.*

За цим напрямом першочерговими є такі завдання:

а) розвиток системи спеціалізованої освіти і професійної підготовки фахівців, залучених до реалізації державної стратегії протидії інформаційній війні, а також упровадження механізмів державного замовлення на їх підготовку для різних органів, установ і підрозділів;

б) упровадження рівневої підготовки фахівців: базової, спеціалізованої, підготовки керівників середньої ланки та підготовки керівників вищої ланки, а також удосконалення системи оцінювання якості освіти;

в) впровадження в освітній процес сучасних інформаційних технологій, новітніх методик підготовки кадрів, а також підвищення професійного рівня науково-педагогічних працівників;

г) удосконалення системи перепідготовки кадрів з метою максимального наближення її до практичних потреб державного управління у сфері протидії інформаційній війні;

ґ) планове проведення тренінгових заходів за сучасними програмами підвищення кваліфікації, спрямованими на опанування професійних знань, умінь і навичок, необхідних для роботи в умовах активного інформаційного протиборства;

д) розроблення дієвих праксеологічних заходів взаємодії закладів вищої освіти та наукових установ із державними органами, аналітичними структурами, центрами стратегічних комунікацій та іншими практичними суб’єктами;

е) поглиблення міжнародного співробітництва, розширення програм стажування фахівців у відповідних органах зарубіжних держав, міжнародних організаціях, аналітичних і безпекових центрах [8, с. 241–243; 189, с. 282–283].

Зазначимо, що професійне інформування у цій сфері складається з таких елементів:

1) професійна освіта – має на меті ознайомлення населення зі змістом і умовами професійної діяльності у сфері протидії інформаційній війні, рівнем оплати праці, режимом роботи, перспективами підвищення кваліфікації, різними спеціальностями й посадами у структурі відповідних державних органів та установ;

2) професійна пропаганда – формує у кандидатів позитивне уявлення щодо цієї сфери діяльності, інформує про кращих її представників, історію становлення та професійні традиції, з метою підвищення її суспільного авторитету та об'єктивного сприйняття значення діяльності, спрямованої на захист інформаційного простору держави;

3) професійна агітація, на відміну від професійної пропаганди, що не має чітко визначеного адресата, націлена на залучення до цієї сфери молодих людей, інформування їх про конкретні заклади освіти, освітні програми, умови вступу, навчання та подальшої професійної діяльності.

11. *Упровадження гнучкої системи мотивації працівників, залучених до реалізації державної стратегії протидії інформаційній війні, шляхом*:

а) забезпечення достатнього і стабільного рівня фінансово-матеріального забезпечення, що має ґрунтуватися не лише на посадовому окладі, а й на складності виконуваної роботи, рівні відповідальності, інтенсивності навантаження, особливостях служби в умовах воєнного стану та інших чинниках;

б) упровадження дієвих заходів мінімізації суб'єктивізму та обмеження надмірного впливу керівника на визначення виду й розміру винагороди; розширення системи суспільного і професійного заохочення працівників;

в) аналізу та застосування кращих міжнародних практик підвищення професійної активності, відповідальності й заінтересованості працівників у досягненні реальних результатів.

12. *Упровадження збалансованої системи правового і соціального захисту працівників, які беруть участь у реалізації державної стратегії протидії інформаційній війні*, шляхом:

а) створення ефективної, реально діючої системи правового захисту таких працівників від ризиків і загроз, пов'язаних із їх професійною діяльністю;

б) оптимізації системи гарантій соціального захисту працівників і членів їх сімей з метою забезпечення належного балансу між рівнем оплати праці та додатковими соціальними пільгами і гарантіями;

в) удосконалення системи медичного забезпечення, профілактики та реабілітації працівників;

г) удосконалення системи психологічного забезпечення і психологічного супроводу професійної діяльності осіб, залучених до реалізації державної стратегії протидії інформаційній війні;

ґ) реформування системи соціального і медичного страхування таких працівників;

д) забезпечення доступності житлових програм, пільгового кредитування та інших дієвих соціальних механізмів підтримки;

е) удосконалення системи захисту професійних прав та інтересів працівників, зокрема шляхом оновлення адміністративно-правових засад діяльності їх представницьких і професійних об'єднань, перегляду їх функцій та меж повноважень;

є) гармонізації національного законодавства із законодавством ЄС у частині посилення правового і соціального захисту осіб, діяльність яких пов'язана із забезпеченням інформаційної безпеки держави.

13. *Модернізація організаційно-правового механізму оцінювання ефективності державної стратегії протидії інформаційній війні в Україні*.

Відповідний напрям передбачає:

а) упровадження новітніх методик оцінювання якості й результатів діяльності уповноважених органів, структурних підрозділів та окремих посадових осіб за відповідними напрямами роботи;

б) оновлення критеріїв оцінки, перехід від переважно кількісних до якісних показників; урахування громадської думки; залучення експертного середовища, консультативних та дорадчих органів, а також збільшення частки представників громадськості й наукової спільноти в процедурах оцінювання [41, с. 504].

Оцінювання доцільно розуміти як систематичний процес порівняння діяльності та/чи результатів виконання державної політики, програми або комплексу заходів із поставленими цілями, завданнями, визначеними критеріями та стандартами з метою внесення необхідних управлінських чи політичних змін [117]. У системі органів публічної влади оцінювання виступає аналітичною діяльністю, спрямованою на збір, аналіз, тлумачення та передавання інформації про економічність, ефективність, результативність державної політики, програм і проєктів, які здійснюються з метою забезпечення належного рівня захисту національного інформаційного простору, суспільної стійкості та інформаційної безпеки. Окрім того, оцінювання має бути систематичним і об’єктивним, оскільки воно спрямоване на заплановані, поточні або завершені управлінські впливи і стосується встановлення значущості діяльності, державної політики чи окремої програми.

Серед основних завдань оцінювання у сфері реалізації державної стратегії протидії інформаційній війні слід назвати: забезпечення стабільності здійснення відповідних заходів органами державної влади всіх рівнів відповідно до вимог законодавства та пріоритетів державної політики; постійне вдосконалення якості таких заходів і підвищення рівня суспільної довіри до них; обмеження надмірних витрат і досягнення належної результативності; оптимізацію інформаційного забезпечення процесу прийняття рішень у сфері державної політики; ефективне управління ризиками; вирішення питань раціонального використання наявних ресурсів, у

тому числі бюджетних [168]. Значення оцінювання полягає й у тому, що воно дає змогу визначити, наскільки обрані напрями діяльності та засоби досягнення цілей співвідносяться з фактичними результатами [117].

Саме за допомогою оцінювання можна об'єктивно встановити, які існують недоліки в діяльності органів державної влади та посадових осіб, відповідальних за формування і втілення державної стратегії протидії інформаційній війні. Варто відзначити, що на практиці оцінка діяльності посадових осіб часто проводиться за формальними критеріями, які дають змогу визначити рівень їх професійної підготовки, обсяг виконаної роботи, теоретичні знання та практичні навички. Водночас такий підхід не завжди дає можливість реально оцінити, наскільки ефективно відповідний суб'єкт виконує покладені на нього завдання, якою є якість його взаємодії з іншими органами, медіа, інститутами громадянського суспільства та населенням, а також наскільки результативно він впливає на зниження інформаційних загроз.

З метою покращення якості оцінювання державної стратегії протидії інформаційній війні доцільно, по-перше, проводити анонімні опитування та анкетування. Опитування є одним із найпоширеніших методів дослідження суспільних процесів, а його мета полягає в отриманні інформації про об'єктивні й суб'єктивні факти з боку респондентів [76]; по-друге, використовувати механізми внутрішнього контролю, незалежного аудиту, експертного аналізу та спеціальних перевірочних заходів, які дають змогу оцінити не лише формальні показники, а й фактичну результативність виконаної роботи.

Необхідно зазначити і про розвиток професійної етики та культури службової поведінки у сфері реалізації державної стратегії протидії інформаційній війні шляхом прийняття Кодексу етичної поведінки працівників, діяльність яких пов'язана із забезпеченням інформаційної безпеки; створення системи належних професійних комунікацій і культури службової взаємодії; запобігання деструктивній поведінці працівників;

упровадження апробованих методик профілактики професійного виснаження; формування і підтримання позитивного службового клімату; підвищення якості контролю за додержанням законності, службової дисципліни та антикорупційного законодавства [134].

Поряд із цим варто створити сприятливий психологічний клімат у колективах, які забезпечують формування і втілення державної стратегії протидії інформаційній війні. Для належного виконання покладених обов'язків необхідно, щоб у колективі існували довіра, доброзичлива та доречна критика, можливість вільно висловлювати особисту думку під час обговорення питань, що стосуються службової та професійної діяльності, відсутність тиску з боку керівництва, визнання права працівників ухвалювати самостійні рішення в межах їх компетенції, взаємна підтримка та взаємодопомога. Задоволення своєю належністю до колективу підвищує ефективність праці й посилює відповідальність кожного працівника за стан справ [68].

14. *Внутрішнє забезпечення державної стратегії протидії інформаційній війні в Україні*, яке передбачає:

а) інформаційно-технологічне супроводження шляхом розроблення та впровадження єдиної інформаційної платформи, удосконалення облікової, аналітичної та статистичної роботи;

б) покращення фінансового, матеріально-технічного й ресурсного забезпечення;

в) проведення науково-праксеологічних досліджень із використанням механізмів прогнозування, планування та моніторингу проблем у сфері інформаційної безпеки та протидії інформаційній війні.

До цього напряму доцільно віднести й налагодження тісної взаємодії та співпраці між практичними органами державної влади, з одного боку, та закладами вищої освіти, науковими установами, аналітичними центрами, інститутами громадянського суспільства й профільними міжнародними структурами – з іншого, а також проведення спільних заходів; вивчення та

впровадження зарубіжного досвіду організації діяльності у сфері протидії інформаційній війні та міжнародних стандартів забезпечення інформаційної безпеки [24].

Отже, з метою вирішення і врегулювання окреслених проблемних питань щодо вдосконалення державної стратегії протидії інформаційній війні в Україні доцільно визначити основний напрям удосконалення її організаційно-правових засад, а саме: закріплення на законодавчому рівні стратегічних напрямів державної політики у цій сфері, її цілей та завдань, особливостей реалізації, зокрема, шляхом розроблення та прийняття нової *Державної стратегії протидії інформаційній війні в Україні*, у якій доцільно визначити: правову основу державної стратегії протидії інформаційній війні в Україні; поняття та мету державної стратегії протидії інформаційній війні; чинники, що впливають на ефективність її формування та реалізації; основні принципи державної стратегії протидії інформаційній війні; основні проблеми у цій сфері та напрями їх подальшого вирішення; цілі та завдання державної стратегії протидії інформаційній війні; очікувані результати досягнення поставлених цілей і виконання визначених завдань.

Наостанок зазначимо, що вдосконалення державної стратегії протидії інформаційній війні в Україні тривалий час залишатиметься одним із пріоритетних завдань діяльності держави. Належне організаційно-правове забезпечення роботи органів публічної влади у цій сфері є важливим критерієм дієвості всього механізму захисту національного інформаційного простору, а відтак – показником результативності державної політики у сфері національної безпеки. Зазначене стосується питань покращення організації роботи відповідних органів, посилення контролю за результативністю їх діяльності, запровадження новітніх інформаційних технологій, вироблення комунікаційної стратегії для інформування суспільства про діяльність держави у цій сфері та зміцнення суспільної довіри.

Безумовно, належна організація роботи та ефективне виконання завдань, що покладаються на суб’єктів реалізації державної стратегії протидії

інформаційній війні, безпосередньо залежать від знань, професійних якостей, рівня підготовки та відповідальності як керівництва, так і кожного окремого працівника. Проте вирішення цих питань значною мірою залежить від якості організаційно-правового забезпечення (публічного управління). У цьому аспекті державна політика має бути спрямована насамперед на покращення становища відповідних органів і установ, належну організацію роботи кожного з них та адаптацію національних підходів до міжнародних цінностей і стандартів, упровадження яких сприятиме зміцненню довіри громадян, посиленню авторитету держави та підвищенню результативності її діяльності в інформаційній сфері.

Висновки до розділу 3

1. Виокремлено основні проблеми реалізації державної стратегії протидії інформаційній війні, серед яких: зростання вразливості державних цифрових ресурсів до кібератак, інформаційного втручання та технічного блокування; нерівномірний рівень використання електронних державних сервісів населенням; залежність значної частини аудиторії від соціальних мереж і цифрових платформ як основних каналів отримання новин; поширення через такі платформи маніпулятивного контенту, фейкових повідомлень і ворожих наративів; недостатня узгодженість між розвитком цифрових послуг, їх кіберзахистом і належним інформаційним супроводом з боку держави. Зокрема, за наявними даними застосунок «Дія» охоплює близько 75% користувачів, тоді як «Електронний суд» – лише 40%, що свідчить про нерівномірність цифрового залучення населення до державних сервісів. Водночас для отримання новин Facebook використовують близько 60% аудиторії, YouTube – 55%, Telegram –50%, а це підтверджує високу залежність інформаційного споживання від платформного середовища. В цілому ж основні труднощі реалізації державної стратегії протидії інформаційній війні зосереджені у технічній, комунікаційній та організаційній

площинах. Наведені показники додатково свідчать, що держава одночасно стикається з двома взаємопов'язаними викликами: необхідністю захищати дедалі ширший масив цифрових сервісів і потребою ефективно діяти в інформаційному середовищі, де основними каналами впливу на аудиторію залишаються соціальні мережі та цифрові платформи.

2. Вдосконалення державної стратегії протидії інформаційній війні в Україні має здійснюватися за взаємопов'язаними організаційно-правовими, інституційними, кадровими та функціональними напрямами. До основних із них віднесено: створення дієвого механізму нормативного та організаційного регулювання у цій сфері; удосконалення системи публічного управління та адміністративно-правового статусу суб'єктів реалізації стратегії; розвиток професійної орієнтації, професійного відбору, формування кадрового резерву, адаптації, підготовки, перепідготовки та професійного розвитку фахівців; забезпечення системи реалізації стратегії кваліфікованими і компетентними кадрами; упровадження гнучкої системи мотивації, а також належного правового і соціального захисту працівників; модернізацію механізму оцінювання ефективності державної стратегії та посилення її внутрішнього забезпечення. Доведено, що вирішення лише окремих із зазначених питань не забезпечить належного результату, оскільки ефективність державної стратегії у цій сфері прямо залежить від узгодженості правових засад, інституційної спроможності та кадрового потенціалу.

3. Основним напрямом удосконалення організаційно-правових засад державної стратегії протидії інформаційній війні визначено закріплення на законодавчому рівні її стратегічних напрямів, цілей, завдань і особливостей реалізації шляхом розроблення та прийняття нової Державної стратегії протидії інформаційній війні в Україні. Запропоновано, щоб у її змісті, з урахуванням проведеного дослідження були чітко визначені: правова основа державної стратегії; поняття та мета; чинники, що впливають на ефективність її формування та реалізації; основні принципи; проблеми у цій сфері та

напрями їх подальшого вирішення; цілі й завдання; очікувані результати виконання.

ВИСНОВКИ

У **дисертації**, на основі комплексного аналізу наукових напрацювань вітчизняних учених у галузі публічного управління та адміністрування, національного законодавства, правоохоронної практики та зарубіжного досвіду, розроблені напрями розроблені напрями формування та реалізації державної стратегії протидії інформаційній війні з урахуванням умов воєнного стану. Сукупність одержаних висновків і рекомендацій має важливе значення для вдосконалення організаційно-управлінських механізмів координації суб'єктів державної політики у відповідній сфері, підвищення результативності стратегічних комунікацій, забезпечення інформаційної стійкості держави та суспільства, а також зміцнення спроможності публічної влади своєчасно виявляти, попереджати й нейтралізувати загрози інформаційного характеру, зокрема:

1. Встановлено, що інформаційна війна в сучасних воєнно-політичних умовах перетворилася на один із базових різновидів загроз інформаційній безпеці держави, оскільки її вплив спрямований не лише на поширення неправдивої інформації, а й на підрив довіри до органів публічної влади, послаблення національної стійкості, дестабілізацію суспільних процесів, викривлення історичної пам'яті та формування сприятливого середовища для зовнішнього політичного й інформаційного тиску. Для сфери публічного управління та адміністрування така загроза має системний характер, а отже потребує не ситуативних рішень, а послідовної, інституційно забезпеченої й науково обґрунтованої державної політики.

2. Доведено, що сучасні пропагандистські технології становлять самостійний механізм деструктивного впливу на інформаційний простір держави. Виокремлено історичний аспект пропагандистського впливу та встановлено, що особливо небезпечними є історичні фальсифікації, маніпулювання колективною пам'яттю, міфологізація минулого, нав'язування псевдоісторичних наративів, а також викривлення фактів, пов'язаних із

державотворенням України. До найбільш поширених пропагандистських технологій віднесено масове поширення фейкових повідомлень, селективний добір і замовчування фактів, використання емоційного тиску, анонімних цифрових ресурсів, бот-мереж, псевдоекспертного середовища, візуальних маніпуляцій та прихованих форм інформаційного впливу.

3. Обґрунтовано, що державна інформаційна політика має розглядатися як головний інструмент протидії пропаганді та інформаційній війні. Встановлено, що її сучасний стан характеризується низкою системних проблем, серед яких фрагментарність інформаційного законодавства, недостатня узгодженість діяльності суб'єктів публічної влади, певна вразливість цифрового середовища до дезінформаційних кампаній, нерівномірність комунікаційної інфраструктури та обмежений розвиток просвітницьких механізмів. У зв'язку з цим доведено необхідність переходу від розрізнених заходів реагування до цілісної концепції державної інформаційної політики, у межах якої поєднуватимуться правові, організаційні, безпекові, медійні, технологічні та освітньо-просвітницькі засоби. У даній концпецій запропоновано визначити мету, принципи, завдання, напрями реалізації, систему суб'єктів, механізми впровадження, етапи реалізації та показники результативності. Окремо обґрунтовано поділ суб'єктів її реалізації на три рівні: суб'єкти стратегічного формування політики; суб'єкти безпосередньої реалізації та координації; суб'єкти суспільної підтримки, громадського контролю й інформаційного партнерства. Така Концепція повинна бути використана як методологічна та прикладна основа для вдосконалення державної інформаційної політики України.

4. На підставі аналізу зарубіжного досвіду встановлено, що найбільш результативні механізми протидії інформаційній війні у провідних країнах Європи та США спираються на поєднання інституційно оформлених стратегічних комунікацій, міжвідомчої координації, розвитку медіаграмотності, міжнародного партнерства та залучення суспільства до зміцнення інформаційної стійкості. Доведено, що для України практичне

значення мають не механічне копіювання окремих іноземних інституцій, а адаптація перевірених управлінських рішень, зокрема щодо посилення координаційного центру, інституціоналізації медіаграмотності, розвитку урядових стратегічних комунікацій та спеціалізованого моніторингу зовнішніх інформаційних впливів.

5. Визначено, що формування державної стратегії протидії інформаційній війні повинно здійснюватися на основі чіткої системи принципів і стратегічних засад. До принципів віднесено: верховенство права та законність; пріоритет прав і свобод людини; ідеологічну багатоманітність і недопустимість цензури; достовірність, повноту та своєчасність офіційної інформації; системність і міжвідомчу координацію; стійкість та адаптивність держави і суспільства; міжнародну взаємодію; поєднання інформаційної та кібернетичної складових безпеки. До стратегічних засад віднесено конституційно-безпекову природу такої стратегії, її включеність у систему стратегічного планування, міжсекторальний характер, доказовість, ресурсну забезпеченість, чіткий механізм реалізації та зовнішньополітичний вимір. Доведено, що лише за наявності таких орієнтирів державна стратегія набуває внутрішньої цілісності, правової визначеності та орієнтована на покриття практичних проблем.

6. З’ясовано, що інституційний механізм формування та реалізації державної стратегії протидії інформаційній війні є складною системою взаємопов’язаних суб’єктів, повноважень, процедур координації та засобів реагування, через які забезпечується вироблення, ухвалення та практичне виконання стратегічних рішень у сфері інформаційної безпеки. Його ефективність залежить не від кількості залучених інституцій, а від точності розмежування компетенції, стабільності міжвідомчої взаємодії, узгодженості публічних комунікацій, поєднання інформаційного та кібернетичного напрямів, належного кадрового забезпечення та наявності механізму оцінювання результатів. Водночас встановлено, що сучасний стан цього механізму потребує подальшого вдосконалення через розпорошення

повноважень, недостатню процедурну визначеність і нерівномірний рівень інституційної спроможності окремих суб'єктів.

7. Виокремлено основні проблеми реалізації державної стратегії протидії інформаційній війні, до яких віднесено незахищеність державних цифрових ресурсів до кібератак, інформаційного втручання та технічного блокування; нерівномірний рівень користування електронними державними сервісами; високу залежність інформаційного споживання населення від соціальних мереж та інших цифрових платформ; поширення через них маніпулятивного контенту, фейкових повідомлень і ворожих наративів; недостатню узгодженість між розвитком цифрових послуг, їх кіберзахистом і належним інформаційним супроводом. Перелічені проблеми мають взаємопов'язаний характер, оскільки розширення цифрових сервісів без належного технічного захисту підвищує вразливість держави до зовнішнього інформаційного впливу, а залежність населення від платформного середовища посилює ризик швидкого поширення дезінформації та маніпуляцій. Основні труднощі реалізації державної стратегії у цій сфері зосереджені в технічній, комунікаційній та організаційній площинах, що свідчить про необхідність комплексного посилення цифрової стійкості держави, безпечного функціонування електронних сервісів, оперативного інформаційного реагування та підвищення довіри населення до офіційних джерел інформації.

8. Вдосконалення державної стратегії протидії інформаційній війні має бути пов'язане з прийняттям нового стратегічного документа, у якому повинні бути чітко визначені правова основа, понятійний апарат, принципи, стратегічні цілі, основні завдання, суб'єкти реалізації, механізми міжвідомчої координації, порядок інформаційно-аналітичного супроводу, критерії оцінювання ефективності, проблеми реалізації та напрями їх подолання, а також очікувані результати виконання. Обґрунтовано, що в такому документі доцільно окремо закріпити систему загроз інформаційній безпеці, пріоритетні напрями державного реагування, заходи щодо поєднання інформаційної безпеки та кіберзахисту, розвиток стратегічних комунікацій, механізми

взаємодії з громадянським суспільством і міжнародними партнерами, а також питання кадрового, фінансового й технологічного забезпечення. Створення відповідного документа дозволить перевести державну політику у сфері протидії інформаційній війні з рівня розрізнених управлінських рішень у площину цілісної, нормативно визначеної, інституційно узгодженої та результативної системи публічного управління.

СПИСОК ВИКОРИСТАНИХ ДЖЕРЕЛ

1. Актуальні проблеми адміністративно-правового регулювання діяльності Національної поліції України : монографія / Гусаров С. М., Салманова О. Ю., Комзюк А. Т., Музичук О. М., Казанчук І. Д. Харків : Факт, 2022. 452 с.

2. Актуальні проблеми управління інформаційною безпекою держави : зб. тез наук. доп. наук.-практ. конф. (Київ, 4 квіт. 2019 р.). Київ : Нац. акад. СБУ, 2019. 384 с.

3. Анісімов К. Г. General Data Protection Regulation: Perspective Ways for Ukrainian Legislation and Business Development. *Право та інновації.* 2018. № 2(22). С. 103–110. DOI: 10.31359/2311-4894-2018-22-2-103.

4. Арзуманов Г. Л., Мокроусова О. Ю. DSA як модель для гармонізації українського законодавства у сфері цифрових послуг. *Юридичний науковий електронний журнал*. 2025. № 11. С. 45–50. DOI : https://doi.org/10.32782/2524-0374/2025-11/8

5. Аулін О., Ауліна О. Стратегічні комунікації у протидії деструктивним російським наративам. *Стратегічні комунікації.* 2023. С. 82–95.

6. Бакаєвич К. Український телемарафон «Єдині новини» під час повномасштабного російського вторгнення: пропаганда, піар чи необхідність? *Integrated communications*. 2024. № 1 (17). С. 139–144. URL : https://intcom.kubg.edu.ua/index.php/journal/article/download/321/272

7. Баран М. В. Адміністративно-правове забезпечення інформаційної безпеки в Україні : дис. … докт. філософ. 081 – Право. Львів, 2022. 244 с.

8. Бігун В. М. Міністерство культури та стратегічних комунікацій України в системі суб'єктів захисту національних інтересів в інформаційній сфері. *Науковий вісник Ужгородського Національного Університету.* Серія : Право. 2024. Вип. 85. Ч. 2. С. 241–247.

9. Бондар В. Т. Фактор перспективи США та протидія дезінформації: удосконалення системи національної безпеки *Вчені записки ТНУ імені В. І. Вернадського*. Серія : Публічне управління та адміністрування. 2023. Т. 34 (73). № 5. С. 94–98.
URL: http://www.pubadm.vernadskyjournals.in.ua/journals/2023/5_2023/16.pdf

10. Бондаренко О. Ф. Психологічна допомога особистості. Харків, 1996. 184 с.

11. Бондаренко С. Інформаційна політика органів влади у контексті брендингу територій. *Модернізація соціогуманітарного простору*: історичний досвід, виклики та перспективи : зб. матеріалів Всеукр. наук.-практ. конф. з міжнар. участю (м. Вінниця, 14–15 трав. 2015 р.). Вінниця, 2015. С. 223–224.

12. Бочарова Н. В., Биков О. М. Праволюдинний зміст сучасної цифрової стратегії Європейського Союзу. *Вісник Університету імені Альфреда Нобеля*. Серія «Право». 2022. № 1 (4). С. 34–42. URL: https://law.duan.edu.ua/images/PDF/2022/1/4.pdf

13. Брижко В. М. Сучасні основи захисту персональних даних в європейських правових актах. *Інформація і право*. 2016. № 3 (18). С. 45–57. DOI: 10.37750/2616-6798.2016.3(18).272967.

14. Брижко В. М., Дзьобань О. П. Дезінформація як фактор маніпулювання свідомістю. *Інформація і право.* 2023. № 2 (45). С. 50–63.

15. Будівська Г. Й. Функції журналістики в нормативних теоріях медіа та інтерпретаціях медіапрофесіоналів. *Обрії друкарства*. 2018. № 1 (6). С. 40–48. URL : https://horizons.vpi.kpi.ua/article/download/132818/129361/285764

16. Варжанський І. В. Застосування моделей рефлексивного управління в діяльності органів державної влади в умовах воєнно-політичних викликів : дис. ... докт. філософ. 281 – Публічне управління та адміністрування. К., 2025. 309 с. URL : ela.kpi.ua/bitstreams/9213dd16-93a0-4225-8d21-88ea004f3609/download.

17. Васильєва Н. В. Пропаганда як складова інформаційно-комунікативної політики і загроза національній безпеці. *Таврійський науковий*

вісник. Серія : Публічне управління та адміністрування. 2022. С. 34–41. URL : https://journals.ksauniv.ks.ua/index.php/public/article/view/201/188.

18. Воробець Н. Р. Інституційні особливості формування та функціонування інформаційної безпеки в Україні: аналіз та перспективи розвитку. *Регіональні студії.* 2023. № 34. С. 75–80. URL : https://regionalstudies.uzhnu.uz.ua/archive/34/12.pdf

19. Глинський Н. Ю., Сохацька О. О. Вплив лідерів думок на громадську думку і поведінку молоді в умовах цифрового середовища. С. 142–151. URL : https://science.lpnu.ua/sites/default/files/journal-paper/2025/may/38876/250524maket-144-153.pdf

20. Головка А. А. Інститути громадянського суспільства в системі інформаційної безпеки України. *Вісник НТУУ «КПІ». Політологія. Соціологія. Право.* 2015. № 3–4 (27/28). С. 13–16. URL : https://socio-journal.kpi.kiev.ua/archive/2015/3-4/4.pdf

21. Голуб'як І., Голуб'як Н. Політичні ініціативи ЄС для підтримки розвитку інформаційного суспільства. *Вісник Прикарпатського університету*. Серія : Політологія. 2024. Вип. 18. С. 92–100. URL : https://lib-repo.pnu.edu.ua/bitstream/123456789/23169/1/14%20%282%29.pdf

22. Горбань Ю. О. Інформаційна війна проти України та засоби її ведення. *Вісник Національної академії державного управління при Президентові України.* 2015. № 1. С. 136–141.

23. Горлач М. І., Кремень В. Г. Політологія: наука про політику: підручник. Київ : Центр учбової літератури, 2009. 840 с.

24. Горяченко Р. І. Загальна характеристика кадрової політики в органах Національної поліції України. *Сучасні погляди на актуальні питання правових наук* : матеріали Міжнар. наук.-практ. конф. (м. Запоріжжя, 27–28 листоп. 2020 р.). Запоріжжя, 2020. С. 19–23.

25. Грабовець І. М., Михальчук Н. В. Стратегія кризової комунікації у системі «влада – громадськість» в умовах воєнного стану в Україні: етапи, чинники, характерні риси. *Grani.* 2025. Т. 28. № 2. С. 305–315.

26. Грицай Р. О. Інформаційна політика у протидії пропаганді. *Наукові інновації та передові технології.* 2026. № 3 (55). С. 3005–3015. https://doi.org/10.52058/2786-5274-2026-3(55)-3005-3015

27. Грицай Р. О. Інформаційні війни: пошук стратегій протидії. *Публічне управління і адміністрування в Україні.* 2023. № 33. С. 18–23. URL : https://pag-journal.iei.od.ua/archives/2023/33-2023/3.pdf https://doi.org/10.32782/pma2663-5240-2023.33.3

28. Грицай Р. О. Концептуальні засади національної інформаційної політики як превентивний механізм протидії пропаганді. *Актуальні питання діяльності Національної поліції як суб'єкту протидії організованій злочинності :* матеріали Всеукр. наук.-практ. конф. (Кропивницький, 2 квіт. 2026 р.). Кропивницький, 2026.

29. Грицай Р. О. Практики та інструменти протидії інформаційній війні: досвід зарубіжних країн. *Публічне управління і адміністрування в Україні.* 2024. № 39. С. 14–19. URL : https://pag-journal.iei.od.ua/archives/2024/39-2024/4.pdf https://doi.org/10.32782/pma2663-5240-2024.39.2

30. Грицай Р. О. Протидія пропаганді в Україні: інформаційна політика та безпекові виклики. *Фінансова політика: теоретичні та практичні аспекти юридичної науки. Тема року: Сучасний міжнародний правопорядок та міжгалузеві правові процеси :* матеріали VIII Міжнар. наук.-практ. конф. (Ірпінь, 2 квіт. 2026 р.). Ірпінь, 2026.

31. Грицай Р. О. Сучасні методи пропаганди як фактор загроз національній інформаційній безпеці держави. *Національні інтереси України.* 2026. № 3 (20) С. 1150–1162. https://doi.org/10.52058/3041-1793-2026-3(20)-1150-1162

32. Громадське обговорення проєкту розпорядження Кабінету Міністрів України «Про затвердження Плану заходів з реалізації Стратегії інформаційної безпеки на період до 2025 року» URL : https://mkip.gov.ua/news/7512.html

33. Данильян О., Дзьобань О. Інформаційна війна у медіапросторі сучасного суспільства. *Вісник НЮУ імені Ярослава Мудрого. Серія: Філософія, філософія права, політологія, соціологія.* 2022. № 3 (54). С. 11–29. URL : https://fil.nlu.edu.ua/article/view/265589
DOI: https://doi.org/10.21564/2663-5704.54.265589

34. 2023 року кількість зареєстрованих кіберінцидентів зросла на 62,5 %: звіт оперативного центру реагування на кіберінциденти ДЦКЗ. *Державна служба спеціального зв'язку та захисту інформації України.* URL : https://cip.gov.ua/ua/news/2023-roku-kilkist-zareyestrovanikh-kiberincidentiv-zrosla-na-62-5-zvit-operativnogo-centru-reaguvannya-na-kiberincidenti-dckz

35. Де Лара Ф. Дезінформація і пропаганда за доби постправди. *Соціологія: теорія, методи, маркетинг*. 2018. № 4. С. 64–72. URL : http://nbuv.gov.ua/UJRN/stmm_2018_4_6

36. Державна служба спеціального зв'язку та захисту інформації України офіц. вебсайт. CERT-UA у 2025 році опрацювала майже 6000 кіберінцидентів: кількість ворожих атак зросла на 37 %. URL : https://cip.gov.ua/ua/news/cert-ua-u-2025-roci-opracyuvala-maizhe-6000-kiberincidentiv-kilkist-vorozhikh-atak-zrosla-na-37

37. Деякі питання діяльності Міністерства культури : Постанова Кабінету Міністрів України від 16 жовт. 2019 р. № 885. URL : https://zakon.rada.gov.ua/go/885-2019-%D0%BF

38. Деякі питання реагування на кіберінциденти, кібератаки та кіберзагрози : Постанова Кабінету Міністрів України від 26 листоп. 2025 р. № 1533. URL : https://zakon.rada.gov.ua/go/1533-2025-%D0%BF

39. Дмитренко М. А. Національна безпека України: забезпечення в інформаційній сфері : монографія. К., 2021. 325 с.

40. Дубов Д. В. Стратегічні комунікації: проблеми концептуалізації та практичної реалізації. *Стратегічні пріоритети.* 2016. № 4 (41). С. 9–23.

41. Енциклопедичний словник з державного управління / уклад.: Ю. П. Сурмін та ін. ; за ред. Ю. В. Ковбасюка, В. П. Трощинського, Ю. П. Сурміна. Київ : НАДУ, 2010. 820 с.

42. Європейські практики цифрової трансформації: уроки для України. *Інститут євроатлантичного співробітництва.* 2021. URL : https://ieac.org.ua/

43. Єжижанська Т. С. Лідери думок як суб'єкти й інструменти комунікації видавництва. *Вісник Харківського національного університету імені В. Н. Каразіна.* Серія : Соціальні комунікації. 2017. Вип. 12. URL : https://elibrary.kubg.edu.ua/id/eprint/25570/1/T_Yezhyzhanska_VHNU_12.pdf

44. Жуган Вікторія Доктрина інформаційної безпеки України – це лише декларація – експерти.
URL : https://www.radiosvoboda.org/a/28336852.html

45. Захаренко К. В. Відповідальність засобів масової інформації в системі інформаційної безпеки суспільства. *Політикус*. 2019. № 5. С. 4–9.

46. Захаренко К. В. Інституційний вимір інформаційної безпеки України: трансформаційні виклики, глобальні контексти, стратегічні орієнтири : автореф. дис. ... д-ра політ. наук : 23.00.02. Львів, 2021. 37 с. URL : https://lnu.edu.ua/wp-content/uploads/2021/04/aref_zakharenko.pdf

47. Звернення Президентки Європейської Комісії фон дер Ляєн на Всесвітньому економічному форумі.
URL : https://www.eeas.europa.eu/delegations/ukraine/special-address-president-von-der-leyen-worldeconomic-forum_en?s=232

48. Звіт Національної ради України з питань телебачення і радіомовлення за 2024 рік. К., 2025. С. 131–132. URL : https://kompkd.rada.gov.ua/uploads/documents/35332.pdf

49. Звоздецька О. Дезінформація як загроза національній безпеці Європейського Союзу : проблеми та підходи. *Історико-політичні проблеми*

сучасного світу. 2021, Т. 43. С. 30–39. URL : http://nbuv.gov.ua/UJRN/Ippss_2021_43_5

50. Звоздецька О. Я. Інституційні механізми протидії дезінформації в ЄС: проблеми та здобутки. *Медіафорум: аналітика, прогнози, інформаційний менеджмент.* 2022. Т. 10. С. 107–122. URL : journals.chnu.edu.ua/mediaforum/article/view/89

51. Зеленін В. В. Психотехнології інформаційної війни. *Імперативи розвитку цивілізації.* 2015. № 2. С. 136–139.

52. Зибарева О. В. Дезінформація щодо надзвичайних ситуацій як деструктивний фактор розвитку регіональних суспільних систем. *Економіка та держава*. 2014. № 1. С. 6–8. URL : http://nbuv.gov.ua/UJRN/ecde_2014_1_3

53. Зражевська Н. І. Комунікаційні технології : лекції. Черкаси : Брама-Україна, 2010. 224 с. URL : https://eprints.cdu.edu.ua/241/1.pdf

54. Зубков В. П. Механізм впливу на інформаційні системи противника як складова інформаційного забезпечення сил оборони України. *Збірник наукових праць Центру воєнно-стратегічних досліджень Національного університету оборони України*. 2023. № 2 (78). С. 27–34. URL : znp-cvsd.nuou.org.ua/article/view/290202.

55. Зубчик О. А., Грицай Р. О. Державна стратегія захисту когнітивного простору: архітектоніка та управлінські інструменти формування суспільної резильєнтності. *Актуальні проблеми інноваційної економіки та права.* 2026. № 1. С. 132–138. https://doi.org/10.36887/2524-0455-2026-1-32

56. Зубчик О. А., Грицай Р. О. Функціональна конвергентність суб'єктів публічного управління в системі протидії семантичним загрозам. *Актуальні проблеми інноваційної економіки та права.* 2025. № 4. С. 127–131. https://doi.org/10.36887/2524-0455-2026-1-27

57. Іваненко В., Кривошеїн В. Державна політика пам'яті в сучасній Україні в умовах інформаційної війни (2014–2021 рр.). *Науково-теоретичний*

альманах Грані. № 25 (2). С. 16–21. URL : https://grani.org.ua/ndex.php/journal/article/view/1756

58. Іноземцева К. О. Кадрова політика в системі судоустрою як основа якісного правосуддя. *Правові новели*. 2019. № 8. С. 76–81.

59. Інформаційна безпека особистості, суспільства, держави : підручник / Жарков Я. М., Дзюба М. Т., Замаруєва І. В. та ін. Київ : Видавничо-поліграфічний центр «Київський університет», 2008. 274 с.

60. Інформаційна безпека сучасного суспільства : навчальний посібник / за заг. ред. А. І. Міночкіна. Київ : ВІТІ НТУУ «КПІ», 2006. 188 с. URL : viknu.mil.gov.ua/

61. Інформаційна безпека : підручник / В. В. Остроухов, М. М. Присяжнюк, О. І. Фармагей, М. М. Чеховська та ін. ; Під ред. В. В. Остроухова. Київ : Ліра-К, 2021. 412 с.

62. Історія інформаційно-психологічного протиборства : підручник / Я. М. Жарков, Л. Ф. Компанцева, В. В. Остроухов, В. М. Петрик, М. М. Присяжнюк, Є. Д. Скулиш ; за заг. ред. Є. Д. Скулиша. Київ : НАСБУ, 2012. 212 с.

63. Калініченко Б. Інформаційне протиборство: ретроспективний аналіз світової історії. *Вісник Черкаського університету.* Серія: Історичні науки. 2025. № 1. С. 14–18.

64. Калініченко Б. Трансформація сучасної інформаційної парадигми глобальної цивілізації. *Політологічний вісник.* 2025. № 96. С. 238–246. URL : https://zpv.knu.ua/index.php/pb/article/view/336/331 https://doi.org/10.17721/2415-881x.2025.96.238-246

65. Карапетян О. О. Адміністративно-правове забезпечення свободи слова та права на інформацію в умовах обмежень, пов'язаних із пропагандою війни і дезінформацією : дис. … докт. філософ. Запоріжжя, 2025. 235 с. URL : https://phd.znu.edu.ua/page/Doc/2025/karapetyan_o/Karapetian_O_.pdf

66. Карасаєв С. У., Лікарчук Н. В. Міжнародні аспекти використання інформаційних технологій у державному управлінні. *Міжнародні відносини:*

теоретико-практичні аспекти. 2023. № 12. С. 151–163. URL : https://international-relations.knukim.edu.ua/article/view/292411/285582 https://doi.org/10.31866/2616-745X.12.2023.292411

67. Карташов П. І. Захист цифрових прав особи. *Право і суспільство*. 2025. № 1. С. 576–581. DOI : https://doi.org/10.32842/2078-3736/2025.1.84. URL: https://pravoisuspilstvo.org.ua/archive/2025/1_2025/86.pdf

68. Клочко А. М. Кадрове забезпечення органів внутрішніх справ України: порядок та основні елементи. *Форум права*. 2014. № 4. С. 175–180.

69. Кобко Є. В. Інформаційна війна та дезінформація: вплив на національну безпеку України. *Правові новели.* 2023. № 20. С. 141–147. URL : https://legalnovels.in.ua/journal/20_2023/20.pdf

70. Козаков В., Стадник Ю. Державно-управлінські стратегії в інформаційній війні з агресором. *Публічно-управлінські та цифрові практики.* 2025. Вип. 4 (7).
URL : https://journals.dut.edu.ua/index.php/public/article/view/3373

71. Козьміних А. В. Складники механізму реалізації інформаційної політики України. *Політикус.* 2020. Вип. 2. С. 52–58. URL : https://politicus.od.ua/2_2020/9.pdf

72. Коломоєць Т. О. Сучасні завдання національної системи стратегічних комунікацій в Україні. *Law. State. Society.* 2024. С. 20–27. URL : https://www.lsej.org.ua/8_2024/148.pdf

73. Кондратенко В. М., Мігалатюк В. В. Адміністративно-правові засади забезпечення діяльності органів публічної влади у сфері інформаційної безпеки України. *Аналітично-порівняльне правознавство.* 2025. № 3. Ч. 2. С 27–132. URL : https://app-journal.in.ua/wp-content/uploads/2025/06/22-1.pdf

74. Конституція України від 28 черв. 1996 р № 254к/96-ВР. URL : https://zakon.rada.gov.ua/laws/show/254%D0%BA/96-%D0%B2%D1%80#Text

75. Користін О. Є., Свиридюк Н. П. Оцінювання гібридних загроз та спроможностей протидії їм при формуванні стратегічних комунікацій.

Науковий вісник Ужгородського Національного Університету. Серія: Право. 2023. Вип. 77. Ч. 2. С. 66–74.

76. Корнєєв Ю. В. Адміністративно-правове забезпечення особистої безпеки працівників податкової міліції : дис. … канд. юрид. наук: 12.00.07. Ірпінь, 2002. 196 с.

77. Косиця О. О. Інституціональний механізм системи інформаційної безпеки. *Порівняльно-аналітичне право.* 2016. № 4. С. 150–153. URL : https://dspace.univd.edu.ua/server/api/core/bitstreams/3d130e83-16eb-4cdc-b32e-c70b53618061/content

78. Красноступ Г. М. Правові засади медіаграмотності: від теоретичної концепції до інституціоналізації в державі. *Інформація і право.* 2025. № 3 (54). С. 19–29.

79. Крикун В., Бауліна Т. Дезінформація як засіб гібридної війни : сутність і наслідки. *Вісник Київського національного університету імені Тараса Шевченка.* Філософія. 2022. Вип. 2. С. 30–33. URL : http://nbuv.gov.ua/UJRN/ VKNUF_2022_2_7

80. Курбан О. Бойові наративи в системі сучасних геополітичних інформаційних війн (досвід російсько-української гібридної інформаційної війни 2014–2021 рр.). *Синопсис: текст, контекст, медіа.* 2021. № 27 (3). С. 149–158. URL : http://nbuv.gov.ua/UJRN/stkm_2021_27(3)__6.

81. Кутуза Н. В., Тельпіс Д. М. Дезінформація як складник ІПсО в мегадискурсі: маніпулятивний аспект (на прикладі російсько-української війни періоду повномасштабного вторгнення). *Записки з українського мовознавства*. 2023. Вип. 30. С. 282–292. URL : http://nbuv.gov.ua/UJRN/zukm_2023_30_28

82. Липовська Н. А., Сахарова К. О. Стратегічні комунікації в умовах війни: публічно-управлінський аспект. *Наукові перспективи*. 2024. № 6 (48). С. 181–192.
URL : https://perspectives.pp.ua/index.php/np/article/download/12754/12816/12816

83. Ліснецька А. Дезінформація в новинному відеоконтенті : маркери та методи розпізнавання. *Вісник Львівського університету*. Серія : Журналістика. 2019. Вип. 45. С. 60–66. URL : http://nbuv.gov.ua/UJRN/VLNU_Jur_2019_45_10

84. Любовець Г. Контент негативу. Як захистити себе та країну в умовах тотального інформаційного протистояння : монографія. Київ : Видавничий дім «Києво-Могилянська академія», 2021. 266 с.

85. Магда Є. В. Виклики гібридної війни: інформаційний вибір. *Наукові записки Інституту законодавства Верховної Ради України*. 2014. № 5. С. 138–142. URL : http://nbuv.gov.ua/UJRN/Nzizvru_2014_5_29

86. Марунченко О. П. Інформаційна війна в сучасному політичному просторі : дис. … канд. політ. наук : 23.00.02. Одеса, 2012. 208 с. URL : http://dspace.pdpu.edu.ua/bitstream.pdf

87. Марутян Р. Р. Інтелектуально-ресурсне забезпечення державного управління у сфері національної безпеки України : монографія. Київ : ЦП «Компринт», 2020. 410 с.

88. Мельник Д. С. Актуальні загрози національній безпеці України в інформаційній сфері: питання визначення та протидії. *Інформаційна безпека людини, суспільства, держави*. 2021. № 1–3 (31–33). С. 16–27.

89. Міненко Є. Вплив російської пропаганди на суспільно-державну стабільність України: аналіз методів та наслідків. *Наукові праці Міжрегіональної Академії управління персоналом*. Серія : Політичні науки та публічне управління. 2023. № 3 (69). С. 47–51.

90. Міністерство цифрової трансформації України : офіц. вебсайт. URL : https://thedigital.gov.ua/

91. МКСК: завершено реєстрацію Центру стратегічних комунікацій та інформаційної безпеки. *Урядовий портал.* 17 січ. 2025 р. URL : https://www.kmu.gov.ua/news/mksk-zaversheno-reiestratsiiu-tsentru-stratehichnykh-komunikatsii-ta-informatsiinoi-bezpeky

92. Младьонова А. Д. Інформаційна війна і політика безпеки: політико-правовий вимір : дис. ... д-ра філософії : 052. Харків, 2021. 200 с.

93. Мороз В. М. Воєнний стан vs свобода слова: проблеми правового регулювання. *Юридичний науковий електронний журнал.* 2023. № 10. С. 446–450. URL : https://lsej.org.ua/10_2023/107.pdf

94. Мосяко А. С. Еволюція ЗМІ як системного чинника політичного процесу: кваліфікаційна робота. *Київський столичний університет імені Бориса Грінченка.* К., 2025. 94 с. URL : https://elibrary.kubg.edu.ua/id/eprint/55651/1/A_Mosiako_FSHN_2025.pdf

95. Національний тест з медіаграмотності – важлива частина реалізації стратегії інформаційної безпеки України. *Міністерство культури України.* URL : https://mcip.gov.ua/news/naczionalnyj-test-z-mediagramotnosti-vazhlyva-chastyna-realizacziyi-strategiyi-informaczijnoyi-bezpeky-ukrayiny-taras-shevchenko

96. Негодченко В. О. Основні напрями державної інформаційної політики в Україні. *Підприємництво, господарство і право.* 2016. № 4. С. 77–81. URL : https://www.pgp-journal.kiev.ua/archive/2016/04/15.pdf

97. Негодченко В. О. Сучасний підхід до класифікації принципів державної інформаційної політики України. *Науковий вісник Міжнародного гуманітарного університету.* Сер. : Юриспруденція. 2017. № 25. С. 34–38. URL : https://www.vestnik-pravo.mgu.od.ua/archive/juspradenc25/11.pdf

98. «Неонацисти, антиросія, каратели»: путін близько півгодини свого виступу в парламенті присвятив Україні та Заходу. URL : https://www.slovoidilo.ua/2023/02/21/novyna/polityka/neonacysty-antyrosiyakarateli-putin-pivhodyny-svoho-vystupu-parlamentiprysvyatyvukrayini-ta-zaxodu

99. Ніщименко О. А. Інформаційна безпека України на сучасному етапі розвитку держави і суспільства. *Наше право.* 2016. № 1. С. 17–23. URL : https://www.irbis-nbuv.gov.ua/cgi-bin/irbis_nbuv/cgiirbis_64.exe?C21COM=2&I21DBN=UJRN&IMAGE_FILE_D

OWNLOAD=1&Image_file_name=PDF%2FNashp_2016_1_6.pdf&P21DBN=UJRN

100. Новакова О., Черненко О. Розвиток стратегічних комунікацій як засіб боротьби з дезінформацією в українському суспільстві. *Вісник Львівського університету*. Серія : Філософсько-політологічні студії. 2023. Вип. 49. С. 308–314.

101. Новородовський В. Інформаційна безпека України в умовах Російської агресії. *Соціум. Документ. Комунікація.* Сер. Іст. науки. 2020. Вип. 9. С. 150–179.

102. Новосельський І. Ф. Українські соціальні мережі: специфіка та проблеми функціонування. *Політикус.* 2020. № 5. С. 89–94. URL : https://politicus.od.ua/5_2020/16.pdf

103. Остапенко А. І. Теоретико-правові засади оцінки ефективності реалізації нормативно-правових актів у сфері оборони. *Науковий вісник Ужгородського Національного Університету*. Серія : Право. 2024. Вип. 86. Ч. 1. С. 106–114.

104. Остапенко М. А. Соціальна напруженість: зміни в умовах війни. *Науковий часопис УДУ імені Михайла Драгоманова.* Серія 22. Політичні науки та методика викладання соціально-політичних дисциплін. 2023. № 33. С. 13–24.

105. Панченко В. М. Інформаційні операції в системі стратегічних комунікацій. *Стратегічні пріоритети.* Серія «Політика». 2016. № 4 (41). С. 72–79. URL : https://ippi.org.ua/sites/default/files/panchenko.pdf

106. Панченко В. М. Інформаційні операції в системі стратегічних комунікацій: досвід НАТО та українські перспективи. *Studia Politologica Ucraino-Polona.* 2016. Вип. 6. С. 180–185. URL : https://nbuv.gov.ua/j-pdf/sppol_2016_4_11.pdf

107. Парламентське дослідження щодо правових механізмів протидії дезінформації в інформаційному просторі України, Європейського Союзу та

окремих держав-членів Європейського Союзу. К., 2024. 14 с. URL : research.rada.gov.ua/uploads/documents/33490.pdf

108. Пашковський В. Ф. Інституційний механізм інформаційної безпеки України в умовах гібридної війни: характер та перспективи трансформацій. *Politicus.* 2021. № 1. С. 69–78. URL : https://politicus.od.ua/1_2021/11.pdf

109. Петрик В. М. Державна інформаційна політика України в умовах гібридної війни. *Вісник НАДУ при Президентові України.* 2016. № 1. С. 116–122. URL : https://journals.indexcopernicus.com/api/file/viewByFileId/401306.pdf

110. Петрик В. М. Забезпечення інформаційної безпеки держави: підручник / за заг. ред. О. А. Семченка та В. М. Петрика. Київ : ДНУ «Книжкова палата України», 2015. 672 с.

111. Петришин Г. Інформаційна війна росії проти України: еволюція основних засобів, методів та динаміка наративів. *Наукові праці Міжрегіональної академії управління персоналом. Політичні науки та публічне управління.* 2025. Вип. 1 (77). С. 117–128. URL : https://journals.maup.com.ua/index.php/political/article/download/4865/5156/5543

112. Петров В. В. Щодо становлення системи стратегічних комунікацій органів державної влади у контексті розвитку відносин з НАТО. *Стратегічні пріоритети.* 2016. № 4 (41). С. 24–31.

113. Питання Міністерства цифрової трансформації : Постанова Кабінету Міністрів України від 18 верес. 2019 р. № 856. URL : https://www.kmu.gov.ua/npas/pitannya-ministerstva-cifrovoyi-t180919

114. Питання Центру протидії дезінформації : Указ Президента України від 07 трав. 2021 р. № 187/2021. URL : https://zakon.rada.gov.ua/go/187/2021

115. Понад 70 % українців вважають російську дезінформацію в соціальних мережах серйозною загрозою. *Київський міжнародний інститут соціології.* 2024. URL : https://detector.media/infospace/article/231906/2024-09-

09-ponad-70-ukraintsiv-vvazhayut-rosiysku-dezinformatsiyu-v-sotsmerezhakh-seryoznoyu-zagrozoyu-kmis/

116. Почепцов Г. Г. Смислові та інформаційні війни. *Інформаційне суспільство.* 2013. Вип. 18. С. 21–27. URL : http://nbuv.gov.ua/UJRN/is_2013_18_6

117. Приходченко Л. М. Щодо складності застосування показників оцінювання ефективності державного управління: теорія і практика. *Державне будівництво.* 2009. № 1. URL : http://www.kbuapa.kharkov.ua/e-book/db/2009-1/doc/1/07.pdf

118. Про внесення змін до деяких законів України щодо захисту інформаційного телерадіопростору України : Закон України від 05 лют. 2015 р. № 159-VIII. URL : http://zakon2.rada.gov.ua/laws/show/159-19.

119. Про внесення змін до деяких законів України щодо захисту інформації та кіберзахисту державних інформаційних ресурсів, об'єктів критичної інформаційної інфраструктури : Закон України від 27 берез. 2025 р. № 4336-IX. URL : https://zakon.rada.gov.ua/go/4336-20

120. Про доступ до публічної інформації : Закон України від 13 січ. 2011 р. № 2939-VI. URL : https://zakon.rada.gov.ua/laws/show/2939-17

121. Про електронні документи та електронний документообіг : Закон України від 22 трав. 2003 р. № 851-IV. URL : http://zakon4.rada.gov.ua/laws/show/851-15.

122. Про забезпечення адміністративного позову: Ухвала Окружного адміністративного суду міста Києва від 25 берез. 2014 р. № 826/3456/14. URL : http://document.ua/pro-zabezpechennja-administrativnogo-pozovu-doc183108.html.

123. Про затвердження нової редакції Статуту державної установи «Центр стратегічних комунікацій та інформаційної безпеки» : Наказ Міністерства культури України від 16 груд. 2025 р. № 1044. URL : https://mcsc.gov.ua/legislation/nakaz-ministerstva-kultury-ukrayiny-vid-16-12-2025-%E2%84%96-1044-pro-zatverdzhennya-novoyi-redakcziyi-statutu-

derzhavnoyi-ustanovy-czentr-strategichnyh-komunikaczij-ta-informaczijnoyi-bezpeky/

124. Про затвердження плану заходів з реалізації Стратегії інформаційної безпеки на період до 2025 року : Розпорядження Кабінету Міністрів України від 30 берез. 2023 р. № 272-р. URL : https://zakon.rada.gov.ua/go/272-2023-%D1%80

125. Про затвердження Порядку взаємодії суб'єктів національної системи реагування на кіберінциденти, кібератаки, кіберзагрози із суб'єктами забезпечення кібербезпеки, правоохоронними, контррозвідувальними, розвідувальними органами та суб'єктами оперативно-розшукової діяльності : Постанова Кабінету Міністрів України від 13 листоп. 2025 р. № 1471. URL : https://zakon.rada.gov.ua/go/1471-2025-%D0%BF

126. Про захист персональних даних : Закон України від 01 черв. 2010 р. № 2297-VI. URL : https://zakon.rada.gov.ua/laws/show/2297-17

127. Про заходи щодо вдосконалення формування та реалізації державної політики у сфері інформаційної безпеки України : Указ Президента України від 01 трав. 2014 р. № 449/2014. URL : http://www.rnbo.gov.ua/documents/347.html.

128. Про інформацію : Закон України від 02 жовт. 1992 р. № 2657-XII. URL : http://zakon2.rada.gov.ua/laws/show/ 2657-12

129. Про медіа : Закон України від 13 груд. 2022 р. № 2849-IX. URL : https://zakon.rada.gov.ua/laws/show/2849-20

130. Про національну безпеку України : Закон України від 21 черв. 2018 р. № 2469-VIII. URL : https://zakon.rada.gov.ua/go/2469-19

131. Про Національну програму інформатизації : Закон України від 04 лют. 1998 р. № 74/98-ВР. URL : https://zakon.rada.gov.ua/laws/show/2807-20#Text

132. Про основні засади забезпечення кібербезпеки України : Закон України від 05 жовт. 2017 р. № 2163-VIII. URL : https://zakon.rada.gov.ua/laws/show/2163-19

133. Про перейменування Міністерства культури та стратегічних комунікацій України : Постанова Кабінету Міністрів України від 29 жовт. 2025 р. № 1396. URL : https://www.kmu.gov.ua/npas/pro-pereimenuvannia-ministerstva-kultury-ta-stratehichnykh-komunikatsii-ukrainy-1396-291025

134. Про порядок організації проведення тренінгів для державних службовців, які займають посади категорії «А» : Постанова Кабінету Міністрів України від 23 серп. 2016 р. № 536. URL : http://zakon3.rada.gov.ua/laws/show/536-2016-%D0%BF.

135. Про публічні електронні реєстри : Закон України від 18 листоп. 2021 р. № 1907-IX. URL : https://zakon.rada.gov.ua/laws/show/1907-20#Text

136. Про рішення Ради національної безпеки і оборони України від 14 вересня 2020 року «Про Стратегію національної безпеки України» : Указ Президента України від 14 верес. 2020 р. № 392/2020. URL : https://zakon.rada.gov.ua/go/392/2020

137. Про рішення Ради національної безпеки і оборони України від 15 жовтня 2021 року «Про Стратегію інформаційної безпеки» : Указ Президента України від 28 груд. 2021 р. № 685/2021 URL : https://zakon.rada.gov.ua/laws/show/685/2021#Text

138. Про рішення Ради національної безпеки і оборони України від 18 березня 2022 року «Щодо реалізації єдиної інформаційної політики в умовах воєнного стану» : Указ Президента України від 19 берез. 2022 р. № 152/2022 URL : https://zakon.rada.gov.ua/go/152/2022.

139. Про рішення Ради національної безпеки і оборони України від 29 грудня 2016 р. «Про Доктрину інформаційної безпеки України» : Указ Президента України від 25 січ. 2017 р. № 47/2017. URL : https://zakon.rada.gov.ua/go/47/2017

140. Про розвідку : Закон України від 17 верес. 2020 р. № 912-IX. URL : https://zakon.rada.gov.ua/go/912-20

141. Про Службу безпеки України : Закон України від 25 берез. 1992 р. № 2229-XII. URL : https://zakon.rada.gov.ua/go/2229-12

142. Про суспільні медіа України : Закон України від 17 квіт. 2014 р. № 1227-VII. URL : https://zakon.rada.gov.ua/go/1227-18

143. Про схвалення Концепції національної системи стратегічного планування : Розпорядження Кабінету Міністрів України від 13 серп. 2025 р. № 853-р. URL : https://zakon.rada.gov.ua/go/853-2025-%D1%80

144. Про утворення Робочої групи з розроблення Концепції реформування системи професійного навчання державних службовців і посадових осіб місцевого самоврядування : Наказ Нацдержслужби України від 15 трав. 2017 р. № 103. URL : http://document.ua/pro-utvorennjarobochoyi-grupi-z-rozroblennja-koncepciyi-ref-doc319487.html

145. Про Центр. *Центр протидії дезінформації при Раді національної безпеки і оборони України.*
URL : https://cpd.gov.ua/documents/%D0%BF%D1%80%D0%BE-%D1%86%D0%B5%D0%BD%D1%82%D1%80/

146. Протидія дезінформації в умовах гібридної війни: український досвід. *Центр стратегічних комунікацій та інформаційної безпеки.* 2023. URL : https://spravdi.gov.ua/

147. Путрашик В. І., Марчук Г. І., Плеханова Т. М. Цифрова журналістика та вплив соціальних мереж на формування громадського уявлення про російсько-українську війну. *Вчені записки Таврійського національного університету імені В. І. Вернадського*. Серія : Філологія. Журналістика. 2024. Т. 35 (74). № 2. С. 189–195. URL : https://philol.vernadskyjournals.in.ua/journals/2024/2_2024/part_2/32.pdf

148. Руднєва А. Формування державної стратегії інформаційної війни України. *Вісник Львівського університету.* Серія : Філософсько-політологічні студії. 2014. Вип. 5. С. 53–61. URL : https://fps-visnyk.lnu.lviv.ua/archive/5_2016/8.pdf

149. Русакевич А. І. Інформаційна безпека в умовах воєнного стану в Україні // *Держава та регіони.* Серія : Право. 2023. № 2. С. 172–175. URL : https://law.stateandregions.zp.ua/archive/2_2023/31.pdf

150. Ряполов А. П. Нормативно-правові основи інформаційної безпеки України в умовах гібридної агресії. *Науковий вісник Ужгородського Національного Університету*. Серія : Право. 2025. Вип. 89. Ч. 3. С. 87–91.

151. Савосько Т. О. Зміст та функції поняття державної інформаційної політики. *Вчені записки ТНУ імені В. І. Вернадського*. Серія : Публічне управління та адміністрування. 2024. Т. 35 (74). № 1. С. 28–31.

152. Саган О. В. Протидія медіа-інформаційному тероризму як питання національної безпеки України : автореф. дис. … канд. політ. наук : 21.01.01. Київ, 2021. 22 с. URL : https://niss.gov.ua/sites/default/files/2021-04/06.04.2021_1-avtorefer_pidpis.-sagan_sig.pdf

153. Сидоренко І. В. Стратегічні комунікації України: проблеми й перспективи розвитку. *Європейські історичні студії.* 2018. № 5. С. 190–199. URL : https://www.irbis-nbuv.gov.ua/cgi-bin/irbis_nbuv/cgiirbis_64.exe?C21COM=2&I21DBN=UJRN&IMAGE_FILE_DOWNLOAD=1&Image_file_name=PDF%2Fevrpol_2018_5_2_38.pdf&P21DBN=UJRN

154. Ситник Г. П., Бондар В. Т., Орел М. Г. Системний підхід дослідження феномену інформація в державному управлінні. *Проблеми сучасних трансформацій.* Серія : право, публічне управління та адміністрування. 2024. № 11. URL : https://reicst.com.ua/pmtl/article/view/2024-11-02-02/2024-11-02-02 https://doi.org/10.54929/2786-5746-2024-11-02-02

155. Ситник Г. П., Клименко Н. Г., Горєліков І. О. Державна політика забезпечення інформаційної безпеки та кібербезпеки, як її складової: проблеми та шляхи їх вирішення. *Державне управління: удосконалення та розвиток.* 2024. № 5.
URL : https://nayka.com.ua/index.php/dy/article/view/3678/3713
https://doi.org/10.32702/2307-2156.2024.5.4

156. Сливка В. Інформаційна війна проти України: міф чи реальність? URL : http://intkonf.org/slivka-vvinformatsiyna-viyna-proti-ukrayini-mif-chi-realnist/.

157. Смотрич Д., Іванов Н. Правові аспекти боротьби з дезінформацією в Європейському Союзі: уроки для України. *Вісник Національного університету «Львівська політехніка».* Серія : «Юридичні науки». 2023. № 4 (40). С. 155–160. URL : science.lpnu.ua/sites/default/files/journal-paper/2023/dec/32531/231576maket4-157-163.pdf

158. Сопілко І. М., Сопілко Д. І. Правове забезпечення інформаційної безпеки та медіаграмотності в умовах гібридних загроз. *Юридичний вісник.* 2024. № 4. С. 18–24.

159. Список інструментів поширення ворожої дезінформації. *Центр протидії дезінформації при Раді національної безпеки і оборони України.* URL : https://cpd.gov.ua/reports/spysok-instrumentiv-poshyrennya-vorozhoyi-dezinformacziyi/

160. Співак К. Інформаційна політика протидії російської пропаганди в Україні. *Вісник Львівського університету.* Серія : Міжнародні відносини. 2019. Вип. 46. С. 189–198.

161. Сприйняття українцями загроз у виборчому процесі та ролі громадянського суспільства: результати опитування для ОПОРИ. *Київський міжнародний інститут соціології.* 2024. URL : https://www.kiis.com.ua/?cat=reports&id=1428&lang=ukr&page=1

162. Стебловський В. В. Суб’єкти побудови безпекового середовища в інформаційній сфері: поняття, види. *Науковий вісник Ужгородського Національного Університету*. Серія : Право. 2025. Вип. 89. Ч. 3. С. 112–117.

163. Стратегічний оборонний бюлетень України : Указ Президента України 29 грудня 2012 р. № 771/2012. URL : https://zakon.rada.gov.ua/laws/show/771/2012#n16

164. Стратегічний оборонний бюлетень України : Указ Президента України від 17 вересня 2021 року № 473/2021. URL : https://www.president.gov.ua/documents/4732021-40121

165. Стратегія інформаційної безпеки. URL : https://zakon.rada.gov.ua/laws/show/685/2021#n14.

166. Стратегія розвитку кібербезпеки України на 2021–2025 роки. *Рада національної безпеки і оборони України.* 2021. URL : https://www.rnbo.gov.ua/

167. Суржинський М. Виклики та можливості адаптації законодавства України до європейських стандартів захисту персональних даних у сфері штучного інтелекту. *Право України.* 2025. № 4. С. 26–37. DOI : 10.33498/louu-2025-04-026.

168. Сухінін Д. В. Роль оцінювання в діяльності органів місцевої влади: основні принципи, методи та завдання. *Публічне адміністрування: теорія та практика : електронний збірник наукових праць*. 2012. Вип. 1 (7). URL : http://www.dbuapa.dp.ua/ zbirnik/2012-01(7)/12sdvpmz.pdf

169. Таньчук О. А. Основні підходи до оцінювання ефективності публічного управління. *Вісник НАДУ*. 2015. № 3. С. 63–70.

170. Таран Є. І. Інформаційна політика як складова стратегії національної безпеки України. *Наукові перспективи.* 2025. № 3(57). С. 546–554.
URL : https://perspectives.pp.ua/index.php/np/article/view/21905/21874https://doi.org/10.52058/2708-7530-2025-3(57)-546-554

171. Таран Є. І. Трансформація державної політики національної безпеки в умовах геополітичних змін. *Центральноукраїнський вісник права та публічного управління*. 2025. № 3. С. 14.
URL : https://cuj.dnuvs.ukr.education/index.php/cuj/article/view/134
https://doi.org/10.32782/cuj-2025-3-14

172. Тарасюк В. М. Стратегічні орієнтири інформаційної політики України в умовах зовнішньої агресії. *Правова держава.* 2022. Вип. 33. С. 70–82.

173. Тарасюк В. М. Стратегічні орієнтири інформаційної політики України в умовах сучасних безпекових викликів. *Право та державне управління.* 2022. № 3. С. 200–205. URL : https://jnas.nbuv.gov.ua/j-pdf/PrDe_2022_33_9.pdf

174. Таркін В. П. Інформаційні війни у сучасному політичному просторі як феномен XX–XXI ст. : дис. ... д-ра філософії : 052. Одеса, 2023. 220 с.

175. Тертичка В. Аналіз державної політики і політологія. *Політичний менеджмент*. 2004. № 6. С. 3–22.

176. Токар О. Державна інформаційна політика: проблеми визначення концепту. *Політичний менеджмент*. 2009. № 5. С. 131–141.

177. Тюря Ю. І. Роль ЄСПЛ у формуванні стандартів функціонування суспільних медіа. *Науковий вісник Ужгородського національного університету*. Серія : Право. 2025. Вип. 87. Ч. 4. С. 305–307. URL : https://visnyk-juris-uzhnu.com/wp-content/uploads/2025/03/49-3.pdf

178. У Києві презентували аналітичний посібник «Гібридна війна Росії проти України. Як перемогти на інформаційному фронті». *Міністерство культури та стратегічних комунікацій України : офіц. вебсайт.* 22.02.2023. URL : https://mcip.gov.ua/news/u-kyievi-prezentuvaly-analitychnyy-posibnyk-hibrydna-viyna-rosii-proty-ukrainy-yak-peremohty-na-informatsiynomu-fronti/

179. У 2022 році кількість зареєстрованих кіберінцидентів виросла майже втричі: звіт. *Державна служба спеціального зв'язку та захисту інформації України : офіц. вебсайт.* URL : https://cip.gov.ua/ua/news/u-2022-roci-kilkist-zareyestrovanikh-kiberincidentiv-virosla-maizhe-vtrichi-zvit

180. Федорчак О. В. Інституційний механізм державного управління. *Ефективність державного управління.* 2017. Вип. 1 (50). Ч. 1. С. 53–63. URL : https://epa.nltu.edu.ua/index.php/journal/article/download/350/345

181. Хімей В. Основні сучасні проблеми інформаційної безпеки України. *Теле- та радіожурналістика.* 2014. Вип. 13. С. 127–132.

182. Центр фіксує продовження хвилі ШІ-фейків від імені українських військових. *Центр протидії дезінформації при Раді національної безпеки і оборони України : офіц. вебсайт.* URL : https://cpd.gov.ua/international-direction/ssha/czentr-fiksuye-prodovzhennya-hvyli-shi-fejkiv-vid-imeni-ukrayinskyh-vijskovyh/

183. Цимбалюк В. С., Бабінська А. В. Правове регулювання інформаційної безпеки в Україні: проблеми теорії та практики. *Адміністративне право і процес.* 2014. № 2 (8). С. 22–30. URL : https://applaw.net/index.php/journal/article/download/418/365/

184. Черговий фейк про «мобілізацію жінок в Україні». *Центр протидії дезінформації при Раді національної безпеки і оборони України.* URL : https://cpd.gov.ua/international-direction/ssha/chergovyj-fejk-pro-mobilizacziyu-zhinok-v-ukrayini/

185. Шемаєв В. М. Державна політика України у сфері забезпечення інформаційної безпеки: теоретичні та практичні аспекти. *Інформаційна безпека людини, суспільства, держави*. 2021. № 1–3 (31–33). С. 97–105. URL : https://www.journals.uran.ua/ispss/article/download/260263/256623.

186. Шемчук В. В. Концептуальні підходи до розуміння інформаційної війни в сучасному світі. *Вчені записки Таврійського національного університету імені В. І. Вернадського.* Серія : Юридичні науки. 2019. Т. 30 (69). № 3. С. 29–35.
URL : https://www.juris.vernadskyjournals.in.ua/journals/2019/3_2019/8.pdf

187. ШІ-фейки проти ТЦК та СП: спроба зірвати мобілізацію. *Центр протидії дезінформації при Раді національної безпеки і оборони України.* URL : https://cpd.gov.ua/international-direction/ssha/shi-fejky-proty-tczk-ta-sp-sproba-zirvaty-mobilizacziyu/

188. Шляхи імплементації європейської політики впровадження цифрових технологій: монографія / за ред. К. В. Єфремової. Харків : НДІ правового забезпечення інноваційного розвитку НАПрН України, 2022. 272 с. URL : https://ndipzir.org.ua/wp-content/uploads/2023/05/monografiya.pdf

189. Шопіна І. М. Діяльність органів виконавчої влади в інформаційній сфері у період воєнного стану: проблеми і перспективи. *Науковий вісник Ужгородського Національного Університету*. Серія : Право. 2025. Вип. 91. Ч. 3. С. 282–287.

190. Штанько В., Дресвянніков А. Аналіз змін законодавства ЄС у сфері цифрових сервісів та платформ й їхній вплив на цифрову економіку України. Київ : ГО «Український центр європейської політики», 2022. 63 с. URL : https://ucep.org.ua/wp-content/uploads/2022/10/new_digit_2_03.10.2022.pdf

191. Штучний інтелект і дезінформація: можливості та ризики в умовах війни. *Центр стратегічних комунікацій та інформаційної безпеки : офіц. вебсайт.* 2023. URL : https://spravdi.gov.ua/shtuchnyj-intelekt-i-dezinformacziya-mozhlyvosti-ta-ryzyky-v-umovah-vijny/

192. Як працює дезінформаційна сітка в Telegram-каналах (частина 1). *Центр протидії дезінформації при Раді національної безпеки і оборони України : офіц. вебсайт.* URL: https://cpd.gov.ua/glossary/principles/czpd_poyasnyuye-yak-praczyuye-dezinformaczij/

193. Як російський інформаційний корабель пішов на… Наративи пропаганди під час повномасштабної війни. *Центр стратегічних комунікацій та інформаційної безпеки : офіц. вебсайт.* 2024. URL : https://spravdi.gov.ua/wp-content/uploads/2024/02/yak-rosijskyj-informaczijnyj-korabel-pishov-na%E2%80%A6-naratyvy-propagandy-pid-chas-povnomasshtabnoyi-vijny.pdf

194. Яфонкін А. А. Інформаційна війна проти держави та інформаційна безпека України. *Форум права.* 2017. № 5. С. 408–413.

195. 10 famous of Russian propaganda in 2023. *Центр стратегічних комунікацій та інформаційної безпеки.* 2023. URL : https://spravdi.gov.ua/en/budanov-in-a-coma-new-jerusalem-and-hamas-obtaining-ukrainian-weapons-10-famous-of-russian-propaganda-in-2023/

196. 2022 Strengthened Code of Practice on Disinformation. Shaping Europe’s digital future. 16 June 2022. URL : https://digital-strategy.ec.europa.eu/en/library/2022-strengthened-code-practice-disinformation

197. Car P. European declaration on digital rights and principles. *EPRS | European Parliamentary Research Service.* Brussels, 2022. 9 p. URL : https://www.europarl.europa.eu/RegData/etudes/BRIE/2022/733518/EPRS_BRI%282022%29733518_EN.pdf

198. Code of Conduct on Disinformation. *Transparency Centre.* 2025. URL : https://disinfocode.eu/assets/pdfs/2025_Code_of_Conduct_on_Disinformation.pdf

199. Code of Practice on Disinformation: new reports available in the Transparency Centre. *Shaping Europe's digital future.* 26 September 2023. URL : https://digital-strategy.ec.europa.eu/en/news/code-practice-disinformation-new-reports-available-transparency-centre

200. Countering disinformation to defend human rights. *Ministry for Foreign Affairs. Finnish Government.* 26 February 2021. URL : https://valtioneuvosto.fi/en/-/countering-disinformation-to-defend-human-rights

201. Culture and Leadership Across the World: The Globe Book of In-Depth Studies of 25 Societies / Edited by J. S. Chokar, F. C. Brodbeck, R. J. House. Mahwah, New Jersey. London : s. n., 2007. 1162 p.

202. Detector Media. Media Literacy Index of Ukrainians: 2020–2023 Fourth Wave. 2024. URL : https://en.detector.media/post/media-literacy-index-of-ukrainians-2020-2023-fourth-wave

203. Digital Services Act. URL : https://www.eu-digitalservices-act.com/

204. DOD Training: U.S. Cyber Command and Services Should Take Actions to Maintain a Trained Cyber Mission Force : GAO-19-362. Washington : U.S. Government Accountability Office, 2019. 40 p. URL : https://www.gao.gov/assets/gao-19-362.pdf

205. European Commission. European Declaration on Digital Rights and Principles. Shaping Europe's digital future. 15 December 2022. URL : https://digital-strategy.ec.europa.eu/en/library/european-declaration-digital-rights-and-principles

206. European Court of Auditors. Special report: Disinformation affecting the EU: tackled but not tamed. 2021. P. 6–8. URL : op.europa.eu/webpub/eca/special-reports/disinformation-9-2021/en/

207. European Declaration on Digital Rights and Principles for the Digital Decade. URL : https://digital-strategy.ec.europa.eu/en/library/european-declaration-digital-rights-and-principles

208. Evans Jacqueline Putin's Information War Against the United States. *Russian Analytical Digest.* 2022. № 282. P. 9–12. URL : https://css.ethz.ch/content/dam/ethz/special-interest/gess/cis/center-for-securities-studies/pdfs/RAD282.pdf

209. FY 2024 Budget Overview. Washington : Department of Defense, 2023. 29 p.
URL : https://comptroller.defense.gov/Portals/45/Documents/defbudget/FY2024/FY24_ITCA_Budget_Overview_Final.pdf

210. Honest Ads Act : bill S. 486, 118th Congress, 1st Session. *Introduced in the Senate on February 16, 2023.*
URL : https://www.govinfo.gov/link/bills/118/s/486?link-type=pdf

211. How to Survive an Era of Disruption, Misinformation, and Division. URL : https://www.weforum.org/agenda/2024/01/how-to-navigate-an-eraof-disruption-disinformation-and-division/

212. Information about Civil Service Learning : The Services it Offers Civil Servants and How to Contact the Team. *GOV.UK.* URL : https://www.gov.uk/government/collections/civil-service-learning.

213. Ivashkevych Yu. Cooperation between the EU and Ukraine to fight disinformation during wartime. URL : https:// https://euneighbourseast.eu/young-european-ambassadors/blog/blog-cooperation-between-theeu-and-ukraine-to-fight-disinformation-during-wartime/

214. Kahler M. Foreign Influence and Democratic Governance: Defining and Countering Malign Influence. New York : Council on Foreign Relations, 2024. 65 p.

URL : https://assets.cfr.org/images/CFR_CSR98_Full_ForeignInfluenceDemGovernance_135613c7520/CFR_CSR98_Full_ForeignInfluenceDemGovernance_135613c7520.pdf

215. Key «Pain Points» Exploited by Russian Propaganda in 2024 to Influence Ukrainians. *Detector Media team*. URL : https://en.detector.media/post/key-pain-points-exploited-by-russian-propaganda-in-2024-to-influence-ukrainians

216. Likarchuk N. Information state in the context of international security and global identity: Challenges and prospects. *International Relations: Theory and Practical Aspects*. 2024. № 14. С. 107–121. URL : https://international-relations.knukim.edu.ua/article/view/319359/310078 https://doi.org/10.31866/2616-745X.14.2024.319359

217. Measures taken by the Federal Government to fight disinformation. *Federal Ministry of the Interior and Community*. URL : https://www.bmi.bund.de/SharedDocs/schwerpunkte/EN/disinformation/measures-taken-by-the-federal-government.html

218. Media Literacy Education System OECD. 20 February 2023. URL : https://www.oecd.org/en/publications/mis-and-disinformation_b00de6dc-en/media-literacy-education-system_d067f517-en.html

219. Media Literacy Index of Ukrainians: 2020–2024 Fifth Wave. *Detector Media team*. URL : https://en.detector.media/post/media-literacy-index-of-ukrainians-2020-2024-fifth-wave

220. NATO ACT. *Cognitive Warfare*. URL : act.nato.int/activities/cognitive-warfare/.

221. On the European Action Plan for Democracy Communication from the commission to the European parliament, the council, the European economic and social committee and the committee of the regions. URL : https://eur-lex.europa.eu/legal-content/EN/TXT/HTML/?uri=CELEX:52020DC0790

222. Online platforms put special focus on elections in the third batch of reports under the Code of Practice on Disinformation. *Shaping Europe's digital*

future. 26 March 2024. URL : https://digital-strategy.ec.europa.eu/en/news/online-platforms-put-special-focus-elections-third-batch-reports-under-code-practice-disinformation

223. Open Hearing on Foreign Influence Operations' Use of Social Media Platforms (Third Party Expert Witnesses): hearing before the Select Committee on Intelligence of the United States Senate, One Hundred Fifteenth Congress, second session, August 1, 2018. Washington : U.S. Government Publishing Office, 2018. 178 p. URL : https://www.intelligence.senate.gov/wp-content/uploads/2024/08/sites-default-files-hearings-chrg-115shrg30959.pdf

224. Questions for the Record for Mr. Jack Dorsey, Chief Executive Officer, Twitter, Senate Select Committee on Intelligence, Hearing on Foreign Influence Operations Using Social Media, September 17, 2018. 35 p. URL : https://www.intelligence.senate.gov/wp-content/uploads/2024/08/sites-default-files-documents-twitter-questions-for-the-record.pdf

225. Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation). *Official Journal of the European Union.* 2016. L 119. P. 1–88.

226. Samantha Lai, Kamya Yadav Operational Reporting in Practice: The EU's Code of Practice on Disinformation URL : https://carnegieendowment.org/2023/11/21/operational-reporting-in-practice-eu-s-code-of-practice-on-disinformation-pub-91060

227. Sandberg Sh. Testimony of Sheryl Sandberg, Chief Operating Officer, Facebook, before the United States Senate Select Committee on Intelligence, September 5, 2018. 10 p. URL : https://www.intelligence.senate.gov/wp-content/uploads/2024/08/sites-default-files-documents-os-ssandberg-090518.pdf

228. Signatories of the 2022 Strengthened Code of Practice on Disinformation. Shaping Europe's digital future. 16 June 2022. URL : https://digital-

strategy.ec.europa.eu/en/library/signatories-2022-strengthened-code-practice-disinformation

229. State Service of Special Communications and Information Protection of Ukraine. *Russian Cyber Operations.* 2024. URL : https://cip.gov.ua/services/cm/api/attachment/download?id=68776

230. Swedish Psychological Defence Agency. Government Offices of Sweden. URL : https://www.government.se/government-agencies/swedish-psychological-defence-agency/

231. Tackling online disinformation: a European Approach. *European Commission.* COM (2018) 236 final. Brussels, 26.04.2018. *Communication from the commission to the European parliament, the council, the European economic and social committee and the committee of the regions.* URL : eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX:52018DC0236

232. The Strengthened Code of Practice on Disinformation. 2022. URL : https://disinfocode.eu/wp-content/uploads/2023/01/The-Strengthened-Codeof-Practice-on-Disinformation-2022.pdf

233. Walker K. Written Testimony of Kent Walker, Senior Vice President and General Counsel, Google, before the Senate Select Committee on Intelligence, November 1, 2017. 5 p. URL : https://www.intelligence.senate.gov/wp-content/uploads/2024/08/sites-default-files-documents-os-kwalker-110117.pdf

ДОДАТКИ

Додаток 1

СПИСОК ОПУБЛІКОВАНИХ ПРАЦЬ ЗА ТЕМОЮ ДИСЕРТАЦІЇ

Статті у наукових фахових виданнях України:

(які входять до переліку МОН України)

1. **Грицай Р. О.** (2023). Інформаційні війни: пошук стратегій протидії. Публічне управління і адміністрування в Україні, 33, 18–23. https://pag-journal.iei.od.ua/archives/2023/33-2023/3.pdf https://doi.org/10.32782/pma2663-5240-2023.33.3

2. **Грицай, Р. О.** (2024). Практики та інструменти протидії інформаційній війні: досвід зарубіжних країн. Публічне управління і адміністрування в Україні, 39, 14–19. https://pag-journal.iei.od.ua/archives/2024/39-2024/4.pdf https://doi.org/10.32782/pma2663-5240-2024.39.2

3. Зубчик О.А., **Грицай Р. О.** (2025). Функціональна конвергентність суб'єктів публічного управління в системі протидії семантичним загрозам. Актуальні проблеми інноваційної економіки та права, 4, 131–142. https://doi.org/10.36887/2524-0455-2025-4-33 https://apie.org.ua/uk/publications-uk/2025-4/

5. Зубчик О. А., **Грицай Р. О.** Державна стратегія захисту когнітивного простору: архітектоніка та управлінські інструменти формування суспільної резильєнтності. Журнал "Актуальні проблеми інноваційної економіки та права". 2026 / #1. 143-147. https://apie.org.ua/uk/derzhavna-strateg%D1%96ia-zahistu-kogn%D1%96tiv/ https://doi.org/10.36887/2524-0455-2026-1-31

5. **Грицай Р.О.** Інформаційна політика у протидії пропаганді. *Журнал «Наукові інновації та передові технології»* № 3(55) 2026. С. 3005-3015. https://doi.org/10.52058/2786-5274-2026-3(55)-3005-3015 https://perspectives.pp.ua/index.php/nauka/article/view/39023/39033

6. **Грицай Р.О.** Сучасні методи пропаганди як фактор загроз національній інформаційній безпеці держави. *«Національні інтереси України»*. №3(20) 2026. С. 1150-1162. https://doi.org/10.52058/3041-1793-2026-3(20)-1150-1162
https://perspectives.pp.ua/index.php/niu/article/view/39319/39333

Тези наукових доповідей:

Грицай Р. О. Концептуальні засади національної інформаційної політики як превентивний механізм протидії пропаганді. *Актуальні питання діяльності Національної поліції як суб'єкту протидії організованій злочинності:* матеріали Всеукр. наук.-практ. конф. (Кропивницький, 2 квіт. 2026 р.). Кропивницький, 2026.

Грицай Р. О. Протидія пропаганді в україні: інформаційна політика та безпекові виклики. *Фінансова політика: теоретичні та практичні аспекти юридичної науки. Тема року: Сучасний міжнародний правопорядок та міжгалузеві правові процеси:* матеріали VIII Міжнар. наук.-практ. конф. (Ірпінь, 2 квіт. 2026 р.). Ірпінь, 2026.

Додаток 2
ДОВІДКИ ПРО ВПРОВАДЖЕННЯ

ДОВІДКА
про впровадження результатів дисертаційного дослідження
Грицая Романа Олексійовича
у науково-дослідну роботу та освітній процес

Цією довідкою підтверджується, що результати дисертаційного дослідження Грицая Романа Олексійовича на тему «Особливості державної стратегії протидії інформаційній війні» впроваджено у наукову діяльність та освітній процес Навчально-наукового інституту публічного управління та державної служби Київського національного університету імені Тараса Шевченка.

Наукові положення та практичні рекомендації дисертації використано у науково-дослідній роботі, а сме, результати дослідження інтегровано у виконання науково-дослідної теми кафедри державного управління «Використання можливостей статусу кандидата на вступ в ЄС для підвищення ефективності публічного управління та адміністрування в Україні» (номер державної реєстрації 0123U102187). Зокрема, авторські розробки щодо структурно-функціональної моделі інституційного механізму протидії інформаційній війні було використано для обґрунтування напрямів адаптації вітчизняного законодавства до стандартів Європейського адміністративного простору в частині забезпечення інформаційної стійкості.

У навчальному процесі матеріали дисертації, які стосуються сучасних пропагандистських технологій, методів предиктивної аналітики та стратегічних комунікацій, впроваджено у викладання навчальних дисциплін для магістрів та аспірантів спеціальності 281 «Публічне управління та адміністрування», зокрема блоками тем «Інформаційна політика та цифрова трансформація», «Стратегічне управління в публічному секторі», «Національна безпека та антикризове управління».

Довідка видана на підставі витягу з протоколу №6 засідання вченої ради Навчально-наукового інституту публічного управління та державної служби Київського національного університету імені Тараса Шевченка від 30 грудня 2025 року про затвердження анотованого звіту по кафедральній науково-дослідній роботі кафедри державного управління, тема науково-дослідної роботи «Використання можливостей статусу кандидата на вступ в ЄС для підвищення ефективності публічного управління та адміністрування в Україні» (номер державної реєстрації 0123U102187) за 2023-2025 роки.

Директор Інституту
_____ **Лариса КОМАХА**

Додаток 3

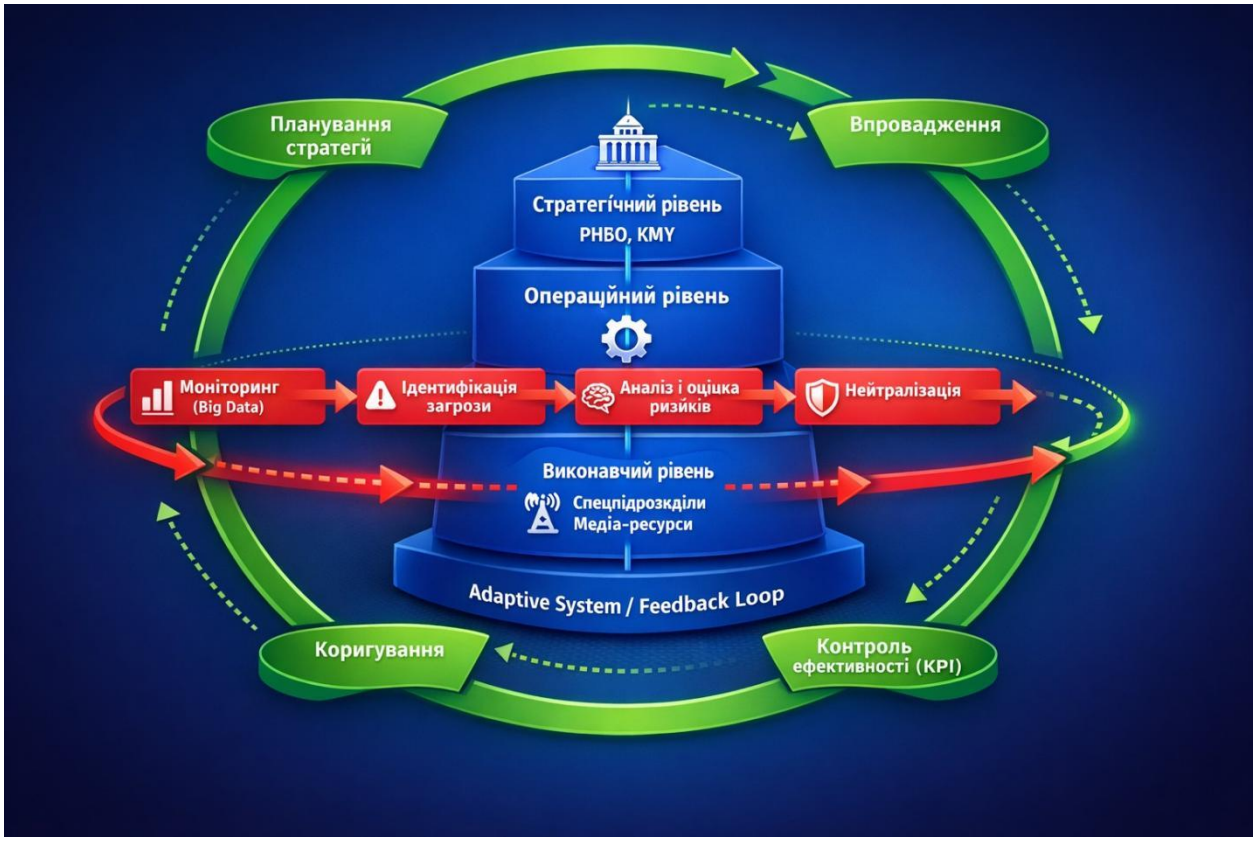

Рис. 1. Схема структурно-функціональної моделі формування та реалізації державної стратегії протидії інформаційній війні (авторська розробка)

Додаток 4

Рис. 2. Схема трирівневої системи суб’єктів (стратегічного, виконавчого та партнерського рівнів) публічного управління оновленої державної інформаційної політики України (авторська розробка)