НАЦІОНАЛЬНИЙ АЕРОКОСМІЧНИЙ УНІВЕРСИТЕТ
«ХАРКІВСЬКИЙ АВІАЦІЙНИЙ ІНСТИТУТ»

Кваліфікаційна наукова праця
на правах рукопису

КОТЛЯРОВ ВАЛЕРІЙ ОЛЕКСАНДРОВИЧ

УДК: 351.816/.817:351.746.1:004

МЕХАНІЗМИ РЕАЛІЗАЦІЇ ІНФОРМАЦІЙНОЇ БЕЗПЕКИ У СИСТЕМІ ПУБЛІЧНОГО УПРАВЛІННЯ

25.00.02 – механізми державного управління

Подається на здобуття наукового ступеня доктора наук з державного управління

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


_____ В.О. Котляров

Харків-2026

АНОТАЦІЯ

Котляров В.О. Механізми реалізації інформаційної безпеки у системі публічного управління. – Кваліфікаційна наукова праця на правах рукопису.

Дисертація на здобуття наукового ступеня доктора наук з державного управління за спеціальністю 25.00.02 – механізми державного управління. Національний аерокосмічний університет «Харківський авіаційний інститут», Харків, 2026.

Обґрунтовано та розроблено інтегративну модель механізмів реалізації інформаційної безпеки у системі публічного управління України, яка, на відміну від існуючих, ґрунтується на міжсекторальному та комунікаційно-стратегічному підходах та включає: удосконалену інституційно-правову конструкцію ключових суб'єктів забезпечення інформаційної стійкості (РНБО, Центр протидії дезінформації; Міністерство культури України); критерії функціональної діагностики управлінських обмежень в умовах воєнного стану; комплексну концепцію стратегічного управління інформаційною безпекою, що забезпечує синергію між захистом критичної інфраструктури та підтримкою інформаційної гігієни громадянського суспільства.

Поглиблено теоретико-методологічні засади дослідження інформаційної безпеки у системі публічного управління шляхом системного аналізу її подвійної природи та авторського структурування її ключових елементів: інформаційна безпека як система суспільних відносин: Здійснено комплексне розмежування та структурування її елементів (суб'єкти: держава, громадянське суспільство, бізнес; об'єкт: інформаційне середовище; регулювання; інститути; цілі), а також ідентифіковано її ключові особливості (суб'єктна взаємозалежність, громадянська участь, інформаційна грамотність, етика та відповідальність), що дозволяє перейти від статичного опису до динамічного управління процесами; інформаційна безпека як об'єкт правової охорони:

Проаналізовано та систематизовано вітчизняні та зарубіжні наукові парадигми (кримінально-правова, цифрова, адміністративно-правова) та запропоновано науково-обґрунтовані рекомендації щодо її ефективної правової охорони, які включають необхідність законодавчого ототожнення термінів «інформаційна безпека держави» та «інформаційна безпека громадянина» як де-факто об'єктів правової охорони.

Розроблено підходи до інституційного механізму забезпечення інформаційної безпеки в системі публічного управління шляхом: розробки та обґрунтування мультифункціональної архітектурної моделі взаємодії ключових суб'єктів – Служби безпеки України (СБУ), Ради національної безпеки та оборони України (РНБО) та Міністерства цифрової трансформації України (Мінцифри) – виведеної за тривимірним кластерним співвідношенням (моніторинг-координація-впровадження), що дозволяє перейти від лінійного переліку функцій до системного розуміння механізму забезпечення національної інформаційної стійкості; концептуалізації соціальної ролі Міністерства культури та стратегічних комунікацій України (Мінкульт) як повноправного суб'єкта забезпечення інформаційної безпеки, який виконує стратегічну місію із забезпечення культурно-інформаційної стійкості та нормативно-правового регулювання інформаційної політики, доповнюючи техніко-правовий та правоохоронний сегменти (СБУ, Нацполіція).

Систематизовано та концептуалізовано методологічні засади дослідження інформаційної безпеки у системі публічного управління, що дозволило: розширити та уточнити зміст таких ключових методологічних підходів (системність, міждисциплінарність, комплексність) шляхом додавання до них прогностично-моделювального та кореляційно-взаємодоповнювального елементів, що є критично важливим для аналізу ІБ в умовах динамічних гібридних загроз; науково обґрунтувати та ввести до наукового обігу принципи дослідження інформаційної безпеки (комплексність, прогнозованість та глобальність) у контексті публічного управління, розкривши їхню суть через

орієнтацію на майбутні виклики (принцип прогнозованості) та потенційну рецепцію міжнародних стандартів і досвіду (принцип глобальності) у національно-правове та інституційне поле України; актуалізувати застосування філософських основ дослідження ІБ, зокрема, через призму ціннісної парадигми інформації як активу та діалектичного співставлення категорій «безпека» та «свобода» як конституційно гарантованого прояву інформаційної політики.

Концептуалізовано сутнісне призначення механізму правового регулювання ІБ через: 1) інтеграцію двох ключових функціональних кластерів: регулювання інформаційної діяльності (включно з обов'язком державних органів дотримуватись ІБ-законодавства) та розвиток інформаційного середовища (орієнтація на інновації та формування "інформаційного суспільства"); 2) теоретичне обґрунтування власного підходу до кореляції між механізмом правового регулювання ІБ та правом людини на інформацію як взаємного забезпечення прав, де реалізація права на інформацію громадян детермінує діяльність інституцій ІБ-парадигми, а інформаційна безпека має на меті конституційну непорушність цього права; 3) систематизації та початкового опису дванáдцяти ключових принципів побудови механізму правового регулювання забезпечення інформаційної безпеки в Україні, які інтегрують правовий, управлінський та технологічний аспекти (законності, захисту прав та свобод людини, національного суверенітету, прозорості, превентивності, технологічної адаптивності, міжвідомчої координації, співпраці та інтеграції, пропорційності, відповідальності, безперервності); 4) концептуалізацію моделі державного управління ІБ в умовах воєнного стану через систематизацію його основних закономірностей (пріоритетність загальнонаціональних інтересів, превенція дезінформації, інституціоналізація та оперативність управління), а також запропоновано шляхи його розвитку шляхом інтеграції механізмів громадського контролю та підвищення прозорості державних заходів для посилення суспільної довіри.

Систематизовано та науково обґрунтовано методичні підходи протидії загрозам інформаційній безпеці України в умовах військової агресії, що виражається у кластеризації методичних підходів протидії загрозам інформаційній безпеці у системі публічного управління, виділивши п'ять взаємодоповнюючих кластерів: нормативно-правові та організаційні механізми (через аналіз ЗУ «Про національну безпеку України» та ЗУ «Про основні засади забезпечення кібербезпеки України»); технічні засоби та методологія кіберзахисту (використання SIEM, IDS/IPS, міжнародна кооперація, наприклад, із NATO CCDCOE та Microsoft DART); інформаційно-психологічна безпека та протидія дезінформації (підвищення медіаграмотності, діяльність Центру протидії дезінформації, використання VoxCheck та StopFake); освітні ініціативи та підвищення цифрової грамотності (аналіз ініціативи «Дія. Цифрова освіта» та застосування ідеологічного контролю в ЗВО, наприклад, через обмеження використання месенджера Telegram); інтеграція міжнародної співпраці (положення Угоди про асоціацію з ЄС, долучення до Cyber Rapid Response Teams, співпраця з Google, Amazon, Microsoft.

Розроблено концептуальну модель переходу до адаптивної архітектури забезпечення ІБ (на основі концепції adaptive security governance), яка передбачає формалізацію архітектури інформаційної безпеки на засадах прозорості та гласності та впровадження трирівневої структури управління: стратегічний рівень (створення аналітичного центру з прогнозування ІБ (орієнтація на передбачення та сценарне планування); оперативний рівень (створення спільних міжвідомчих центрів реагування (забезпечення синхронізованої відповіді); тактичний рівень (розробка локальних сценаріїв дій на рівні відомств та територіальних громад (гнучке реагування).

Розвинуто теоретичні засади стратегічного управління інформаційною безпекою шляхом систематизації та компаративного аналізу міжнародних моделей, що дозволило: уточнити сутність стратегічного управління забезпеченням ІБ як процесу синхронізації юридичних, організаційних та

технічних засобів для захисту державних, економічних і соціальних інтересів, із ключовим акцентом на пошуку оптимального балансу між нормативним закріпленням та фактичним впровадженням безпекової карти; розробити типологію міжнародних моделей стратегічного управління ІБ на основі аналізу досвіду США, ЄС, Великої Британії, Ізраїлю та Китаю; систематизувати мету стратегічного управління ІБ на три взаємопов'язані рівні (захист (базовий): нейтралізація загроз та забезпечення довіри до інформаційного середовища; розвиток (інноваційний): сприяння інноваціям та технологічному розвитку (ІКТ та ШІ) в ІБ; стійкість (соціальний): підвищення обізнаності населення та розвиток культури інформаційної безпеки (кібергігієни); виокремити чотири ключові особливості стратегічного управління ІБ у розвинених державах світу: правове регулювання, інституційна структура, міжнародна співпраця (Будапештська конвенція) та використання інновацій (ШІ та ІКТ).

Узагальнено та систематизовано сучасні виклики та тенденції розвитку механізмів інформаційної безпеки держави, що дозволило: класифікувати та поглибити аналіз сучасних інформаційних ризиків за трьома основними вимірами, акцентуючи на їхній взаємозалежності та кумулятивному ефекті (глобально-політичні ризики: розкрито як систему взаємопов'язаних загроз: гібридні війни (поєднання військових, кібернетичних та інформаційних засобів), дезінформація та інформаційна асиметрія (дисбаланс між швидкістю поширення та здатністю суспільства до критичного осмислення); технологічні ризики: визначено штучний інтелект (ШІ) як інструмент подвійної дії (можливість для захисту vs. інструмент для автоматизованих фішингових схем), аналітику великих даних (Big Data) як джерело монополізації інформації та deepfake-технології як чинник «кризи достовірності»; соціально-комунікаційні ризики: доведено, що соціальні мережі та цифрові платформи є феноменом подвійної природи (канал демократизації та арена гібридних атак), а їхня алгоритмічна архітектура є каталізатором поляризації та поширення сенсаційного контенту, що вимагає регулювання не лише контенту, а й самих

алгоритмічних процесів); обґрунтувати необхідність інтеграції нових підходів до зміцнення кіберстійкості суспільства та сформувати двопланову модель протидії ризикам (поведінковий/освітній вимір: акцентовано на інформаційній гігієні та медіаграмотності як базових елементах зменшення вразливості громадян (приклад Швеції та Фінляндії); інституційно-правовий вимір: систематизовано нові регуляторні механізми (зокрема, Digital Services Act (DSA) та Data Governance Act (DGA) ЄС), які створюють інституційну рамку для боротьби з дезінформацією та забезпечення прозорості алгоритмів, що є прикладом збалансованого регулювання).

Обґрунтовано теоретико-методологічні засади формування механізмів забезпечення інформаційної безпеки шляхом: систематизації та критичного аналізу трьох основних управлінських моделей (централізованої, децентралізованої та публічно-приватного партнерства) у контексті протидії гібридним загрозам, з виокремленням їхніх переваг і обмежень для України (централізована модель (США, Ізраїль): визначено як ефективну для швидкого реагування та уніфікації стандартів, але вказано на ризики бюрократизації та дублювання повноважень в українських умовах (СБУ, РНБО); децентралізована модель (Німеччина, Японія): обґрунтовано її переваги у гнучкості та врахуванні секторної специфіки (Мінцифра, НБУ, ДССЗЗІ), проте виявлено ключовий недолік — ризик розрізненості стандартів та низька узгодженість без належних координаційних механізмів; публічно-приватне партнерство (США – CISA, Велика Британія – CiSP): обґрунтовано його як критично важливий механізм для оперативного обміну інформацією про загрози та інтеграції технологічної експертизи приватного сектору, що є необхідним для протидії сучасним інформаційним та кіберзагрозам).

Розроблено та науково обґрунтовано стратегію-модель національної цифрової стійкості України, яка є інтегральною трирівневою системою (стратегічний, тактичний та операційний рівні) та забезпечує синергію між державним управлінням, приватним сектором і громадянським суспільством у

протидії гібридним загрозам, включає чотири ключові принципи (проактивність, багаторівнева координація, гнучкість, демократичний контроль), що формують методологічний каркас стратегії-моделі, забезпечуючи перехід від реактивного до прогнозно-превентивного управління інформаційною безпекою, та інституційно-інструментальне забезпечення (створення Єдиного національного центру стратегічних комунікацій як ключової координуючої інституції, що інтегрує моніторинг загроз, міжрівневу координацію та стратегічні комунікації).

Ключові слова : інформаційна безпека, національна безпека, державне управління, інформаційні загрози, правове регулювання, кібербезпека, комунікаційна стратегія, глобалізація, механізми захисту, суб'єкти безпеки.

ABSTRACT

Kotliarov Valerii. Mechanisms for the Implementation of Information Security in the System of Public Administration. – Qualified Scientific Work on the Rights of a Manuscript.

Dissertation for the Degree of Doctor of Sciences in Public Administration, specialty 25.00.02 – Mechanisms of Public Administration. National Aerospace University "Kharkiv Aviation Institute", Kharkiv, 2026.

The integrative model of mechanisms for the implementation of information security in the system of public administration in Ukraine is substantiated and developed. This model, in contrast to existing ones, is based on intersectoral and communication-strategic approaches and includes: an improved institutional and legal structure for the key subjects of ensuring information resilience (NSDC, Center for Countering Disinformation; Ministry of Culture and Information Policy); criteria for the functional diagnostics of managerial limitations under martial law; a comprehensive concept of strategic management of information security that ensures synergy between the protection of critical infrastructure and the maintenance of information hygiene in civil society.

The theoretical and methodological foundations for studying information security in the system of public administration are deepened through a systemic analysis of its dual nature and the author's structuring of its key elements:

Information security as a system of social relations: A comprehensive differentiation and structuring of its elements are carried out (subjects: state, civil society, business; object: information environment; regulation; institutions; goals), and its key features are identified (subject interdependence, civil participation, information literacy, ethics, and responsibility), which allows for a shift from static description to dynamic process management.

Information security as an object of legal protection: Domestic and foreign scientific paradigms are analyzed and systematized (criminal law, digital, administrative law), and scientifically grounded recommendations for its effective legal protection are proposed, which include the necessity of legally equating the terms "state information security" and "citizen information security" as de facto objects of legal protection.

Approaches to the institutional mechanism for ensuring information security in the system of public administration are developed through:

the development and substantiation of a multi-functional architectural model of interaction between key subjects – the Security Service of Ukraine (SSU), the National Security and Defense Council of Ukraine (NSDC), and the Ministry of Digital Transformation of Ukraine (Mincifra) – derived from a three-dimensional cluster relationship (monitoring-coordination-implementation), which allows for a shift from a linear list of functions to a systemic understanding of the mechanism for ensuring national information resilience;

the conceptualization of the social role of the Ministry of Culture and Strategic Communications of Ukraine (Minkult) as a fully-fledged subject of information security, which carries out the strategic mission of ensuring cultural and information resilience and the regulatory framework of information policy, complementing the technical-legal and law enforcement segments (SSU, National Police).

The methodological foundations for studying information security in the

system of public administration are systematized and conceptualized, which allowed for: expanding and clarifying the content of key methodological approaches (systemic, interdisciplinary, comprehensive) by adding prognostic-modeling and correlative-complementary elements, which is critically important for analyzing IS under dynamic hybrid threats; scientifically substantiating and introducing into scientific discourse the principles of information security research (complexity, predictability, and globality) in the context of public administration, revealing their essence through focusing on future challenges (the principle of predictability) and the potential reception of international standards and experience (the principle of globality) into the national legal and institutional field of Ukraine; actualizing the application of the philosophical foundations of IS research, particularly through the prism of the value paradigm of information as an asset and the dialectical juxtaposition of the categories "security" and "freedom" as a constitutionally guaranteed manifestation of information policy.

The essential purpose of the mechanism of legal regulation of IS is conceptualized through: integration of two key functional clusters: regulation of information activities (including the obligation of state bodies to comply with IS legislation) and development of the information environment (focus on innovation and the formation of an "information society"); theoretical substantiation of an original approach to the correlation between the mechanism of legal regulation of IS and the human right to information as mutual guarantees of rights, where the realization of citizens' right to information determines the activity of IS paradigm institutions, and information security aims at the constitutional inviolability of this right; systematization and initial description of the twelve key principles for building the mechanism of legal regulation for ensuring information security in Ukraine, which integrate legal, managerial, and technological aspects (legality, protection of human rights and freedoms, national sovereignty, transparency, prevention, technological adaptability, interagency coordination, cooperation and integration, proportionality, accountability, continuity); conceptualization of the model of state

administration of IS under martial law through the systematization of its basic patterns (priority of national interests, prevention of disinformation, institutionalization, and operational management), and proposals for its development through the integration of public control mechanisms and increased transparency of state measures to strengthen public trust.

Methodological approaches to counteracting threats to Ukraine's information security under military aggression are systematized and scientifically substantiated, which is expressed in the clustering of methodological approaches to counteracting information security threats in the public administration system, highlighting five complementary clusters: regulatory and organizational mechanisms (through the analysis of the Law of Ukraine "On National Security of Ukraine" and the Law of Ukraine "On the Basic Principles of Cybersecurity in Ukraine"); technical means and cybersecurity methodology (use of SIEM, IDS/IPS, international cooperation, for example, with NATO CCDCOE and Microsoft DART); information and psychological security and counteracting disinformation (increasing media literacy, the activities of the Center for Countering Disinformation, use of VoxCheck and StopFake); educational initiatives and increasing digital literacy (analysis of the "Diia. Digital Education" initiative and the application of ideological control in higher education institutions, for example, through limiting the use of the Telegram messenger); integration of international cooperation (provisions of the Association Agreement with the EU, joining Cyber Rapid Response Teams, cooperation with Google, Amazon, Microsoft).

A conceptual model for transitioning to an adaptive IS architecture is developed (based on the concept of adaptive security governance), which provides for the formalization of a new systemic logic and the implementation of a three-level management structure: strategic level (creation of an analytical center for IS forecasting (focus on foresight and scenario planning)); operational level (creation of joint interagency response centers (ensuring a synchronized response)); tactical level (development of local action scenarios at the level of agencies and territorial

communities (flexible response)).

The theoretical foundations of strategic information security management are developed by systematizing and comparatively analyzing international models, which allowed for: clarifying the essence of strategic management of IS provision as a process of synchronizing legal, organizational, and technical means to protect state, economic, and social interests, with a key emphasis on finding an optimal balance between regulatory enforcement and the actual implementation of the security map; developing a typology of international models of strategic IS management based on an analysis of the experience of the USA, EU, Great Britain, Israel, and China; systematizing the goals of strategic IS management into three interconnected levels: Protection (basic): neutralization of threats and ensuring trust in the information environment; Development (innovative): promoting innovation and technological development (ICT and AI) in IS; Resilience (social): raising public awareness and developing a culture of information security (cyber hygiene); highlighting four key features of strategic IS management in developed countries: legal regulation, institutional structure, international cooperation (Budapest Convention), and the use of innovation (AI and ICT).

Contemporary challenges and trends in the development of state information security mechanisms are summarized and systematized, which allowed for: classifying and deepening the analysis of current information risks across three main dimensions, emphasizing their interdependence and cumulative effect: Global-political risks: revealed as a system of interconnected threats: hybrid warfare (a combination of military, cybernetic, and informational means), disinformation and information asymmetry (an imbalance between the speed of dissemination and society's ability to critically comprehend); Technological risks: Artificial Intelligence (AI) is defined as a dual-use instrument (potential for defense vs. a tool for automated phishing schemes), Big Data analytics as a source of information monopolization, and deepfake technologies as a factor in the "crisis of authenticity"; Socio-communicational risks: It is proven that social networks and digital platforms are a

dual-nature phenomenon (a channel for democratization and an arena for hybrid attacks), and their algorithmic architecture is a catalyst for polarization and the spread of sensational content, which requires the regulation of not only content but also the algorithmic processes themselves; substantiating the necessity of integrating new approaches to strengthening society's cyber resilience and forming a two-pronged risk counteraction model: behavioral/educational dimension (emphasis on information hygiene and media literacy as basic elements to reduce citizen vulnerability (e.g., Sweden and Finland)); institutional-legal dimension (systematization of new regulatory mechanisms (in particular, the EU's Digital Services Act (DSA) and Data Governance Act (DGA)), which create an institutional framework for fighting disinformation and ensuring algorithm transparency, serving as an example of balanced regulation).

The theoretical and methodological foundations for the formation of information security mechanisms are substantiated through: the systematization and critical analysis of three main managerial models (centralized, decentralized, and public-private partnership) in the context of counteracting hybrid threats, with the isolation of their advantages and limitations for Ukraine: centralized model (USA, Israel): identified as effective for rapid response and standardization, but risks of bureaucratization and duplication of powers in the Ukrainian context (SSU, NSDC) are noted; decentralized model (Germany, Japan): its advantages in flexibility and accounting for sectoral specifics (Mincifra, NBU, SSSCIP) are justified, but a key drawback is identified—the risk of disparate standards and low coordination without proper mechanisms; public-private partnership (USA – CISA, Great Britain – CiSP): justified as a critically important mechanism for the operational exchange of threat information and the integration of private sector technological expertise, which is necessary to counteract modern information and cyber threats.

The strategy-model of national digital resilience of Ukraine is developed and scientifically substantiated. It is an integral three-level system (strategic, tactical, and operational levels) that ensures synergy between public administration, the private

sector, and civil society in counteracting hybrid threats. It includes four key principles (proactivity, multi-level coordination, flexibility, democratic control) that form the methodological framework of the strategy-model, ensuring the transition from reactive to prognostic-preventive information security management, and provides for institutional and instrumental support (creation of a Unified National Center for Strategic Communications as a key coordinating institution that integrates threat monitoring, inter-level coordination, and strategic communications).

Keywords: information security, national security, public administration, information threats, legal regulation, cybersecurity, communication strategy, globalization, protection mechanisms, security subjects.

СПИСОК ПУБЛІКАЦІЙ ЗА ТЕМОЮ ДИСЕРТАЦІЇ

Наукові праці, в яких опубліковані основні наукові результати дисертації

Монографії:

1. Загородня А.С., Котляров В. Управління економічною безпекою: стратегічні цілі та механізми реалізації. Київ: Національний університет біоресурсів і природокористування, 2024. 200 с. *Особистий внесок: розроблено механізми управління економічною безпекою в системі публічного управління.*

Статті у наукових періодичних виданнях, проіндексованих у базах даних Web of Science Core Collection та/або Scopus:

2. Zbarsky, V.K., Reznik, N.P., Ostapchuk, A.D., Alekseieva, K.A., Kotliarov, V.O. (2025). Institutional and Informational Prerequisites of Secure Development of Farms in the Agrarian Economy Model of Ukraine. In: Alareeni, B., Elgedawy, I. (eds) Opportunities and Risks in AI for Business Development. Studies in Systems, Decision and Control, vol 546. Springer, Cham. https://doi.org/10.1007/978-3-031-65207-3_53. *Особистий внесок: розроблено*

концептуальну модель інформаційної безпеки аграрних господарств, адаптованої до умов цифрової трансформації та європейських стандартів.

3. Rogovskii, I., Kotliarov, V., Bondarenko, V., Havrylyuk, V., Gaojiang, C., Zehao, L. (2024). Engineering and Security Management of Smart Technology of Agrotronics of Crop Production. In: Mansour, N., Bujosa Vadell, L.M. (eds) Green Finance and Energy Transition. Contributions to Finance and Accounting. Springer, Cham. https://doi.org/10.1007/978-3-031-75960-4_10 *Особистий внесок: формалізовано ризики кібербезпеки в агротехнологічних системах та розробці алгоритмів управління інформаційними загрозами в агровиробництві.полягає у формалізації ризиків інформаційної безпеки в агротрониках.*

4. Cherep A., Voronkova V., Cherep O., Ohrenych Y., Dashko I., Kotliarov V. (2024). Impact of Artificial Intelligence on the Level of Socio-Economic Security of Ukraine in the Conditions of Current European Integration Challenges. In: Alareeni, B., Hamdan, A. (eds) Navigating the Technological Tide: The Evolution and Challenges of Business Model Innovation. ICBT 2024. Lecture Notes in Networks and Systems, vol 1082. Springer, Cham. https://doi.org/10.1007/978-3-031-67434-1_30. *Особистий внесок: визначено критичні точки впливу штучного інтелекту на соціально-економічну стабільність України та розробці рекомендацій щодо інформаційного захисту.*

5. Kotliarov V.O., Kovalchuk O.V., Kovalchuk O.V., Kovalchuk T.V., Kovalchuk O.V. Study of Structural Imbalances in Agricultural Engineering. E3S Web of Conferences. 2022. Vol. 363. Article 01037. URL: https://doi.org/10.1051/e3sconf/202236301037. *Особистий внесок: виявлено інформаційні дисбаланси у системах агроінжинірингу та обґрунтуванні напрямів їх оптимізації з точки зору стратегічної безпеки.*

Статті у наукових виданнях, включених до Переліку наукових фахових видань України:

6. Котляров В.О. Еволюція міжнародно-політичної взаємодії у сфері

інформаційних відносин. Публічне управління і адміністрування в Україні. 2023. Вип. 37. С. 76–81. DOI: 10.32782/pma2663-5240-2023.37.14

7. Котляров В.О. Комплексний підхід щодо розуміння інформаційної безпеки. Публічне управління і адміністрування в Україні. 2023. Вип. 38. С. 168–172. DOI https://doi.org/10.32782/pma2663-5240-2023.38.30

8. Котляров В.О. Особливості категорії «Інформаційна безпека» у міжнародному контексті. Наукові праці МАУП. Політичні науки та публічне управління. 2023. № 4(70). С. 21–26. DOI: 10.32689/2523-4625-2023-4(70)-3

9. Котляров В.О. Система забезпечення інформаційної безпеки України. Наукові праці МАУП. Політичні науки та публічне управління. 2024. № 2(74). С. 40–44. DOI: 10.32689/2523-4625-2024-2(74)-6

10. Котляров В.О. Інформаційне забезпечення безпеки вітчизняної та світової спільноти. Наукові праці МАУП. Політичні науки та публічне управління. 2024. № 1(73). С. 45–52. DOI: 10.32689/2523-4625-2024-1(73)-6

11. Котляров В.О. Теоретичні засади сутності та концепції інформаційної безпеки. Наукові перспективи. 2023. № 6(36). С. 131–142. DOI: 10.52058/2708-7530-2023-6(36)-131-142

12. Котляров В.О. Формування державної політики кібергігієни. Наукові перспективи. 2025. № 7(61). С. 162–174. DOI: 10.52058/2708-7530-2025-7(61)-162-174

13. Котляров В.О. Категоріальний апарат інформаційної безпеки. Суспільство та національні інтереси. 2025. № 8(16). С. 615–629. DOI: 10.52058/3041-1572-2025-8(16)-615-629

14. Котляров В.О. Стратегічні цілі інформаційної безпеки: державне планування та механізми моніторингу ефективності. Національні інтереси України. 2025. № 8(13). С. 903–914. DOI: 10.52058/3041-1793-2025-8(13)-903-914%20

15. Котляров В.О. Інформаційна безпека України: цілі, механізми та адаптація до стандартів ЄС і НАТО. Наукові інновації та передові технології.

2025. № 8(48). С. 180–192. DOI: 10.52058/2786-5274-2025-8(48)-180-192

16. Котляров В.О. Інформаційна безпека як система правовідносин: теоретико-правовий вимір. Актуальні питання у сучасній науці. 2025. № 8(38). С. 245–259. DOI: 10.52058/2786-6300-2025-8(38)-245-259

17. Котляров В.О. Механізми раннього виявлення інформаційних атак: роль штучного інтелекту в прогнозуванні. Успіхи і досягнення у науці. 2025. № 8(18). С. 443–455. DOI: 10.52058/3041-1254-2025-8(18)-443-455

18. Котляров В.О. Інформаційна безпека в умовах глобальної взаємозалежності: міжнародно-правовий контекст та стратегічні практики. Успіхи і досягнення у науці. 2025. № 7(17). С. 474–486. DOI: 10.52058/3041-1254-2025-7(17)-474-486

19. Котляров В.О. Механізми управління репутаційними ризиками у державній інформаційній політиці. Суспільство та національні інтереси. 2025. № 9(17). С. 624–637. DOI: 10.52058/3041-1572-2025-9(17)-624-637

20. Котляров В.О. Методологічні засади дослідження інформаційної безпеки в умовах трансформаційних викликів. Наукові інновації та передові технології. 2025. № 9(49). С. 187–199. DOI: 10.52058/2786-5274-2025-9(49)-187-199

21. Котляров, В.О. Кібертероризм як загроза міжнародній безпеці. Наукові праці Міжрегіональної Академії управління персоналом. Політичні науки та публічне управління, 2023, 5(71), 46-54. DOI: 10.32689/2523-4625-2023-5(71)-6

22. Котляров В.О. Правовий механізм забезпечення інформаційної безпеки: структура, принципи та інституційна модель України. Наукові перспективи. 2025. № 8 (62). С. 907-919. DOI: 10.52058/2708-7530-2025-8(62)-907-919.

23. Котляров В.О. Проблеми інформаційної боротьби у контексті забезпечення національних інтересів. Наукові інновації та передові технології. 2023, № 1(15), DOI: 10.52058/2786-5274-2023-1(15)-499-51

Статті в інших періодичних виданнях України

24. Котляров, В.О. Стратегічне управління інформаційною безпекою України. Київський економічний науковий журнал, 2024, 6, 66-69. DOI: 10.32782/2786-765X/2024-6-9

25. Котляров В.О. Стратегічне управління безпекою організацій. Mechanism of an Economic Regulation, 2024, 1 (103), 41-45. DOI: 10.32782/mer.2024.103.06

26. Котляров В.О. Особливості державної системи стратегічного планування національної безпеки в умовах інформатизації суспільства. Український журнал прикладної економіки та техніки. Том 7, № 4, 2022, С. 225–233. DOI: 10.36887/2415-8453-2022-4-33.

27. Котляров В.О. Стратегічна безпека підприємства: підходи, особливості, механізм та проблеми забезпечення. Український журнал прикладної економіки та техніки. 2022. №3. 214-222 pp. DOI: 10.36887/2415-8453-2022-3-29.

28. Котляров В.О. Поняття стратегічного управління національною безпекою. Український журнал прикладної економіки та техніки. 2023. №1. 159-165 pp. DOI: 10.36887/2415-8453-2023-1-23

29. Котляров В.О. Кібертероризм як загроза міжнародній безпеці. Український журнал прикладної економіки та техніки. 2023. №2. 314-321 pp. DOI: 10.36887/2415-8453-2023-2-45

30. Bytov V., Horbach L., Kotliarov V.O. Production as a Main Source of Consumer Goods to Society in the Current Environment. Economic Forum. 2022. Vol. 12, No. 3. P. 138–144. DOI: 10.36910/6775-2308-8559-2022-3-18. *Особистий внесок: розроблено аналітичну модель взаємозв'язку між виробничими процесами та рівнем забезпечення суспільства споживчими товарами, з урахуванням інформаційно-економічних чинників сучасного середовища.*

31. Котляров В.О. Механізм стратегічного управління економічною безпекою підприємства. Наука та освіта як основа модернізації світоустрою,

2023, № 25-01, с. 183–194. DOI: 10.30890/2709-2313.2023-25-00-024

32. Котляров, В.О. Принципи управління безпекою організацій. Mechanism of an Economic Regulation, 2023, 4 (102), 25-28. DOI: 10.32782/mer.2023.102.04

Тези конференцій:

33. Kotliarov V.O. Strategic Security of the Enterprise. 3rd International Conference on Corporation Management (ICCM-2023). 29.06.2023. Estonia. URL: https://conf.scnchub.com/index.php/ICCM/ICCM-2023/paper/view/547

34. Reznik N.P., Kotliarov V.O. Information Security: Challenges to the Global Information Society. ICEAF-2023. 15.12.2023. Estonia. URL: https://conf.scnchub.com/index.php/ICEAF/ICEAF-2023/paper/view/696. *Особистий внесок: класифіковано глобальні виклики інформаційній безпеці та формуванні аналітичної моделі оцінки їх впливу на міжнародні інститути.*

35. Reznik N.P., Kotliarov V.O. Особливості системи забезпечення стратегічної безпеки компанії. II International Scientific and Practical Conference «Modern Approaches to Problem Solving in Science and Technology». 15–17.11.2023. Варшава, Польща. URL: https://isu-conference.com/en/archive/modern-approaches-to-problem-solving-in-science-and-technology; PDF. *Особистий внесок: розроблено структурну модель корпоративної інформаційної безпеки з урахуванням репутаційних ризиків.*

36. Reznik N.P., Kotliarov V.O. Аспекти державної системи стратегічного планування національної безпеки України. III International Scientific and Practical Conference «Collective Thinking: Unifying Scientific Approaches in Multifaceted Research». 29.11–01.12.2023. Амстердам, Нідерланди. URL: https://isu-conference.com/en/archive/collective-thinking-unifying-scientific-approaches-in-multifaceted-research; PDF. *Особистий внесок: змодельовано інформаційний компонент державної системи стратегічного планування та обґрунтуванні його ролі в національній безпеці.*

ЗМІСТ

ВСТУП

Актуальність теми. На сучасному етапі інформаційна безпека держави є фундаментальною складовою публічного управління, яка забезпечує захист її стратегічних інтересів як на внутрішньому національному, так і на міжнародному рівнях. У контексті публічного управління інформаційна безпека виступає як самостійний управлінський конструкт, що охоплює: захищеність, доступність, цілісність та конфіденційність інформаційних ресурсів, якими оперує держава; спрямування та координацію національного інформаційного простору з метою забезпечення його інформаційної гігієни.

Інформаційна безпека в системі публічно-управлінського забезпечення має чітко визначену структуру, модель, а також потребує ефективних механізмів реалізації та системної суб'єктності. Для цілей нашого дослідження є доцільним зосередити увагу на аналізі механізмів правового забезпечення та управлінської практики, застосовуючи порівняльний підхід на прикладі України та країн-партнерів (зокрема, ЄС та США).

Затребуваність тематики дослідження механізмів реалізації інформаційної безпеки у системі публічного управління особливо гостро проявилася в умовах повномасштабного вторгнення рф в Україну (з 24.02.2022 р.). Ця агресія спричинила безпрецедентні виклики для сфери інформаційної безпеки як ключового складника безпеки національної.

У зв'язку з цим, актуальним є огляд управлінської діяльності профільних органів, які відповідають за забезпечення інформаційної гігієни та безпеки держави в умовах воєнного стану: Міністерство культури України; Рада національної безпеки і оборони України (РНБО) та підпорядкований їй Центр протидії дезінформації; Кабінет Міністрів України (як головний суб'єкт управління).

Окремим завданням є дослідження нормативно-правового інструментарію, який використовується цими органами та інституціями для

формування та підтримки безпечного інформаційного простору.

Аналіз наукових праць підтверджує, що проблематика механізмів реалізації інформаційної безпеки та її стратегічних цілей є об'єктом пильної уваги фахівців у галузях публічного управління та адміністрування, права, політології та філософії.

Теоретико-методологічні засади, структура правового механізму, міжнародна практика та аналіз загроз є предметом досліджень таких вітчизняних та іноземних вчених, як: Л. Кочубей, А. Войціховський, О. Олійник, П. Діхтієвський, З. Гбур, Н. Цибульник, В. Торічний, У. Ільницька, В. Панченко, І. Боднар, О. Архипов, В. Шемчук, І. Валюшко, Л. Мазуренко, І. Поліщук, І. Ломака, В. Шишко, В. Горовий, С. Петренко, Н. Назаренко, Є. Рогова, К. Захаренко, Т. Амро, Б. Кормич та інші; Б. Гудмен, Г.Г. Фостер, Т. Фітцджералд, М. Фазілда, Дж. Грамма, С. Кайпак, К. Кіфер, М. Камаріоту, Т. Лідтке, Д. Маркополу, В. Лонг, М. Мерков, Г. Паананен, Н. Ріпсмен, Н. Робертс, А. Сахід, М. Шумейкер, С. Штітцлейн та ін.

Незважаючи на достатньо велику загальну кількість робіт з проблем механізмів реалізації інформаційної безпеки держави, потребують вирішення наукові питання щодо: комплексної розробки та обґрунтування інтегративної моделі механізмів реалізації інформаційної безпеки у системі публічного управління України, яка б поєднувала інституційно-правовий, комунікаційно-стратегічний та міжсекторальний аспекти в умовах гібридних загроз та викликів воєнного часу; формування цілісної концепції стратегічного управління інформаційною безпекою, що включає діагностику управлінських обмежень та розробку науково обґрунтованих напрямів удосконалення функціоналу ключових суб'єктів (РНБО, Центр протидії дезінформації; Кабінет Міністрів України) з урахуванням сучасного міжнародного досвіду.

Потреба у теоретичному, методологічному та практичному вирішенні окреслених завдань підтверджує актуальність дослідження, його наукову новизну та зумовлює мету, завдання, предмет і об’єкт роботи.

Зв'язок роботи з науковими програмами, планами, темами.

Дисертаційне дослідження проведено в межах науково-дослідної роботи, яка виконувалась Національним авіаційним університетом за темою: «Традиції і новації у сучасній український державності та правовому житті» (державний реєстраційний номер 0106U004970). Внесок автора полягає у теоретичному обґрунтуванні теоретико-методологічних засад забезпечення інформаційної безпеки в умовах глобалізації, означенні та науковому аналізі структури механізму правового забезпечення інформаційної безпеки безпосередньо в Україні, дослідженні міжнародних норм та практик забезпечення інформаційної безпеки, аналізі сучасних загроз інформаційній безпеці України. Окремим кластерним пунктом внеску автора дослідження доцільно визначити розробку Стратегії-моделі національної інформаційної стійкості України.

Мета і задачі дослідження. Мета дослідження полягає у теоретичному обґрунтуванні та науково-практичному аналізі механізмів реалізації інформаційної безпеки у системі публічного управління, визначенні їх стратегічних цілей і функціонального призначення, а також у з'ясуванні особливостей формування та функціонування інформаційно-безпекового середовища України в особливий період.

Реалізація визначеної мети зумовила постановку й вирішення наступних завдань :

–обґрунтувати та розробити інтегративну модель механізмів реалізації інформаційної безпеки у системі публічного управління України;

–уточнити теоретико-методологічні засади дослідження інформаційної безпеки у системі публічного управління;

–обґрунтувати підходи до інституційного механізму забезпечення інформаційної безпеки в системі публічного управління;

–систематизувати та концептуалізувати методологічні засади дослідження інформаційної безпеки у системі публічного управління;

–розкрити сутнісні характеристики механізму правового регулювання

інформаційної безпеки;

–систематизувати та науково обґрунтувати методичні підходи протидії загрозам інформаційній безпеці України в умовах військової агресії;

–розробити концептуальну модель переходу до адаптивної архітектури забезпечення інформаційної безпеки;

–розвинути теоретичні засади стратегічного управління інформаційною безпекою;

–узагальнити та систематизувати сучасні виклики та тенденції розвитку механізмів інформаційної безпеки держави;

–обґрунтувати теоретико-методологічні засади формування механізмів забезпечення інформаційної безпеки;

–розробити та науково обґрунтувати стратегію-модель національної цифрової стійкості України.

Об'єкт дослідження – інформаційна безпека держави як система суспільних відносин у сфері публічного управління.

Предмет дослідження – механізми реалізації інформаційної безпеки у системі публічного управління.

Методи дослідження.

Методологічну основу проведеного дослідження становить сукупність взаємопов'язаних загальнонаукових і спеціалізованих підходів, серед яких застосовано системний, історико-ретроспективний, компаративний, структурно-функціональний методи, а також методи аналізу й синтезу, узагальнення та класифікації, індуктивного й дедуктивного мислення, принципи взаємозв'язку частини та цілого, проблемного і прогностичного аналізу. Застосування історико-ретроспективного методу дало змогу здійснити концептуалізацію термінологічного та категоріального апарату поняття «інформаційна безпека» в межах системи національної безпеки [параграф 1.1]. У свою чергу, через узагальнення й систематизацію вітчизняних наукових джерел було проаналізовано інформаційну безпеку як багатовимірну систему

суспільних відносин і водночас – як об’єкт правової охорони [параграф 1.2], а також виокремлено ключові методологічні орієнтири для подальшого дослідження даного феномену [параграф 1.3].

Системний та структурно-функціональний підходи надали можливість розкрити сутність та принципи побудови механізму правового регулювання забезпечення інформаційної безпеки, концептуалізувавши нормативні особливості такого процесу та систему суб’єктів забезпечення інформаційної безпеки [параграф 2.1; параграф 2.2; параграф 2.3]. Використання емпіричних методів, індукції й дедукції забезпечило розкриття сутності, мети та особливостей стратегічного управління забезпеченням інформаційної безпеки [параграф 3.1]. Метод моделювання дозволив сформувати концепцію розвитку інформаційної безпеки держави та розробити відповідну Стратегію-модель національної цифрової стійкості [параграф 5.3]. Завдяки проблемному й прогностичному підходам проаналізовано глобальний характер інформаційної безпеки крізь призму інституційних можливостей та ризиків, а також комунікаційну стратегію як складову національного управління інформаційною безпекою та, на додаток, класифіковано загрози інформаційній безпеці України і систематизовано методичні підходи протидії загрозам інформаційній безпеці України.

Наукова новизна одержаних результатів полягає полягає у комплексному теоретичному обґрунтуванні стратегічних орієнтирів та інституційно-правових механізмів реалізації інформаційної безпеки (ІБ) у системі публічного управління як автономного, системно організованого феномену в контексті сучасних трансформаційних викликів. Найбільш вагомими науковими результатами дисертаційного дослідження є такі:

уперше

–обґрунтовано та розроблено інтегративну модель механізмів реалізації інформаційної безпеки у системі публічного управління України, яка, на відміну від існуючих, ґрунтується на міжсекторальному та комунікаційно-

стратегічному підходах та включає: удосконалену інституційно-правову конструкцію ключових суб'єктів забезпечення інформаційної стійкості (РНБО, Центр протидії дезінформації; Міністерство культури України); критерії функціональної діагностики управлінських обмежень в умовах воєнного стану; комплексну концепцію стратегічного управління інформаційною безпекою, що забезпечує синергію між захистом критичної інфраструктури та підтримкою інформаційної гігієни громадянського суспільства;

–обґрунтовано теоретико-методологічні засади формування механізмів забезпечення інформаційної безпеки шляхом: систематизації та критичного аналізу трьох основних управлінських моделей (централізованої, децентралізованої та публічно-приватного партнерства) у контексті протидії гібридним загрозам, з виокремленням їхніх переваг і обмежень для України (централізована модель (США, Ізраїль): визначено як ефективну для швидкого реагування та уніфікації стандартів, але вказано на ризики бюрократизації та дублювання повноважень в українських умовах (СБУ, РНБО); децентралізована модель (Німеччина, Японія): обґрунтовано її переваги у гнучкості та врахуванні секторної специфіки (Мінцифра, НБУ, ДССЗЗІ), проте виявлено ключовий недолік — ризик розрізненості стандартів та низька узгодженість без належних координаційних механізмів; публічно-приватне партнерство (США – CISA, Велика Британія – CiSP): обґрунтовано його як критично важливий механізм для оперативного обміну інформацією про загрози та інтеграції технологічної експертизи приватного сектору, що є необхідним для протидії сучасним інформаційним та кіберзагрозам);

–розроблено та науково обґрунтовано стратегію-модель національної цифрової стійкості України, яка є інтегральною трирівневою системою (стратегічний, тактичний та операційний рівні) та забезпечує синергію між державним управлінням, приватним сектором і громадянським суспільством у протидії гібридним загрозам, включає чотири ключові принципи (проактивність, багаторівнева координація, гнучкість, демократичний

контроль), що формують методологічний каркас стратегії-моделі, забезпечуючи перехід від реактивного до прогнозно-превентивного управління інформаційною безпекою, та інституційно-інструментальне забезпечення (створення Єдиного національного центру стратегічних комунікацій як ключової координуючої інституції, що інтегрує моніторинг загроз, міжрівневу координацію та стратегічні комунікації);

удосконалено

– підходи до інституційного механізму забезпечення інформаційної безпеки в системі публічного управління шляхом: розробки та обґрунтування мультифункціональної архітектурної моделі взаємодії ключових суб'єктів — Служби безпеки України (СБУ), Ради національної безпеки та оборони України (РНБО) та Міністерства цифрової трансформації України (Мінцифри) — виведеної за тривимірним кластерним співвідношенням (моніторинг-координація-впровадження), що дозволяє перейти від лінійного переліку функцій до системного розуміння механізму забезпечення національної інформаційної стійкості; концептуалізації соціальної ролі Міністерства культури та стратегічних комунікацій України (Мінкульт) як повноправного суб'єкта забезпечення інформаційної безпеки, який виконує стратегічну місію із забезпечення культурно-інформаційної стійкості та нормативно-правового регулювання інформаційної політики, доповнюючи техніко-правовий та правоохоронний сегменти (СБУ, Нацполіція);

–концептуалізацію сутнісного призначення механізму правового регулювання ІБ через: 1) інтеграцію двох ключових функціональних кластерів: регулювання інформаційної діяльності (включно з обов'язком державних органів дотримуватись ІБ-законодавства) та розвиток інформаційного середовища (орієнтація на інновації та формування "інформаційного суспільства"); 2) теоретичне обґрунтування власного підходу до кореляції між механізмом правового регулювання ІБ та правом людини на інформацію як взаємного забезпечення прав, де реалізація права на інформацію громадян

детермінує діяльність інституцій ІБ-парадигми, а інформаційна безпека має на меті конституційну непорушність цього права; 3) систематизації та початкового опису дванáдцяти ключових принципів побудови механізму правового регулювання забезпечення інформаційної безпеки в Україні, які інтегрують правовий, управлінський та технологічний аспекти (законності, захисту прав та свобод людини, національного суверенітету, прозорості, превентивності, технологічної адаптивності, міжвідомчої координації, співпраці та інтеграції, пропорційності, відповідальності, безперервності); 4) концептуалізацію моделі державного управління ІБ в умовах воєнного стану через систематизацію його основних закономірностей (пріоритетність загальнонаціональних інтересів, превенція дезінформації, інституціоналізація та оперативність управління), а також запропоновано шляхи його розвитку шляхом інтеграції механізмів громадського контролю та підвищення прозорості державних заходів для посилення суспільної довіри;

–систематизацію та наукове обґрунтування методичних підходів протидії загрозам інформаційній безпеці України в умовах військової агресії, що виражається у кластеризації методичних підходів протидії загрозам інформаційній безпеці у системі публічного управління, виділивши п'ять взаємодоповнюючих кластерів: нормативно-правові та організаційні механізми (через аналіз ЗУ «Про національну безпеку України» та ЗУ «Про основні засади забезпечення кібербезпеки України»); технічні засоби та методологія кіберзахисту (використання SIEM, IDS/IPS, міжнародна кооперація, наприклад, із NATO CCDCOE та Microsoft DART); інформаційно-психологічна безпека та протидія дезінформації (підвищення медіаграмотності, діяльність Центру протидії дезінформації, використання VoxCheck та StopFake); освітні ініціативи та підвищення цифрової грамотності (аналіз ініціативи «Дія. Цифрова освіта» та застосування ідеологічного контролю в ЗВО, наприклад, через обмеження використання месенджера Telegram); інтеграція міжнародної співпраці (положення Угоди про асоціацію з ЄС, долучення до Cyber Rapid Response

Teams, співпраця з Google, Amazon, Microsoft;

– концептуальну модель переходу до адаптивної архітектури забезпечення ІБ (на основі концепції adaptive security governance), яка передбачає формалізацію інформаційної безпеки на засадах прозорості та гласності та впровадження трирівневої структури управління: стратегічний рівень (створення аналітичного центру з прогнозування ІБ (орієнтація на передбачення та сценарне планування); оперативний рівень (створення спільних міжвідомчих центрів реагування (забезпечення синхронізованої відповіді); тактичний рівень (розробка локальних сценаріїв дій на рівні відомств та територіальних громад (гнучке реагування);

дістали подальшого розвитку:

–поглиблено теоретико-методологічні засади дослідження інформаційної безпеки у системі публічного управління шляхом системного аналізу її подвійної природи та авторського структурування її ключових елементів: інформаційна безпека як система суспільних відносин: Здійснено комплексне розмежування та структурування її елементів (суб’єкти: держава, громадянське суспільство, бізнес; об’єкт: інформаційне середовище; регулювання; інститути; цілі), а також ідентифіковано її ключові особливості (суб’єктна взаємозалежність, громадянська участь, інформаційна грамотність, етика та відповідальність), що дозволяє перейти від статичного опису до динамічного управління процесами; інформаційна безпека як об'єкт правової охорони: Проаналізовано та систематизовано вітчизняні та зарубіжні наукові парадигми (кримінально-правова, цифрова, адміністративно-правова) та запропоновано науково-обґрунтовані рекомендації щодо її ефективної правової охорони, які включають необхідність законодавчого ототожнення термінів «інформаційна безпека держави» та «інформаційна безпека громадянина» як де-факто об’єктів правової охорони;

–систематизовано та концептуалізовано методологічні засади дослідження інформаційної безпеки у системі публічного управління, що дозволило:

розширити та уточнити зміст таких ключових методологічних підходів (системність, міждисциплінарність, комплексність) шляхом додавання до них прогностично-моделювального та кореляційно-взаємодоповнювального елементів, що є критично важливим для аналізу ІБ в умовах динамічних гібридних загроз; науково обґрунтувати та ввести до наукового обігу принципи дослідження інформаційної безпеки (комплексність, прогнозованість та глобальність) у контексті публічного управління, розкривши їхню суть через орієнтацію на майбутні виклики (принцип прогнозованості) та потенційну рецепцію міжнародних стандартів і досвіду (принцип глобальності) у національно-правове та інституційне поле України; актуалізувати застосування філософських основ дослідження ІБ, зокрема, через призму ціннісної парадигми інформації як активу та діалектичного співставлення категорій «безпека» та «свобода» як конституційно гарантованого прояву інформаційної політики;

–теоретичні засади стратегічного управління інформаційною безпекою (ІБ) шляхом систематизації та компаративного аналізу міжнародних моделей, що дозволило: уточнити сутність стратегічного управління забезпеченням ІБ як процесу синхронізації юридичних, організаційних та технічних засобів для захисту державних, економічних і соціальних інтересів, із ключовим акцентом на пошуку оптимального балансу між нормативним закріпленням та фактичним впровадженням безпекової карти; розробити типологію міжнародних моделей стратегічного управління ІБ на основі аналізу досвіду США, ЄС, Великої Британії, Ізраїлю та Китаю; систематизувати мету стратегічного управління ІБ на три взаємопов'язані рівні (захист (базовий): нейтралізація загроз та забезпечення довіри до інформаційного середовища; розвиток (інноваційний): сприяння інноваціям та технологічному розвитку (ІКТ та ШІ) в ІБ; стійкість (соціальний): підвищення обізнаності населення та розвиток культури інформаційної безпеки (кібергігієни); виокремити чотири ключові особливості стратегічного управління ІБ у розвинених державах світу: правове

регулювання, інституційна структура, міжнародна співпраця (Будапештська конвенція) та використання інновацій (ШІ та ІКТ);

– узагальнено та систематизовано перелік сучасних викликів та тенденцій розвитку механізмів інформаційної безпеки держави, що дозволило: класифікувати та поглибити аналіз сучасних інформаційних ризиків за трьома основними вимірами, акцентуючи на їхній взаємозалежності та кумулятивному ефекті (глобально-політичні ризики: розкрито як систему взаємопов'язаних загроз: гібридні війни (поєднання військових, кібернетичних та інформаційних засобів), дезінформація та інформаційна асиметрія (дисбаланс між швидкістю поширення та здатністю суспільства до критичного осмислення); технологічні ризики: визначено штучний інтелект (ШІ) як інструмент подвійної дії (можливість для захисту vs. інструмент для автоматизованих фішингових схем), аналітику великих даних (Big Data) як джерело монополізації інформації та deepfake-технології як чинник «кризи достовірності»; соціально-комунікаційні ризики: доведено, що соціальні мережі та цифрові платформи є феноменом подвійної природи (канал демократизації та арена гібридних атак), а їхня алгоритмічна архітектура є каталізатором поляризації та поширення сенсаційного контенту, що вимагає регулювання не лише контенту, а й самих алгоритмічних процесів);

Практичне значення одержаних результатів. Основні ідеї та висновки дослідження доведено до конкретних положень, методик і рекомендацій. Вони можуть бути використані у практичній діяльності органами публічного управління на національному й регіональному рівнях, підприємствами, громадськими організаціями.

Результати дисертації були впроваджені у діяльність Національної акціонерної компанії «Надра України» (довідка про впровадження НАК «Надра України»). Зокрема, розроблені у межах дослідження рекомендації використані для удосконалення механізмів захисту інформаційного простору національної акціонерної компанії, забезпечення кіберстійкості державних підприємств та

протидії інформаційним загрозам в умовах воєнного стану. Результати наукового дослідження були впроваджені у діяльність Національного агентства кваліфікацій в таких напрямах: оцінка ризиків у сфері кваліфікаційної безпеки (інтегровано методику класифікації інформаційних загроз та ризиків в регламенти роботи із даними Реєстру кваліфікацій); модернізація аналітичних систем (алгоритми прогнозування загроз, запропоновані в дисертації, стали основою вдосконалення цифрової інфраструктури аналітичних модулів); оновлення професійних стандартів (наукові положення використано при оновленні кваліфікаційних вимог для фахівців з кібербезпеки, зареєстрованих у Національному реєстрі кваліфікацій); аналітична підтримка державної політики (висновки дисертації включено до експертних матеріалів щодо гармонізації українських кваліфікаційних норм з європейськими рамками) (довідка Національного агентства кваліфікацій від 22.07.2025 р. № 01/01.01-06/1647).

Результати дисертації були впроваджені у діяльність Департаменту кадрової політики Міністерства оборони України (довідка про впровадження Департаменту кадрової політики Міністерства оборони України). Зокрема, розроблені у межах дослідження автора рекомендації використані для удосконалення механізмів захисту інформаційного простору департаменту та протидії інформаційним загрозам в умовах воєнного стану.

Особистий внесок здобувача. Представлена дисертація є результатом самостійного наукового дослідження, в якому автор формулює власне бачення вирішення актуальних проблем публічного управління у сфері стратегічного забезпечення інформаційної безпеки держави в умовах посилення зовнішніх і внутрішніх викликів. Усі положення, що виносяться на захист, а також ключові висновки сформульовані дисертантом особисто. У разі використання наукових напрацювань, створених у співавторстві, до тексту дисертації включено виключно ті ідеї й концептуальні підходи, які є результатом індивідуальної наукової діяльності автора.

У працях, що опубліковані в співавторстві, особистий внесок зазначено у переліку наукових праць автора.

Апробація результатів дослідження. Основні положення дисертаційного дослідження були представлені та пройшли апробацію на міжнародних науково-практичних конференціях, а саме: «3rd International Conference on Corporation Management (ICCM-2023)» (Estonia, 2023), «ICEAF-2023» (Estonia, 2023), «II International Scientific and Practical Conference «Modern Approaches to Problem Solving in Science and Technology» (Варшава, Польща, 2023), «II International Scientific and Practical Conference «Collective Thinking: Unifying Scientific Approaches in Multifaceted Research» (Амстердам, Нідерланди, 2023).

Публікації. Основні положення дисертаційної роботи опубліковано у 36 наукових працях, загальним обсягом 29,3 обл.-вид. арк. (24,7 обл.-вид. арк. належить автору), зокрема у розділі колективної монографії, 4 статтях, опублікованих у періодичних виданнях, включених до категорії «А» Переліку наукових фахових видань України та у закордонних виданнях, проіндексованих у базах даних Web of Science Core Collection та/або Scopus, 18 статтях у наукових фахових виданнях з державного управління, 9 статтях у інших періодичних виданнях України, 4 тезах доповідей на науково-практичних конференціях.

Обсяг та структура роботи. Дисертація складається зі вступу, п’яти розділів, висновків, списку використаних джерел, додатків. Повний обсяг роботи – 398 сторінок. Дисертація містить 1 таблицю та 4 рисунки. Список використаних джерел містить 300 найменувань.

РОЗДІЛ 1
НАУКОВО-ТЕОРЕТИЧНІ ЗАСАДИ МЕХАНІЗМІВ РЕАЛІЗАЦІЇ ІНФОРМАЦІЙНОЇ БЕЗПЕКИ У СИСТЕМІ ПУБЛІЧНОГО УПРАВЛІННЯ

1.1. Понятійно-категоріальний апарат реалізації механізмів інформаційної безпеки у системі публічного управління

Розуміння та осмислення теоретико-методологічних засад забезпечення інформаційної безпеки в умовах загальносвітової глобалізації, на наш погляд, найдоцільніше розпочинати із аналізу категоріально-понятійної складової «інформаційної безпеки» як конструкту у двох незалежних, але взаємопоєднанних та взаємодоповнюваних проєкціях – автономній та системній (де інформаційна безпека розглядається конструктом безпеки національної).

Так, початкової необхідності, на наш погляд, набуває аналіз та систематизація термінологічної складової «інформаційна безпека» та пов'язаних із даним терміном понять у автономному вимірі. Серед вчених, які розглядали дане питання у вітчизняному науковому полі, доцільно звернути увагу на напрацювання В. Шемчука [197, с. 51-59], Л. Мазуренко [121, с. 50-57], В. Торічного [170, с. 183-185], О. Довганя та Т. Ткачук [33, с.73-85], А. Войціховського [18, с. 281-288], А. Нашинець-Наумової [128, 168 с.], Л. Кочубей [110, с. 220-237], У. Ільницької [63, с. 27-32], О. Архипова та Є. Архипової [4, с. 18-30], І. Валюшко [14, с. 30-43] та ін.

В свою чергу, іноземний вимір аплікації наукових розробок та здобутків у сфері розуміння понятійно-категоріальних особливостей терміну «інформаційна безпека» та пов'язаних з ним термінів розкривається через напрацювання Н. М. Ріпсмена та Т. Пола [271, с. 3-19], Н. М. Ахмеда [205,

с.113-126], В. Лонга [262, с. 325-344], Ш. Кайпака [256, с. 855-868], Г. Фаррелла та А. Ньюмена [236, 248 с.] та Н. Зюфле [300, 45 с.].

У вищенаведених дослідженнях як вітчизняного, так і зарубіжного форматів насамперед розглядалися питання позиціювання терміну (поняття) «інформаційна безпека» у його доктринальних пропорціях. Дефініції, запропоновані науковцями та подані до огляду нижче, на наш погляд, потребують деяких допрацювань у питаннях практичного пристосування останніх до реалій застосування в епоху глобалізації, інформатизації та діджиталізації. Відтак, варіативність та варіабельність систематизації інформаційно-безпекового простору за соціальною, публічно-управлінською, геополітичною та внутрішньополітичною ознаками свідчить про багатофункціональний характер даного феномену і, водночас, необхідність проведення належних теоретичних деск[і]рипцій зазначеної проблеми, котрі і будуть надалі здійснені в сегментарному пристосуванні до національно-безпекового кластеру.

У контексті повноцінного розуміння понятійно-категоріального апарату терміну «інформаційна безпека» у контексті безпеки національної, пропонуємо стандартизувати два зазначених поняття за принципом поєднаного аплікаційного дослідження. У якості кейсу для науково-доктринального дефініціювання застосуємо російсько-українську війну, що була розпочата росією та триває із 2014 р. у гібридному форматі та із 2022 р. – у повномасштабному.

Вітчизняне дискурсне поле у даному випадку є затребуваним у контексті дослідження Л. Мазуренко, котра, розглядаючи системні риси глобального характеру вітчизняної інформаційної безпеки пристосовно до неспровокованої російської військової агресії [121, с. 55], звернула увагу на співвідношення понять «інформаційна безпека» та «національна безпека» в умовах глобально нестійких політичних подразників.

Конкретніше, дослідниця схиляється до думки, що термінологічні межі

«інформаційної безпеки держави» якраз-таки обмежуються національно-безпековою парадигмою, котру остання для себе обирає. Вибір такої парадигми насамперед залежить від базових факторів державотворення, а саме – державного устрою, державно-політичного курсу на міжнародній арені, урахування загальноправових цінностей в процесі реалізації внутрішньодержавної політики тощо. З огляду на це, термін «інформаційна безпека» у дослідженні пропонується розглядати як засіб (метод) реалізації курсу національної безпеки держави, що «передбачає зберігання, систематизацію та архівування інформації (даних) за встановленими державними стандартами та звичаям інформаційного обороту» [121, с. 55-56].

Поняття «національна безпека», до прикладу, у праці вищезазначеної вченої Л. Мазуренко [121, с. 56] визначається з позиції узагальненого спрямування та координації владними органами та інституціями державної політики, що концептуалізується за багатьма структурними одиницями управління (політична безпека, військова безпека, економічна безпека, соціальна безпека), включно із безпекою в інформаційному просторі (а саме – інформаційною безпекою). Термін «національна безпека» у зазначеній праці розглядається як «сукупність спрямування та координації владою ключових елементів внутрішньодержавної політики, до яких належить сфера політичної, військової, економічної, соціальної та, зокрема, інформаційної безпеки [121, с. 56-57].

Загалом погоджуючись із науковими підходами та пропозиціями Л. Мазуренко [121], пропонуємо ураховувати модерні підходи до взаємозв’язку між термінами «інформаційна безпека» та «національна безпека», що диктують необхідність не лише їх поєднаного розуміння, але й наявності окремої дефініції, що дескриптувала би їхню змістовно-формальну взаємну залежність. Так, на наш погляд, доцільно увести в обіг дефініцію «співвідношення інформаційної безпеки та національної безпеки», надавши останній наступне визначення : «Співвідношення інформаційної безпеки та

національної безпеки полягає у реалізації за допомогою першої завдань другої, а саме таких кластерів, як інформаційна захищеність держави та населення, безпека нації та населення, захищеність даних та інформації, що складають державну таємницю та ін., котрі власне детермінують виміри державної стабільності на внутрішньодержавному рівні».

Теоретизування особливостей статичного розуміння терміну «інформаційна безпека», одночасно, у вітчизняній дослідницькій системі має ознаки узагальненого осмислення від частини до цілого.

Такий проміжний висновок напрошується, виходячи із матеріалів аналітичної праці В. Торічного, котрий розглянув особливості побудови державної системи інформаційної безпеки України [170, с. 184], підійшовши до конкретизації особливостей останньої з позиції дослідження пов’язаних із інформаційно-безпековим феноменом категорій та термінів. Серед них виділяємо та пропонуємо до огляду поняття «безпека», «державна система» та, знову-таки, «інформаційна безпека» у їхній органічній та взаємопоєднаній сукупності.

Поняття «безпека» у дослідженні В. Торічного аналізується насамперед з позиції стану спокою та захищеності регулярних державних дій та ситуацій [170, с. 184]. Уніфіковане розуміння терміну «безпека» у наведеній праці також де-факто ототожнюється зі станом індиферентності, коли держава може самостійно визначати власні межі розвитку внутрішньо та зовнішньо, а такі складові державної координації, як дані, інформація, політикум та соціальна сфера доповнюють, а не дестабілізують та десинхронізують одна одну.

Розуміння терміну «безпека» у вищенаведеному дослідженні вбачаємо повноцінним та структурно комплексним. Водночас маємо зауважити, що тут термін «безпека» підлягає трактуванню виключно в межах державно-управлінської теорії та публічно-управлінського теоретизування, що повністю або частково обмежує можливість його пристосування до поля його предметної інкорпорації на практиці.

Задля усунення зазначеної техніко-теоретичної колізії, у даному визначенні пропонуємо конкретизувати сегмент застосування поняття «безпека». При цьому, доцільно визначати конструкти «інформаційне розуміння терміну безпека», «державно-управлінське розуміння терміну безпека» та ін., залишаючи «тіло» загальнобезпекової дефініції.

Із урахуванням узагальнених пропозицій це може мати наступний вигляд : «Поняття безпека – комплексний феномен, що включає в себе стан спокою та захищеності регулярних державних дій та ситуацій на рівні публічної служби, інституційного забезпечення, інформаційного простору, соціальної сфери тощо», доповнивши таку конотацію тезами «інформаційне розуміння терміну «безпека» базується на єдності державних та недержавних ресурсів, сервісів та баз даних, що прямо або опосередковано визначають незалежність державного розвитку» та «окрім того, державно-управлінське розуміння терміну «безпека» концентрується на узгодженості роботи інституційного та легіслативного апарату у забезпеченні національної стабільності».

Потрібно зазначити, що у рамках вітчизняної дослідницької схематики наявні комплексно-компаративні погляди на розуміння терміну «інформаційна безпека» та пов’язані із останньою дефініції. Якнайкраще ілюструє таку апропріацію праця А. Войціховського [18, с. 283-284], у котрій останній здійснює поєднаний огляд терміну інформаційна безпека у рамках вітчизняного та зарубіжного теоретико-практичного поля. Серед термінології понятійно-категоріальної площини науковець в даному випадку виділяє такі, як «безпека інформації», «безпека громадянина» та «безпека держави». Розглянемо їх детальніше.

Термін «безпека інформації» вчений відносить до теоретичного складника практичного розуміння обігу, обміну, збереження та забезпечення схоронності даних. Дослідник надає останньому визначення як «здатність державного та нормативно-правового апарату скеровувати аспекти обміну та агрегації даних в безпекове та масштабоване поле за принципом непорушності

прав та свобод людини і громадянина, а також кореляції безпеки інформації із безпекою нації».

Відзначимо позитивні та контраверсійні положення подібного дефініціювання. В першу чергу, нам імпонує встановлення причинно-наслідкового зв'язку між термінами «державне регулювання» та «нормативно-правове регулювання», що встановлюється відносно конструкту «безпека інформації», яким фактично визначається фактор доповнюваності інституційного та законодавчого спрямування даної сфери. По-друге, однак, вважаємо не повною мірою опрацьованим аспект забезпечення прав та свобод людини і громадянина в сегменті безпеки інформації.

Враховуючи зазначену вищеописану проблему, пропонуємо надати додаткове пояснення особливостям реалізації прав та свобод людини і громадянина в контексті термінологізації дефініції «безпека інформації». На наш погляд, не зайвим буде акцентувати увагу на визначенні меж таких прав : «Права та свободи людини і громадянина у системі безпеки інформації відіграють системну роль у становленні демократії, що включає непорушність індивідуальних засобів комунікації, персональних даних та інформації, а також чутливих даних». Ми схиляємось до думки, що наявність подібного дефінціювання у структурі розуміння поняття «безпека інформації» може дозволити конкретизовано розкрити її соціально-гуманне призначення.

Розуміння терміну «безпека громадянина» як похідного від дефініції «безпека інформації» поняття у зазначеному дослідженні має яскраво виражене демократичне та людиноцентристське призначеннєве категоризування [18, с. 285]. Так, визначити його пропонується з позиції стану захищеності прав, свобод, а також життя і здоров'я індивіда від внутрішніх та зовнішніх загроз, до яких, до слова, науковець відносить дестабілізуючі фактори інформаційної типології. Потрібно зауважити, що у вищенаведеному аналітичному дослідженні саме інформаційний аспект захищеності людини і громадянина узвичаєний у розрізі захисту особистих даних, конфіденційності та права на

отримання достовірної інформації, що, своєю чергою, складаються із протидії маніпуляціям, дезінформації та кібератакам – котрі комплексно є запорукою успішного виконання державної функції конструювання як інформаційно-безпекового, так і національно-безпекового середовища.

У цьому сенсі категорія «безпека громадянина» постає не лише як юридична конструкція чи норма, а як своєрідна соціально-етична гарантія, котра визначає міру впевненості людини у стабільності власного інформаційного простору. Йдеться не лише про формальний захист персональних даних або технічне убезпечення від кіберзагроз, а насамперед про створення такого комунікаційного середовища, де громадянин може вільно сприймати, аналізувати й передавати інформацію без страху бути введеним в оману, підданим маніпуляції або об’єктом тиску. Саме у цьому контексті поняття «безпека громадянина» трансформується у більш широкий цивілізаційний концепт, що поєднує в собі аспекти індивідуальної автономії, цифрової гігієни, критичного мислення та здатності до самозахисту у віртуальному просторі.

Загрози, які мають інформаційне походження, науковці розглядають як чинники, здатні не лише вплинути на поведінкові установки людини, але й деструктивно позначитися на функціонуванні демократичних інститутів, підриваючи довіру до влади, правосуддя чи медіа. Саме тому автори, які досліджують цю проблематику, вбачають у забезпеченні інформаційної безпеки громадянина передумову стабільності всієї системи національної безпеки. Йдеться про своєрідний ланцюговий зв’язок: від рівня поінформованості та захищеності індивіда безпосередньо залежить ефективність реалізації державних стратегій, політична стійкість суспільства, а також його здатність протистояти зовнішнім маніпулятивним впливам.

Водночас інформаційна безпека громадянина не зводиться виключно до оборонного компоненту. Вона включає також активний аспект — здатність користуватися своїм правом на достовірну, своєчасну та повну інформацію. Це

означає, що у демократичній державі інформаційна безпека не може бути досягнута лише через обмеження, контроль або цензуру. Навпаки, вона забезпечується шляхом розширення можливостей доступу до правдивих даних, підтримання плюралізму думок, розвитку якісних медіа та освіти у сфері цифрової грамотності. Усе це формує підґрунтя для свідомого громадянства, яке розуміє власну роль у формуванні інформаційного порядку денного й може чинити опір деструктивним інформаційним практикам.

Таким чином, у межах сучасного публічного управління поняття «безпека громадянина» стає інтегральним компонентом державної політики, що спрямована на формування гармонійного, збалансованого і стійкого до зовнішніх загроз інформаційного простору. Саме комплексність цього підходу дозволяє розглядати інформаційну безпеку як складову не лише національної, але й соціальної безпеки, у якій людина виступає не об’єктом, а активним суб’єктом захисту. Держава ж, своєю чергою, має забезпечити не лише технічні й нормативно-правові механізми цього процесу, але й створити умови для розвитку громадянської компетентності, яка стає одним із ключових чинників збереження демократичного ладу у добу глобальних інформаційних викликів [18, с. 285].

Дану наукову конотацію вбачаємо застосовною до сфери понятійно-категоріального розмежування поєднаних із терміном «інформаційна безпека» положень та дефініцій. «Безпека громадянина» як константа, водночас, на наше переконання, потребує певного трансформування пропорційно не лише державно-інформаційній, але й загальнодержавній стратегії.

Враховуючи, що термін «безпека громадянина» може мати дотичний понятійний апарат у вигляді понять «інформаційна безпека», а також «національна безпека», «безпека» та «соціальна безпека», пропонуємо розширити та конкретизувати доктринальні погляди на зазначену проблему. Наприклад, вбачаємо за потрібне надати визначення терміну «безпека громадянина» у контексті національної безпеки як стан захищеності

конституційних, природних та похідних прав та свобод людини і громадянина; у контексті підсегменту «безпека» дефініціювати термін «безпека громадянина» крізь призму стану стабільності в державній парадигмі та соціальні структурі, що детермінує можливість соціального, індивідуального, освітнього розвитку особистості; в свою чергу, у розрізі термінологізації поняття «безпека громадянина» з позиції парадигми «соціальної безпеки» вважаємо за доцільне розглядати останнє як стан захищеності та права на реалізацію умінь, знань та навичок в межах соціального середовища, що забезпечується державним апаратом на рівні створення відповідної законодавчої бази, що спрямована на забезпечення цілей та завдань прогностичного публічно-управлінського розвитку у загальнобезпековому сегменті.

Найбільшого рівня узагальненості у згаданому дослідженні А. Войціховського [18, с. 286-287] набуває розуміння терміну «безпека держави». Серед структури із трьох визначень, включно із двома вищеоглянутими, останнє має статус найбільш комплексно в сегменті понятійного категоризування пристосовно до терміну «інформаційна безпека». Так, «безпека держави» у зазначеному дослідженні визначається як сукупність комплексного її захисту на рівні управління, законодавства, внутрішнього, міжнародного статусу, зв’язків із громадськістю та рівнем комунікаційної синхронізації із населенням та громадянським суспільством. При цьому в дослідженні відмічено, що безпека держави має складниками різноманітні підформи, як-от національна, інформаційна, політична, соціальна, мілітарна та ін.

З наведеного визначення випливає, що «безпека держави» розглядається як багатовимірне явище, що поєднує в собі не лише класичні аспекти обороноздатності, але й соціально-комунікаційні, інформаційно-аналітичні та управлінсько-інституційні елементи. Іншими словами, йдеться не про ізольований феномен, а про цілісну систему, у межах якої кожен із компонентів

перебуває у тісній взаємодії з іншими. Саме завдяки цій інтегрованості формується стійкість державного організму до зовнішніх і внутрішніх викликів, зокрема таких, що мають інформаційне чи когнітивне походження.

У цьому контексті поняття «інформаційна безпека» постає не як окрема сфера, а як об'єднувальна ланка між усіма структурними рівнями державного функціонування. Її роль полягає у забезпеченні стабільності комунікацій, достовірності інформаційних потоків, прозорості управлінських рішень і довіри між державою та суспільством. Без належного рівня інформаційної безпеки будь-які спроби гарантувати політичну, економічну чи військову безпеку залишаються фрагментарними, оскільки інформаційна сфера є тим середовищем, у якому формуються суспільні настрої, політична воля, управлінські рішення й стратегічні пріоритети.

Важливо також, що автор, визначаючи безпеку держави через систему її внутрішніх і зовнішніх взаємозв'язків, фактично наголошує на принципі комунікаційної взаємодії як основоположному чиннику стабільності. Держава у такому розумінні не виступає замкненою структурою, а функціонує як відкритий соціально-політичний організм, який здатний до постійного обміну інформацією з громадянами, міжнародними партнерами та інституціями громадянського суспільства. Тому «комунікаційна синхронізація» стає не лише технічним, а насамперед управлінсько-політичним критерієм ефективності державної безпеки [18, с. 286-287].

У свою чергу, багатокомпонентна структура безпеки держави передбачає її поділ на підсистеми, серед яких національна, інформаційна, політична, соціальна та військова виступають ключовими опорами. Кожна з них має власну предметну сферу, але водночас інтегрована в загальну концепцію державної стабільності. Наприклад, політична безпека неможлива без інформаційної прозорості та громадської довіри; соціальна безпека ґрунтується на справедливості та доступі до об'єктивних знань; а військова — на здатності держави оперативно реагувати на загрози, зокрема у кіберпросторі.

Таким чином, інформаційна безпека стає не просто складовою частиною державної безпеки, а її системоутворюючим елементом. Вона не лише забезпечує захист держави від зовнішнього інформаційного втручання, але й формує основу її внутрішньої стійкості, підтримує цілісність політичної комунікації, забезпечує легітимність державної влади через довіру громадян. Без неї неможливо говорити про реальну ефективність публічного управління, адже саме вона визначає ступінь здатності держави адаптуватися до умов глобальної конкуренції, реагувати на гібридні загрози та формувати власний інформаційний суверенітет.

Отже, розуміння «безпеки держави» у викладі А. Войціховського дозволяє зробити висновок, що сучасна держава має розглядати безпекову політику як міждисциплінарну систему, в якій поєднані норми права, етичні принципи, технологічні стандарти, комунікаційні практики та соціальна відповідальність. Такий підхід сприяє формуванню нової парадигми державного управління — гнучкої, відкритої, адаптивної до інформаційних викликів і водночас зорієнтованої на захист базових демократичних цінностей [18, с. 286-287].

На наше переконання, вищезазначене дослідження терміну «безпека держави» відповідає критеріями його наукового модерного розуміння. Певного уточнення, однак, може потребувати аспект взаємозв’язку між терміном «безпека держави», а також зазначеними термінами «безпека» та «безпека громадянина» щодо питання встановлення сферальної парадигми їхнього застосування в теорії задля посилення подальшого практичного призначення задіяності та застосовності останніх. Таким чином можна створити своєрідну безпекову конструкцію в її сучасному інформаційно-соціальному розумінні.

Відтепер пропонуємо сконцентруватися на означенні та огляді нормативно-правового апарату терміну «інформаційна безпека». Юридичне розуміння зазначеного конструкту в полі національної доктрини є обмеженим, проте монографічна праця А. Нашинець-Наумової [128, с. 113-115] оперує

такими термінами, як «юридичне регулювання інформаційної безпеки», «управління інформацією», «нормативно-правове регулювання інформаційного простору». Для більш повного осмислення понятійно-категоріального апарату нашого дослідження вважаємо вмотивованим розглянути останні предметно.

Так, термін «юридичне регулювання інформаційної безпеки» у вищезазначеному дослідженні [128, с. 113] розглядається крізь призму забезпечення на нормативному рівні такого підґрунтя простору даних та інформації, котрий не матиме потенційних ризиків та функціонуватиме з метою її (інформації) систематизації та впорядкування, а не створення інформаційно дестабілізованого, асинхронного інформаційного простору. Відтак, вчений пропонує розуміти термін «юридичне регулювання інформаційної безпеки» не лише у контексті законодавчої статики, але й у сегменті співвідношення та взаємного доповнення нормативного інструментарію інституційним, та навіть більше – використання інституційного інструментарію на основі меж, способів, засобів та механізмів реалізації інформаційно-безпекового середовища, визначених ідеологічно (теоретично).

Власне, така концептуальна рамка дозволяє поглибити розуміння того, що правове забезпечення інформаційної безпеки не може зводитися лише до сукупності законів чи підзаконних актів. Йдеться про цілісний нормативно-організаційний механізм, який формує і підтримує баланс між свободою інформації та необхідністю її захисту. Це означає, що юридичне регулювання має не просто встановлювати межі дозволеного, а й формувати певну «культуру правової взаємодії» в інформаційному просторі.

Такий підхід передбачає розширене розуміння ролі права в інформаційній сфері: не лише як репресивного чи обмежувального інструменту, але як системи координат, що сприяє гармонізації суспільних, державних і приватних інтересів. З одного боку, це дозволяє гарантувати захист базових конституційних прав — на приватність, свободу слова, доступ до інформації, а з іншого — запобігає використанню інформаційних технологій як інструменту

маніпуляцій, пропаганди чи дестабілізації.

Нормативно-правове регулювання інформаційної безпеки у цьому контексті набуває функцій стратегічного управління, яке формує не лише реактивні, а й проактивні моделі правового реагування. Відповідно, воно включає три взаємопов'язані рівні: нормативний (законодавчий), що визначає базові принципи і стандарти; інституційний, що забезпечує реалізацію цих принципів через компетентні органи; і комунікаційний, який гарантує прозорість, узгодженість і довіру між суб'єктами інформаційних правовідносин.

Юридичне регулювання інформаційної безпеки, отже, є динамічною системою, що постійно адаптується до змін технологічного середовища. Це особливо важливо в умовах цифровізації, коли зростає ризик правових лакун і конфліктів між новими формами інформаційної діяльності та чинним законодавством. Право має реагувати на такі трансформації не шляхом запровадження заборон, а через розробку гнучких механізмів контролю, які дозволяють підтримувати стабільність і водночас стимулювати розвиток інформаційної інфраструктури.

Слід також відзначити, що ідеологічна (теоретична) складова, про яку йдеться у дослідженні А. Нашинець-Наумової [128], є не менш значущою за формально-нормативну. Адже саме вона визначає концептуальні межі, в яких право може ефективно функціонувати, і формує світоглядні засади інформаційної політики держави. У цьому сенсі теоретичне осмислення юридичного регулювання виступає передумовою створення збалансованого правового поля, де узгоджуються цінності безпеки, свободи та розвитку.

Таким чином, розуміння «юридичного регулювання інформаційної безпеки» потребує інтеграції кількох наукових вимірів — правового, політичного, управлінського, комунікаційного та навіть філософського. Саме на перетині цих площин формується сучасна парадигма правового забезпечення інформаційної безпеки держави. Її сутність полягає в тому, щоб не лише

створювати закони, а й вибудовувати ефективну систему їх застосування, постійного оновлення та узгодження з реаліями цифрової епохи. Це дозволяє не тільки протидіяти загрозам, але й формувати стійке, кероване, структурно впорядковане інформаційне середовище — основу для сталого розвитку демократичного суспільства та ефективного публічного управління.

Ми, в свою чергу, схильні вважати, що тотожність терміну «юридичне регулювання інформаційної безпеки» із поєднанням статичного (законодавство) та практичного (інституційний складник) механізмів впровадження інформаційно-безпекового простору є виключно концептуальним підходом, що потребує нарощування подальших розробок у даному просторовому вигляді, але не потребує точкового перепрофілювання. Зв'язок між законодавством та інституційним забезпеченням інформаційної безпеки є прямим, адже «сухі» законодавчі норми не здатні врегулювати проблеми простору даних на приватному та державному рівні, потребуючи впорядкування та систематизації.

Розуміння у вищенаведеному дослідженні А. Нашинець-Наумовою [128, с.113-114] терміну «управління інформацією» має яскраво виражений публічно-управлінський аспект осмислення. Так, під «управлінням інформацією» вчена пропонує розглядати спрямування та координацію даних, що підлягають обігу на території певної держави у приватному та публічному форматах, за допомогою державно встановлених засобів, інструментів та механізмів. До таких інструментів та механізмів у зазначеному аналітичному дослідженні віднесено інституції, відповідальні за формування інформаційної політики, а також органи та установи, що регулюють та визначають питання цифрової трансформації (діджиталізації) держави, національних державних ресурсів тощо.

Власне, такий підхід дозволяє розглядати управління інформацією не лише як технічну чи адміністративну процедуру, але як цілісний процес публічного управління, у якому інформація виступає одночасно і ресурсом, і

об’єктом, і засобом впливу. У цьому контексті держава постає не просто суб’єктом, що контролює інформаційні потоки, а координатором складної системи взаємодії між громадянським суспільством, бізнесом, медіа та технологічними інститутами. Таке розуміння управління інформацією фактично підводить до ідеї інформаційного врядування (information governance), де наголос робиться не на обмеженні доступу до інформації, а на створенні умов для її безпечного, ефективного та прозорого використання.

Публічно-управлінський вимір цього поняття має визначальне значення в умовах формування цифрової держави. Адже інформація стає базовим чинником прийняття управлінських рішень, планування державної політики, здійснення моніторингу соціально-економічних процесів та реагування на кризові ситуації. Управління інформацією у такому значенні – це не лише про контроль над потоками даних, а забезпечення їхньої достовірності, цілісності, захищеності й одночасно відкритості для суспільства. Це вимагає від держави гнучких, системних підходів до формування інформаційної інфраструктури, де нормативна, технологічна й організаційна складові діють у синергії.

З позиції публічного управління «управління інформацією» також охоплює питання відповідальності та підзвітності. Йдеться про створення механізмів, що дозволяють відслідковувати, як саме використовується інформація у процесах прийняття рішень, у яких випадках її обіг може створювати ризики для безпеки, приватності чи суспільного порядку. Це означає, що управління інформацією передбачає не лише забезпечення ефективності комунікацій, але й етичну, правову й політичну легітимність усіх дій, пов’язаних із даними [128, с. 113-114].

Важливо зазначити, що в дослідженні А. Нашинець-Наумової наголошується на ролі спеціалізованих інституцій, які мають не лише технічні, але й стратегічні повноваження у сфері інформаційного управління. Йдеться про ті органи, що формують національні стратегії цифрової трансформації, політику відкритих даних, забезпечують кібербезпеку, захист критичної

інформаційної інфраструктури та гарантують правовий режим функціонування інформаційного простору. Ці інституції, фактично, виступають «нервовою системою» держави, яка через інформаційні потоки отримує, обробляє і транслює сигнали, необхідні для стабільного функціонування суспільства [128, с. 113-114].

У ширшому розумінні управління інформацією — це також інструмент реалізації принципу прозорості влади та демократичної підзвітності. Забезпечення вільного, але контрольованого доступу до інформації сприяє зміцненню довіри громадян до державних інституцій, підвищенню рівня громадської участі та розвитку електронного врядування. У цьому аспекті інформаційне управління має подвійне значення: воно водночас є формою реалізації публічної політики і гарантією прав людини в цифровому середовищі.

Таким чином, поняття «управління інформацією» у трактуванні А. Нашинець-Наумової можна розглядати як ключовий компонент сучасної моделі публічного управління. Воно охоплює як нормативно-організаційні механізми, так і управлінську філософію, спрямовану на баланс між безпекою, відкритістю та ефективністю. У результаті держава не лише реагує на інформаційні виклики, але й сама стає активним творцем інформаційного середовища, у якому формуються нові форми комунікації, підзвітності та суспільної взаємодії. Це, у свою чергу, визначає стратегічну роль управління інформацією як центрального елемента публічного управління в умовах цифрової доби.

Подібний підхід до визначення терміну «управління інформацією» з позиції державного апарату наділений достатнім рівнем наукової вмотивованості, проте не враховує розуміння даного поняття в теоретичному сегменті. За його наявності, на наш погляд, можна простіше встановити причинно-наслідковий зв’язок між «управлінням інформацією» як явищем та «управлінням інформацією» як процесом. Пропонуємо викласти дане визначення так : «Управління інформацією є процесом систематизації, обробки,

трансформації, агрегації даних відповідного значення, а також їх вилучення за умови визнання останніх шкідливими або прогностично небезпечними». У таких спосіб можна врахувати усі відмітні риси інформації як об’єкту правовідносин та інформаційного простору як складової національно-безпекового контексту.

В той же час, термін (поняття) «нормативно-правове регулювання інформаційного простору» у праці А. Нашинець-Наумової [128, с. 115] розглядається в аспекті та контексті ширшому, аніж визначення феномену «управління інформацією». Так, під нормативно-правовим регулюванням інформаційного простору науковиця пропонує контекстувати перелік законодавчих документів, за допомогою яких може бути здійснено впорядкування інформаційного середовища, що існує всередині країни. Виходячи із можливої різниці у такому середовищі через об’єктивні фактори на кшталт політичного режиму, внутрішньо- та зовнішньодержавного курсу та ін., сама процедура нормативно-правового забезпечення інформаційного простору має тенденцію до неоднорідності.

Водночас, авторка наголошує, що таке регулювання має не лише техніко-юридичний, а й концептуально-ідеологічний характер. Воно покликане не просто обмежувати або контролювати, а й забезпечувати збалансовану взаємодію між інформаційною свободою та національними інтересами, між правом громадянина на доступ до інформації та необхідністю захисту державних даних. Саме у цьому виявляється подвійна природа інформаційного права — з одного боку, воно спрямоване на лібералізацію, децентралізацію і відкритість інформаційних процесів, а з іншого — на гарантування стабільності, достовірності та безпечності функціонування інформаційного простору.

Законодавча база у цій сфері виступає лише зовнішньою оболонкою більш глибокої нормативної системи, в основі якої лежить ідея про інформацію як стратегічний ресурс держави. Звідси випливає потреба у створенні

збалансованих регуляторних механізмів, що поєднують традиційні юридичні інструменти (закон, підзаконний акт, адміністративна процедура) із сучасними моделями саморегулювання, кіберетичними стандартами, міждержавними домовленостями та міжнародними правовими зобов'язаннями. У цьому розумінні нормативно-правове регулювання не є статичною правовою конструкцією, а виступає живим організмом, який постійно змінюється під впливом цифрової трансформації, розвитку комунікаційних технологій і глобалізації інформаційних потоків [128, с. 115].

Науковиця цілком слушно звертає увагу на те, що у кожній країні інформаційний простір має свою специфіку — політичну, економічну, культурну, мовну, навіть ментальну. Відтак, нормативно-правові інструменти, якими держава впорядковує цей простір, не можуть бути універсальними. У демократичних правопорядках акцент робиться на саморегулюванні, на створенні правових рамок для добровільної відповідальності учасників інформаційних відносин, на прозорості процедур, доступі до публічної інформації, контролі суспільства за діяльністю влади. Натомість у державах із авторитарною або перехідною моделлю державності інформаційна політика нерідко має централізований і директивний характер, де нормативно-правові акти виступають передусім засобом політичного контролю, а не забезпечення балансу інтересів.

Важливо підкреслити, що сама неоднорідність інформаційного простору — як у національному, так і в глобальному вимірі — зумовлює багатовекторність нормативно-правового регулювання. Залежно від політичного режиму, стратегічного курсу держави, її участі у міжнародних організаціях, ступеня цифрової інтегрованості чи навіть рівня довіри суспільства до влади, правове забезпечення інформаційних процесів набуває різних форм і моделей. Тому, як зауважує А. Нашинець-Наумова, нормативно-правове регулювання інформаційного простору не може бути уніфікованим — воно завжди контекстуальне, прив'язане до конкретного історико-політичного

середовища [128, с. 115].

У підсумку, цей концепт дозволяє розглядати інформаційний простір не лише як сукупність технічних мереж чи баз даних, а як правову, соціальну і комунікативну реальність, що потребує постійної правової підтримки, актуалізації та наукового осмислення. Саме через таку призму нормативно-правове регулювання постає не просто інструментом адміністрування, а фактором національної стійкості, гарантією прав людини у цифровому середовищі та засобом підтримання суверенітету держави у сфері інформації.

Зазначений підхід до розуміння терміну «нормативно-правове регулювання інформаційного простору» має тенденцію до аплікації на інформаційне середовище як явище (феномен), котре (котрий) за своєю структурою та оригінацією є комплексним елементом системи управління, зберігання та обігу даних. Одночасно з цим, такий контекст визначення даного терміну не враховує конкретних особливостей управління інформаційного простору не з точки зору теорії, а з точки зору процедури. Урахувати це можна за допомогою наукової конотації наступного формату : «Нормативно-правове регулювання інформаційного простору в практичній площині, водночас, виражається у відповідності генерованого нормотворцем законодавчого інструментарію вимогам та потребам часу, акцентуації на врегулюванні пов’язаних із модерним інформаційним простором викликів, як-о. кіберзагрози, дезінформація, протидія кібератакам тощо».

Потрібно відмітити, що в сучасних умовах понятійно-категоріальні межі вивчення та розуміння терміну «інформаційна безпека» загалом та пов’язаних із ним науково-дискурсних конструкцій дещо видозмінилося. Причиною цьому є такі фактори, як глобалізація, діджиталізація та інформатизація, а також – внутрішньополітичні та геополітичні трансформації, що прямо та опосередковано впливають на дефініціювання зазначеної політико-управлінської та публічно-управлінської категорії.

Як приклад пропонуємо навести дослідження Л. Кочубей [110, с. 222-

224], в котрому остання аналізує трансформації категоріального та практичного апаратів інформаційно-безпекового простору в умовах російської збройної агресії проти України на Донбасі у гібридному прояві.

Зокрема, вчена розглядає такі терміни, як «гарантування інформаційної безпеки» та «інструменти захисту інформаційного поля». Зосередимо увагу на останніх детальніше.

Поняття «гарантування інформаційної безпеки» в дослідженні Л. Кочубей [110, с. 222] проаналізовано крізь призму послідовності та безперервності. Його запропоновано розуміти як «процес, що сприяє інтеграції та впровадженню юридичних, організаційно-розпорядчих, технічних заходів реалізації гігієни даних, що перебувають у офіційному або неофіційному обігу».

У такий спосіб акцент у сучасному розумінні терміну «гарантування інформаційної безпеки» зміщується від пасивної охоронної функції держави до активного процесу управління ризиками, що передбачає прогнозування загроз, формування превентивних механізмів і створення адаптивних систем реагування. Це означає, що інформаційна безпека більше не розглядається як статика, як певний досягнутий стан, а навпаки — як динамічна система, що вимагає постійного моніторингу, аналітики, коригування стратегій і міжінституційної взаємодії. У цьому контексті вчена фактично пропонує трактувати поняття «гарантування» як безперервний цикл, який охоплює не лише захист від зовнішніх впливів, а й підтримання внутрішньої стабільності та стійкості державного, публічного і громадського інформаційного середовища.

У дослідженні Л. Кочубей особливу увагу приділено саме тому, що в умовах гібридних конфліктів класичні засоби захисту інформації (правові, технічні, організаційні) перестають бути достатніми. З’являється потреба у переосмисленні підходів до інформаційної політики, де ключову роль починає відігравати не лише технологічна чи правова компонента, а й гуманітарна — формування критичного мислення, інформаційної культури, психологічної стійкості громадян. Саме ці аспекти стають базисом гарантування

інформаційної безпеки у широкому сенсі, адже мова йде не лише про захист від технічних загроз, але й про запобігання маніпуляціям, пропаганді, навмисному спотворенню фактів, що здатні дестабілізувати соціум.

Таким чином, процес гарантування інформаційної безпеки у сучасних умовах — це багаторівневий і міждисциплінарний механізм, що поєднує правові норми, управлінські рішення, етичні стандарти, інформаційно-аналітичні технології та освітньо-культурні інструменти. Як підкреслює Л. Кочубей, ефективність цього процесу безпосередньо залежить від ступеня координації між державними інституціями, приватним сектором і громадянським суспільством. Вона наголошує, що в умовах гібридної агресії інформаційна безпека не може бути виключно справою спецслужб або регуляторів — це колективна відповідальність усіх суб'єктів, які беруть участь у формуванні національного інформаційного простору.

Окремий аналітичний акцент у роботі Л. Кочубей [110, с. 222] зроблено на понятті «інструменти захисту інформаційного поля», під якими вчена розуміє комплекс практичних, нормативних та комунікаційних засобів, спрямованих на виявлення, попередження та нейтралізацію інформаційних загроз. До таких інструментів, згідно з її підходом, належать: законодавчо визначені протоколи кіберзахисту; державні стратегії у сфері інформаційної політики; механізми контролю за дезінформацією; інформаційно-аналітичні центри при органах влади; а також комунікаційні платформи, через які держава здійснює оперативне інформування населення у кризових ситуаціях.

Водночас авторка робить принципово важливий висновок: у XXI столітті жодна, навіть найсильніша держава, не здатна гарантувати абсолютну безпеку свого інформаційного простору. Натомість ключовим завданням стає забезпечення його стійкості — здатності системи витримувати зовнішні впливи, адаптуватися до нових форм загроз і відновлювати функціональність після атак чи кризових ситуацій. Саме стійкість (resilience), а не ізоляція, стає критерієм ефективності державної політики у сфері інформаційної безпеки.

Погляди Л. Кочубей у цьому сенсі узгоджуються з сучасними міжнародними доктринальними підходами, зокрема з концепціями НАТО та ЄС, де інформаційна безпека розглядається не лише як питання технічного захисту, але й як складова стратегічної комунікації, кібердипломатії та соціальної згуртованості. Національні системи гарантування інформаційної безпеки, на думку вченої, повинні враховувати ці глобальні тенденції, адаптуючи їх до національних особливостей, законодавчої бази та культурного контексту.

Не менш показовим є й те, що в роботі дослідниці наголошено на проблемі балансу між безпекою та свободою слова. Надмірне посилення контролю може призвести до інформаційного авторитаризму, тоді як слабкість регуляторних механізмів — до хаотизації інформаційного простору. Відтак, головним завданням держави є вироблення таких принципів гарантування інформаційної безпеки, які одночасно зберігають відкритість суспільного діалогу та забезпечують стійкість до деструктивних впливів.

У ширшому контексті зазначене дослідження демонструє, що інформаційна безпека перестає бути вузьким питанням кіберзахисту або управління даними — вона трансформується у загальнодержавну парадигму публічного управління, що охоплює правову, соціальну, культурну, етичну та геополітичну площини. Гарантування її в сучасному розумінні — це фактично нова форма державної відповідальності перед громадянином, яка реалізується через політику відкритості, інформаційну освіту, цифрову грамотність та підтримку критичного мислення населення.

Таким чином, узагальнюючи ідеї Л. Кочубей [110, с. 222], можна констатувати, що сучасне осмислення категорії «інформаційна безпека» невід’ємно пов’язане з концепцією адаптивності держави до нових викликів глобального інформаційного середовища. Саме у цій гнучкості, у спроможності поєднувати правові, управлінські й соціальні інструменти захисту, і полягає змістовна сутність гарантування інформаційної безпеки у XXI столітті.

Загалом вважаємо, що така конотація не позбавлена колізійності, адже гарантування інформаційної безпеки у контексті процесу не може бути повністю послідовним та безперервним через зовнішні обставини, що часто непідвладні державному апарату. Наприклад, військова агресія проти держави або інформаційні атаки на її державну чи інституційну інфраструктуру баз даних, як правило, виступають своєрідним джерелом коригування політики інформаційної безпеки. Враховуючи вищезазначене, більш доцільним та вмотивованим вбачаємо використання у даній дефініції термінологічної конструкції «процес, що на засадах постійної державної регуляції та регуляційної адаптації сприяє інтеграції та впровадженню юридичних, організаційно-розпорядчих, технічних заходів реалізації гігієни даних, що перебувають у офіційному або неофіційному обігу».

Термін «інструменти захисту інформаційного поля» у праці Л. Кочубей [110, с. 223-224] запропонований до розгляду в аспекті заходів державної політики, що можуть бути використані конкретним утворенням з метою переконання населення у концептуальності власної позиції. Причому термін «інструменти захисту інформаційного поля» може означати, відповідно матеріалу зазначеної праці [110, с. 224], як благородний та органічно-державницький, так і як антидемократичний феномен (як-от, до слова, приклади російської пропаганди на тимчасово окупованих територіях в Україні).

У сучасному науковому та практичному дискурсі поняття «інструменти захисту інформаційного поля» виходить далеко за межі суто технічного або адміністративного трактування. Це не лише конкретні технологічні засоби контролю та моніторингу інформаційного середовища, але й комплекс управлінських, комунікаційних і соціальних практик, які дозволяють державі формувати та підтримувати баланс між відкритістю інформаційного простору та його безпекою. Відповідно, державні інституції отримують інструментарій для реалізації стратегічної комунікації, планування кризових сценаріїв,

нейтралізації дезінформації та створення системи превентивного реагування на інформаційні загрози.

При цьому слід зазначити, що ефективність зазначених інструментів значною мірою залежить від інтеграції їх у єдину систему державного управління, де передбачено не лише централізовані рішення, а й міжвідомчу координацію, взаємодію з органами місцевого самоврядування, приватним сектором та громадянським суспільством. У цьому сенсі інструменти захисту інформаційного поля стають своєрідним містком між нормативно-правовим регулюванням та практичною реалізацією політики безпеки, де кожний рівень виконавчої влади та громадського контролю доповнює один одного.

Крім того, сучасна концепція цих інструментів передбачає їхню гнучкість і адаптивність. Умови цифрового середовища та інформаційних загроз змінюються з високою швидкістю, тому жорсткі, статичні моделі застосування заходів захисту стають неефективними. Адаптивний підхід дозволяє державі оперативно коригувати стратегії комунікації, оновлювати нормативно-правові акти та технічні протоколи, розширювати або уточнювати компетенції інституцій відповідно до виникаючих викликів.

Особливо важливим є усвідомлення подвійної природи цих інструментів: з одного боку, вони здатні захищати суспільство, зміцнювати довіру громадян до держави та забезпечувати інформаційну стійкість; з іншого — у недобросовісних руках або при відсутності прозорості вони можуть стати механізмом маніпуляції, обмеження свободи слова, формування дезінформаційних наративів та консолідації контролю, що суперечить демократичним принципам.

У підсумку, підходи Л. Кочубей до розуміння «інструментів захисту інформаційного поля» дозволяють оцінити їх не лише як технічні або законодавчі засоби, а як багатовимірну категорію, де поєднуються управлінські, комунікаційні, правові та соціальні компоненти. Вони формують ядро сучасної політики гарантування інформаційної безпеки, спрямованої на підтримку

стабільності та розвитку інформаційного середовища держави, одночасно враховуючи демократичні стандарти і необхідність захисту громадян від потенційних загроз.

Повинні також зауважити, що розуміння терміну «інструменти захисту інформаційного поля» у розрізі певної конфліктної ситуації не дає змоги розглянути дане явище у широкому значенні. Ми вважаємо, що, окрім наданих прикладів протиправних дій рф на території України з точки зору міжнародного права (в т.ч. – у інформаційній площині), доцільно було б надати визначення терміну, що повною мірою розкривало б межі застосування засобів формування інформаційної політики, як-от : «Інструменти захисту інформаційного поля – засоби, механізми та способи, що використовуються для впровадження державних ідей та підходів позитивного та негативного з позиції міжнародного права конотаційного матеріалу. Такий матеріал спрямовується на сприйняття його населенням та громадянським суспільством.

Сучасні погляди на проблему теоретизування та категоризування понятійно-категоріального апарату терміну «інформаційна безпека» та поєднаних із ним понять і термінів також мають проблемно-пошукову форму вираження. Якнайкраще буде розглянути останні на прикладі праці У. Ільницької [63, с. 27-28], де остання конкретизує особливості таких понять, як «протидія негативним інформаційно-психологічним впливам» та «нівелювання проявів інформаційної експансії».

Так, термін «протидія негативним інформаційно-психологічним впливам» визначається у даній праці як пошук варіантів альтернативного реагування на інформаційні збудники та подразники («вкиди», дезінфомрація, генерація «фейкових» даних та перекручування об’єктивної дійсності) за допомогою синхронізованої діяльності державного апарату як інформаційного, так і безпекового сегменту водночас [63, с. 27].

У сучасному науковому дискурсі, зокрема у контексті теоретичного та методологічного осмислення інформаційної безпеки, важливо розглядати

понятійно-категоріальний апарат не лише як сукупність термінів, але й як основу формування практично застосовуваних стратегій і механізмів реагування на інформаційні загрози. Погляди У. Ільницької [63, с. 27-28] дозволяють акцентувати увагу на ключових аспектах такого підходу, де «протидія негативним інформаційно-психологічним впливам» розкривається не як абстрактна концепція, а як система дій, інтегрована у роботу державного апарату та структур забезпечення національної безпеки. Важливо зазначити, що під негативними інформаційно-психологічними впливами розуміються як прямі дії зовнішніх і внутрішніх агентів (наприклад, дезінформаційні кампанії, маніпуляції, технологічне «засмічення» інформаційного середовища), так і комплекс непрямих чинників, що створюють асиметричний тиск на свідомість громадян, їхню здатність до об’єктивного аналізу подій та прийняття рішень.

Таким чином, термін «протидія негативним інформаційно-психологічним впливам» включає в себе комплексну систему стратегічних, тактичних і оперативних заходів, спрямованих на нейтралізацію шкідливих інформаційних потоків та відновлення когнітивної стабільності цільових груп населення. Це передбачає не лише технологічні або кібернетичні інструменти моніторингу та блокування шкідливої інформації, а й активну координацію між різними державними відомствами: органами управління інформаційною політикою, правоохоронними структурами, силовими підрозділами та регуляторами комунікаційного середовища. Особливо важливо, що така протидія повинна здійснюватися системно, синхронізовано, із врахуванням потенційного ефекту «вторинного поширення» шкідливої інформації через соціальні мережі та медіаплатформи, а також із урахуванням психологічних і соціокультурних особливостей різних груп населення.

Природа цього поняття передбачає багаторівневу організацію процесів реагування: стратегічний рівень зосереджується на виробленні політик, нормативно-правових і методичних засад протидії, тактичний — на координації міжвідомчих та міжсекторальних дій, оперативний — на безпосередньому

блокуванні або нейтралізації негативного впливу у цифровому та інформаційному просторі. Завдяки такому підходу, держава отримує можливість не лише швидко реагувати на конкретні загрози, а й формувати превентивну політику, що знижує ймовірність масштабних інформаційних криз та підвищує стійкість населення до маніпулятивних впливів.

У цьому контексті важливо також відзначити зв'язок поняття «протидія негативним інформаційно-психологічним впливам» із категорією «нівелювання проявів інформаційної експансії», що виступає як логічне продовження і уточнення першого. Нівелювання передбачає активну діяльність держави щодо збалансування інформаційного середовища та створення умов, при яких вплив агресивних або дестабілізуючих інформаційних потоків стає мінімальним або контрольованим. Це не лише технічне блокування або цензурування, а й розробка та впровадження просвітницьких кампаній, підтримка медіаграмотності громадян, формування відкритого, прозорого і довірливого середовища комунікації між державою та населенням.

Важливо також зазначити, що підхід У. Ільницької [63, с. 28] орієнтований на системність та інтеграцію у національну безпекову стратегію. Протидія негативним інформаційно-психологічним впливам і нівелювання проявів інформаційної експансії не розглядаються ізольовано, а у тісному взаємозв'язку з іншими елементами національної системи безпеки, включно з оборонною, економічною, соціальною та правовою політикою. Такий комплексний підхід дозволяє забезпечити не лише захист окремих елементів інформаційного простору, а й зміцнення загальної стійкості суспільства до інформаційних загроз, підвищення довіри громадян до державних інститутів і створення умов для ефективної взаємодії між державою, суспільством і приватним сектором у сфері інформаційної безпеки.

У підсумку, запропонована трактовка дозволяє осмислювати поняття «протидія негативним інформаційно-психологічним впливам» як багатовимірний, багаторівневий і інтегрований процес, який охоплює

законодавчий, організаційний, технічний та комунікаційний аспекти і стає ключовою складовою сучасної політики інформаційної безпеки держави, що прагне забезпечити максимальну ефективність захисту суспільства у складних умовах гібридних загроз і глобалізаційних трансформацій.

У даному визначенні присутнє чітке позиціювання призначеннєвої функції «протидії негативним інформаційно-психологічним впливам» як явищу та окреслено інституційний апарат забезпечення даного процесу (інформаційний сегмент, сегмент безпеки). Вбачаємо, що доцільно б додатково розкрити аспект психологічного впливу на індивіда шляхом використання теорії та практики інформаційних загроз, зазначивши наступне : «Психологічна складова інформаційного впливу на індивіда проявляється у ефекті, котрий справляють спроби дестабілізації інформаційної ситуації на окремих представників соціуму, соціальні групи та суспільством (соціум) загалом, тому прямим завданням державного управління є забезпечення стабільного функціонування національного інформаційного апарату та протидія дезінформації».

Розуміння такого явища, як «нівелювання проявів інформаційної експансії» у праці У. Ільницької [63, с. 28] розглядається як дії органів влади, спрямовані на подолання або попередження наявних або потенційних негативних явищ, пов’язаних із дезінформаційними проявами політики інших держав відносно конкретного державного утворення. Доцільно відмітити, що нівелювання проявів інформаційної експансії вчена розглядає у якості як попереджувального механізму (засобу), так і засобу (механізму), що підлягає використанню у випадку наявності певних проблем у інформаційно-безпековій сфері та (або) сфері обігу даних [63, с. 28].

На наше переконання, термін «нівелювання проявів інформаційної експансії» розглянутий дослідницею концептуально, проте потребує більш чіткого дефініціювання саме явище інформаційної експансії. Його доцільно було б визначити, як «прояви провадження політики дезінформації або

інформаційної дестабілізації однією державною щодо іншої шляхом прямого чи опосередкованого втручання першою у державні справи останньої та впливу на них».

Надалі пропонуємо розглянути підходи до визначення та розуміння пов'язаних із терміном «інформаційна безпека» понятійно-категоріальних елементів, як-от «безпека інформації» та «безпека даних».

Зазначені кластери семантично та дещо відмінно розглядалися у працях таких вітчизняних вчених, як О. Архипов та Є. Архипова [4, с. 21-22] та Є. Валюшко [14, с. 35-36] – у обидвох випадках узвичаєння феноменів мало теоретико-практичний характер.

У праці перших термін «безпека інформації» та поняття «безпека даних» розглядалися як тотожні, лише із акцентом на різниці між дефініцією «інформація» та дефініцією «дані» за масштабністю розуміння останніх, адже термін «інформація» може стосуватися будь-яких інтерпретованих матеріалів, що знаходяться на певних носіях, а термін «дані», як правило, стосується певного роду обчислень, структурних елементів певної мережі оброблених архівних та поточних розрахунків систематизаційного характеру [4, с. 22].

Праця другої, в свою чергу, базується на висвітленні різниці між терміном «інформація» та «дані» за призначенням їхнього застосування. Якщо «інформація, на переконання дослідниці, є інтерпретованим виразом певної дійсності, що не позбавлений суб'єктивності, то дані за своєю концепцією є вихідною інформацією, що може бути надалі трансформована у інформаційному просторі [14, с. 36]. Виходячи з цього, «безпека інформації» є схоронністю даних, що підлягали певній видозміні, тоді як «безпека даних» терміном, що позначає неушкодженість вихідної інформації, що підлягає подальшому трактуванню.

Зі свого боку ми вважаємо, що розуміння термінів «безпека інформації» та «безпека даних» у двох вищезазначених дослідженнях є дещо неоднозначним. Так, терміни «інформація» та «дані» у межах зазначених

дефініцій розглядаються з позиції або їхньої приналежності до інформаційного простору, або неоднорідності трактування останніх в силу статусу «інформації» як коригованої константи, а даних – як константи, що підлягає коригуванню.

На наш погляд, доцільно було б конкретизувати відмінності між поняттями «інформація» та «дані» та, як наслідок, поняттями «безпека даних» та «безпека інформації». Зокрема, пропонуємо викласти такі наукові конотації : «Безпека інформації та безпека даних співвідносяться як зміст та форма. Безпека даних є формою – константою, що детермінує можливість надання та оприлюднення інформації. Безпека інформації, в свою чергу, є змістом – константою, що є наслідком належного зберігання та захисту певних інформаційних матеріалів (активів). Враховуючи те, що інформація за своїм призначенням не може бути повною мірою безсторонньою, адже продукується певними суб'єктами (ЗМІ, влада, органи неурядової юрисдикції тощо), поняття «інформація» та «дані» не можуть розглядатися як абсолютно тотожні.

Наразі пропонуємо коротко оглянути підходи та положення щодо визначення феномену «інформаційна безпека» та пов'язаних із ним наукових надбудов в системі іноземного дискурсного поля. На відміну від аналогічного поля досліджень в Україні, нижченаведені підходи базуються насамперед на діалектичному (дослідницько-філософському та необмеженому з позиції наукових розробок та гіпотез) стандарті інкорпорації бачення вчених.

Потребує огляду наукова позиція Н. М. Ахмеда [205, с. 117-118], котрий в пристосуванні до огляду особливостей сучасного дестабілізованого світовпорядкування надав термінологічне пояснення таким дефініціям, як «безпека індивіда» та «економічна безпека», що, своєю чергою, в подальшому відніс до елементів інформаційно-безпекового та національно-безпекового простору. Вчений вважає, що «безпека індивіда» є збірним поняттям, котре визначається як сукупність політичних, економічних, соціальних, академічних, інформаційних прав та свобод, котрі підлягають забезпеченню (реалізації) на рівні публічного управління та адміністрування [205, с. 117]. Економічну

безпеку науковець, в той же час, ототожнює із станом захищеності національного фінансового потенціалу (валютні запаси, золоті резерви тощо), зазначаючи, що безпека економіки також залежить від інформаційної політики держави у даній галузі, що її забезпечує комунікація із громадськістю та охорона державного інформаційно-економічного інтересу [205, с. 118].

У працях таких іноземних учених, як В. Лонг [262, с. 331-333] та Ш. Кайпак [256, с. 868-869] надано визначення поняттям «персональні дані» та «секьюритизація даних», що мають прямий стосунок до понятійно-категоріального апарату терміну «безпека». Так, поняття «персональні дані» розглянуто у обох випадках з позиції чутливої інформації про людину, що агрегується та координується державою та відповідальними за інформаційне поле органами та інституціями [262, с. 331; 256, с. 868], тоді як термін «секьюритизація даних» (інформації) у вищенаведених дослідженнях розглянутий в розрізі процесу вживання державою заходів щодо становлення національного інформаційного простору на предмет гідної його респонденції викликам та загрозам в умовах глобалізованого політичного та геополітичного середовища [262, с. 332-333 ; 256, с. 869].

Понятійно-категоріальні особливості розуміння термінів, дотичних до інформаційно-безпекового простору у модерному форматі виклали іноземні вчені Г. Фаррелл та А. Ньюмен [236, с. 173-174]. Останні виокремили такі терміни, як «соціальні інформаційні трансформації» та «розмивання інформаційного поля» у контексті сучасних тенденцій до політичних видозмін.

Поняття «соціальні інформаційні трансформації» у зазначених дослідженнях [236, с. 173] розглядаються крізь призму перепрофілювань, що продукує сучасний простір даних (соціальних, новинних, політичних та галузевих – цифрових, облікових, розрахункових, обчислювальних тощо), виходячи з чого дана дефініція описана як «інформаційний актив, котрий надається до ознайомлення населенню (громадянському суспільству) з метою формування у нього певної, державно толерованої позиції».

Одночасно з цим, термін «розмивання інформаційного поля» опосередковується через «дії та процеси, що здійснюються державним інституційним апаратом управління інформаційним простором всередині держави або державним апаратом іншої держави щодо держави, проти котрої здійснюється інформаційна кампанія», і, як правило, такі дії спрямовані на видозміну та нівелювання реального стану речей в інформаційному просторі [236, с. 174].

Враховуючи вищезазначене, можемо говорити про подвійний та різнобічний погляд у наведених дослідженнях на проблему інформаційно-безпекового простору. Насамперед, звертаємо увагу на акцентуацію на можливості держави вживати ризикових заходів стабілізації інформаційного поля, що є втратою таких кластерних ознак інформації як соціальної конструкції, як безсторонність, логічність, систематизованість та об'єктивність. Як наслідок, виникають питання щодо опції існування в модерних умовах справедливого та уніфікованого інформаційного простору.

Поміж тим, погляд на проблему розуміння дотичних до понятійно-категоріальної структури терміну «інформаційна безпека» у форматі глобалізованого науково-ретроспективного позиціювання було викладено німецькою вченою Н. Зюфле [300, с. 37-38]. Потрібними вбачаємо визначення термінів «безпекова неоднозначність» та «зростання безпекового тиску», що їх надала остання.

Так, термін «безпекова неоднозначність» у її праці розглянутий як стан наявності подразників політичного, економічного, соціального та інформаційного характеру, котрі прямо або опосередковано здатні дестабілізувати поточний стан соціально-демократичного розвитку та подальший державний розвиток у перспективній сукупності [300, с. 37], тоді як поняття «зростання безпекового тиску» дослідниця пропонує розуміти у якості директивних або індиректних дій органів влади чи інституційного апарату, спрямованих на створення нестабільної внутрішньої інформаційної ситуації,

або ж дії органів влади іншої держави, що організовує несанкціоновані та незаконні втручання у інформаційний простір суверенної держави із використанням методології дезінформації, розмивання інформаційного простору та перекручування реальних фактів та обставин об'єктивної дійсності [300, с. 38].

Додаткової необхідності у формуванні узагальненого бачення проблеми та питання «інформаційної безпеки» набуває її розуміння у статичному полі та, водночас, у практично-прикладній проєкції. Серед вітчизняних досліджень у даному контексті найбільш затребуваним вбачаємо напрацювання В. Шемчука [197, с. 53], котрим було надано індивідуальне дефініціювання понять «інформаційна безпека» та «механізми забезпечення інформаційної безпеки».

Так, вчений вважає, що поняття «інформаційна безпека» підлягає розгляду у вимірі «ступеню захисту систем інформації, баз даних та інших державних ресурсів від несанкціонованого, протиправного (хакерського) доступу, що може передбачати викрадення, повне або часткове знищення (псування) наявної на носіях інформації, а також порушення цілісності і доступності останніх». При цьому, поняття «механізм забезпечення інформаційної безпеки» дослідник пропонує ототожнювати у аспекті пов'язаності останнього із «сукупністю правових, організаційних та іншого роду заходів, за допомогою яких здійснюється приватний та публічний захист інформаційних конструкцій, що сукупно складають систему національної безпеки державного утворення» [197, с. 53-54].

Повинні зауважити, що вищенаведений підхід до концептуалізованого розуміння понять «інформаційна безпека» та «механізм інформаційної безпеки» у якості системного складника безпеки національного масштабу має декілька контраверсійних дескрипцій.

По-перше, нам видається достатньо нелогічним розуміння терміну «інформаційна безпека» виключно у розрізі захищеності даних від внутрішнього втручання. На наш погляд, останнє потребує переосмислення до

питань формування локальних нарисів інформаційної гігієни, інформаційної культури нації, суспільства та, відповідно, засобів масової інформації (ЗМІ).

Також зауважимо, що підхід автора, згідно з яким «механізмом забезпечення інформаційної безпеки» є правові та організаційні конструкції, спрямовані на захист інформаційних конструкцій, залишає певне поле для обговорень у незастосовності інституційного складника реалізації даної державної активності. Враховуючи, що правова та організаційна складові не підлягають реалізації без практично-прикладного впровадження останніх, конкретизації потребує саме залученість державних органів та установ, що реалізують політику у інформаційно-безпековому сегменту державного утворення на локальному та загальнонаціональному рівнях відповідно.

З огляду на вищезазначене, пропонуємо індивідуальні визначення понять «інформаційна безпека» та «механізм інформаційної безпеки» пропорційно матеріалам описаного дослідження. Поняття «інформаційна безпека» доцільно визначати, як захищеність інформаційних систем та баз даних від зовнішнього втручання, а також послідовність внутрішньодержавної інформаційної політики, що гарантує безпеку даних у контексті їхнього зберігання та споживання в політико-соціальному вимірі». В той же час, термін «механізм забезпечення інформаційної безпеки», на наш погляд, повинен визначатися на доктринально-теоретичному рівні як сукупність організаційно-правових та інституційних елементів забезпечення інформаційно-безпекового простору, котрі співвідносяться як зміст та форма реалізації зазначеної феноменологічної конструкції.

Підсумовуючи наявні позитивні та негативні стандарти та особливості розуміння дотичних до «інформаційної безпеки» як явища термінів, можемо відмітити декілька позицій, що потребують видозміни бачення.

В першу чергу, вбачаємо за доцільне трансформувати стилістику визначень дотичних до інформаційної безпеки термінів через урахування у них складових останньої. Наприклад, поняття «економічна безпека», безпека

індивіда» повинні бути дефініційовані шляхом вказання місця інформаційної безпеки у даних феноменологічних категоріях («безпека даних клієнтів банківських установ», «безпека фінансово-економічних ресурсів держави»; «безпека персональних даних індивіда», «безпека чутливих персональних даних індивіда» тощо).

По-друге, термін «інформаційна безпека» міг би бути розглянутий не лише через визначення інваріацій терміну «безпека». Доцільно конкретизувати останній за складовими відмітними характеристиками : «стан захищеності даних», «інформаційна гігієна», «раціональне використання інформаційних ресурсів» тощо. Цим, на наш погляд, можна забезпечити більш предметний погляд на проблему «інформаційної безпеки» в сучасних умовах функціонування понятійно-категоріального апарату, що складають пов’язані із нею терміни та поняття.

Водночас, повноцінна систематизація феноменології понятійно-категоріального апарату конструкту «інформаційна безпека» у системі національної безпеки дозволила дійти наступних проміжних умовиводів.

В першу чергу, визначення дотичних до терміну «інформаційна безпека» понять у межах вітчизняного та зарубіжного науково-дослідницького поля дещо відрізняється : так, в рамках національної системи дискурсу наявний акцент на предметний огляд проблеми «інформаційної безпеки» та пов’язаних із нею феноменів інформаційно-безпекового середовища, тоді як іноземні дослідження та підходи насамперед базуються на діалектичному (дослідницько-філософському та необмеженому з позиції наукових розробок та гіпотез) стандарті інкорпорованого огляду проблеми.

По-друге, проблемним питанням, що, водночас, може бути полем тенденцій до його подальшого врегулювання, можна називати наявність у рамках вітчизняних та іноземних розробок щодо інформаційної безпеки колізій категоріального апарату. До прикладу, контраверсійним вбачається розкриття пов’язаних із терміном «інформаційна безпека» понять виключно через

категоризування та теоретизування дефініції «безпека», а також понять опосередкованої дотичності, як-от «інформація», «дані» та їхнє розмежування.

По-третє, питання понятійно-категоріального розуміння апарату «інформаційної безпеки» як явища та феномену об'єктивної дійсності потребує трансформованого погляду в умовах модерних змін, трансформацій геополітичного, глобалізаційного, інформатизаційного, цифровізаційного та діджиталізаційного спектрів.

1.2. Інформаційна безпека як система суспільних відносин та об'єкт публічного управління

Вищепроведене дослідження понятійно-категоріальних особливостей розуміння термінів, що корелюють із поняттям «інформаційна безпека» дозволило констатувати наявність широково поля для дослідницького аналізу безпосередньо феномену інформаційної безпеки. Пропонуємо нижче розглядати останню у двох проєкціях – як систему суспільних відносин та об'єкт правової охорони.

Початково оглянемо деякі сегментарні особливості терміну та явища «інформаційна безпека», котрі вбачаємо застосовними у контексті проведення дослідження його контекстуальних рис (складових).

Опираючись на іноземну парадигму досліджень категорії «інформаційна безпека», можемо зробити висновки про її принципологічний характер існування.

Зокрема, у матеріалі американських науковців М. Е. Віттмена та Г. Дж. Метторда [294, с. 217] зазначено, що під інформаційною безпекою держави доцільно розглядати кластерний складник національної безпеки, котрий сегментується за заходами, способами, методологією та механізмами, що їх використовує держава у процесі відстоювання національного інтересу крізь

призму діяльності в інформаційному просторі. Безпека інформації в даному випадку розглядається вченими у широкому форматі, адже до джерел (об'єктів) охоплення останньою у праці віднесено інформаційно-ресурсну безпеку, комунікаційно-засобову безпеку та, водночас, безпеку інфраструктури, що використовується для передачі даних (інформації). Ключовим завданням інформаційної безпеки як спрямованої та координованої діяльності держави та відповідальних інституцій у дослідженні виокремлено запобігання загрозам, що прямим або опосередкованим чином можуть завдати шкоди державним інтересам, глобальним (національним) інтересам та громадянам, а також інфраструктурному державному забезпеченню.

Серед іноземних досліджень поняття «інформаційна безпека» також звертаємо увагу на працю М. Воркмена [296, с. 319-320], що розглянув її з позиції менеджменту (управління) останньою та підходу до нівелювання потенційних загроз реалізації останньої як державного курсу. На його переконання, під інформаційною безпекою доцільно розуміти статус захищеності та схоронності даних, що мають значення для повноцінного функціонування держави, та конкретизуються за такими елементами, як захист критичної інфраструктури від кібератак, протидія кіберзлочинності та кібертероризму у якості кіберзагроз, а також протидія інформаційно-психологічним впливам та атакам, котрі, як правило, спрямовані проти населення та громадянського суспільства.

Сукупність проаналізованих підходів до визначення терміну «інформаційна безпека» саме в іноземному науковому полі дозволяє говорити про деякі риси інформаційно-безпекового середовища, котрі детермінують необхідність подальшого її дослідження у якості системи суспільних відносин та об'єкта правової охорони. На відміну від підходів до розуміння терміну «інформаційна безпека» у дослідницькому полі України (інформаційна безпека як ступінь захисту інтересу держави на внутрішній та міжнародній арені), зазначені іноземні підходи надають можливість говорити про значення

інформаційної безпеки як складної державної конструкції, що має власне призначення, завдання та об’єкти реалізації.

Саме тому пропонуємо надалі розглядати особливості інформаційної безпеки як системи суспільних відносин та об’єкта правової охорони, використовуючи іноземний підхід до її трактування, проте із урахуванням та аналізом особливостей зазначених її кластерних складових як в Україні, так і закордоном.

Відтепер вбачаємо за доцільне більш конкретно познайомитися із понятійно-категоріальними визначенням особливостей інформаційної безпеки як системи суспільних відносин. У рамках вітчизняних досліджень дана константа прямо або опосередковано розглянута О. Панченком [136, с. 135-139], М. Гаврильцівим [21, с. 200-203], М. Шевчуком [195, с. 134-139], О. Золотарем [60, с. 139-148] та ін. Іноземні дослідження в сфері категоризування та теоретизування інформаційної безпеки як системи суспільних відносин, в свою чергу, представлені напрацюваннями Г. Біголі [212, 1152 с.], Т. Фітцджеральда [239, 431 с.] та ін.

Загальне бачення інформаційної безпеки як системи суспільних відносин зведено до її розкриття та узвичаєння у форматі сукупних інтеракцій між суб’єктами державного управління та суспільства, що у процесі взаємодії між собою забезпечують належний рівень координаційного впровадження захисту інформаційного простору (ширше – інформаційного середовища) від різноманітних наявних та потенційних загроз [212, с. 177]. Інші, більш конкретизовані контексти розуміння інформаційної безпеки як системи суспільних відносин передбачають її ототожнення із технікою та юридичним (нормативним) сегментом її упровадження на практиці, що, знову-таки, підлягає реалізації такими суспільними групами, як держава, громадяни, бізнес-сфера, освітньо-наукова складова – виходячи з чого доцільно говорити про соціально-феноменологічну структуру розуміння зазначеного терміну [239, с. 97].

Означені вище конструкційні стандарти розуміння інформаційної безпеки як системи суспільних відносин надають виключно статичне, теоретичне розуміння зазначеного феномену. Водночас останній, маючи статус системи, наділений певними елементами та особливостями. Серед ключових, на наш погляд, елементів доцільно виділяти такі, як суб'єкти, об'єкт, нормативне регулювання, соціальні інститути, цілі, засоби, методи; тоді як серед ключових особливостей – аспект суб'єктної взаємозалежності, громадянської участі, інформаційної грамотності, етики та відповідальності. Надалі пропонуємо акцентувати увагу на теоретико-доктринальних твердженнях у вітчизняному та іноземному дослідницькому полі, що розкривають соцілаьно-правову та публічно-управлінську природу складників зазначеної тези.

Так, у дослідженні вітчизняного дослідника О. Панченка [136, с. 137-138] зазначається, що елементом інформаційної безпеки у її суспільному вимірі правовідносин є суб'єктний складник. Так, до суб'єктів інформаційної безпеки держави з точки зору теорії в розрізі ототожнення останньої із системою суспільних відносин, відповідно позиції науковця, необхідно відносити державу, громадянське суспільство, бізнес та міжнародні організації.

Держава як суб'єкт, що входить до системи суспільних відносин у інформаційно-безпековій галузі, на переконання вченого являє собою гаранта, що сприяє адекватному та стратегічному нормативно-правовому, власне інформаційному та інфраструктурному забезпеченню контролю над сферою даних, зокрема, обігом останніх [136, с. 137].

Громадянське суспільство у контексті складової системи суспільних відносин інформаційно-безпекового спрямування науковець розглядає як споживачів та генераторів даних (інформації), до компетентнісної сфери котрих входить предметна обізнаність та протидія загрозам інформаційного спрямування, а також відповідальність за дотримання звичаєвим та предметно-законодавчих нормативів та положень щодо підтримання інформацйної гігієни [136, с. 137].

Сфера бізнесу в статусі учасника системи суспільних відносин у галузі інформаційної безпеки розглядається дослідником як діяльність підприємств, установ та організацій, спрямована на надання послуг інформаційного характеру, а також – розробку програмного забезпечення, покликаного надавати засоби захисту урядовим та неурядовим організаціям у контексті забезпечення захисту персональних даних громадян чи партикулярної клієнтської бази [136, с. 138].

Наостанок, роль та місце міжнародних організацій у стандартизації системи суспільних відносин у галузі інформаційної безпеки, згідно матеріалу зазначеного дослідження [136, с. 138] полягає у глобальному координаційному забезпеченні стандартів сфери інформаційної безпеки.

Вбачаємо зазначене позиціювання особливостей розуміння суб'єктів інформаційної безпеки держави у системі суспільних відносин даної галузі концептуальним. У ньому викладено чотири агрегації системи правовідносин у сфері інформаційної безпеки та розкрито кожен елемент останніх – публічно-управлінський, соціальний, економічний та міжнародний. Дане дослідження було б логічно також доукомплектувати конкретним визначенням усіх зазначених детермінант (держава, громадянське суспільство, бізнес, міжнародні організації як суб'єкти системи суспільних відносин у галузі інформаційної безпеки – із урахуванням відмітним особливостей останніх, що конкретизовані вище).

Об'єкт у якості елемента інформаційної безпеки як системи суспільних відносин у теоретичному розумінні являє собою сталу парадигму інформаційного середовища. Нам імпонує позиція того-таки вітчизняного дослідника О. Панченка, котрий уже у процесі аналізу інформаційної складової національної безпеки [136, с. 7] зазначив, що об'єктом інформаційної безпеки як системи суспільних відносин виступає інформаційне середовище, що наповнене інформаційними ресурсами, такими як бази даних, інформаційні системи чи хмарні сховища. Окрім того, об'єктна складова інформаційної

безпеки як системи суспільних відносин також включає в себе наявність комунікаційних засобів та механізмів (мережа Інтернет, медіапростір), інформаційної інфраструктури (сервери та обладнання мережі) та контенту, що використовується для агрегації даних (новини, повідомлення, статті інформаційного характеру).

Ми вважаємо, що зазначена описова складова об'єкта у якості елемента інформаційної безпеки як системи суспільних відносин виокремлює усіх необхідних дієвих осіб, що можуть прямо або опосередковано впливати на структуризацію інформаційної безпеки на рівні публічного управління та адміністрування. Акцентуація на використанні інформаційних ресурсів цифрового формату для агрегації інформаційної безпеки (мережа Інтернет, бази даних, медіапростір) підкреслює яскравий соціальний характер інформаційної безпеки як суспільного феномену.

В свою чергу, теоретичний огляд та розуміння нормативно-правового регулювання інформаційної безпеки у якості системи суспільних відносин в рамках національного поля досліджень було здійснено М. Гаврильцівим [21, с. 202], котрий відмітив, що процес нормативної регуляції є важливим елемент інформаційної безпеки у якості системи суспільних відносин в силу того, що ним детерміновано права, обов'язки та тенденційність діяльності та взаємодій суб'єктів інформаційного простору, а також за його допомогою відбувається встановлення захист прав та законних інтересів населення в сфері інформаційної безпеки шляхом встановлення юридичної відповідальності за порушення законодавства у зазначеній галузі.

Схиляємось до думки, що зазначений підхід конкретизовано визначає призначеннєву функцію нормативно-правового регулювання у сфері інформаційної безпеки як системи суспільних відносин, проте потребує доопрацювання у питаннях конкретизації видів (типів) такого нормативно-правового регулювання. Так, доцільно термінувати та надати визначення таким поняттям, як «позитивне нормативно-правове регулювання» (законодавча

норма, що має диспозицію та санкціонування) та «негативне нормативно-правове регулювання» (положення законодавства, що врегульовує раніше не врегульовані суспільні відносини у сфері інформаційних відносин ретроспективно).

Соціальні інститути, цілі, а також засоби та методи захисту як складові частини інформаційної безпеки у якості системи суспільних відносин вбачаємо за доцільне розглянути у єдиній органічній сукупності.

Так, у рамках вітчизняних досліджень під соціальними інститутами як елементами інформаційної безпеки як системи суспільних відносин запропоновано розуміти органи державної влади, інституцій правового захисту, освітні та наукові установи, що культивують інформаційно-безпекову обізнаність на суспільному рівні (включно із нормативною базою, програмами медіаграмотності та кібербезпеки, моніторингом інформаційних загроз та своєчасним інцидентним реагуванням) [21]. Одночасно з цим, цілі інформаційної безпеки у якості елемента суспільних відносин в зазначеній галузі розглядаються з позиції таких домінант, як права та свободи громадян та їхній захист, а також відстоювання державного, соціального та економічного інтересу в просторі інформації (даних) [21]. Засоби та методи захисту у якості елементів інформаційної безпеки як системи суспільних відносин доцільно, водночас, розуміти як сукупність технічних та організаційних заходів, спрямованих на створення інформаційно-безпекового культивованого середовища, в котрому активно функціонують комунікаційні канали та системи інформаційного захисту, а також здійснюється моніторинг кіберзагроз та проводяться курси медійної та кіберграмотності [21].

Вищепроаналізоване дозволяє дійти висновку, що зазначена парадигма, котра певним чином передвизначає та детермінує інформаційну безпеку як систему суспільних відносин є структурним тріумвіратом інституційно-методичного впорядкування, що має цілі та функціонуєвідповідно до них. Оглянуті теоретичні підходи вбачаємо інноваційними та схиляємось до думки,

що останні наразі не потребують видозмінених доопрацювань, проте вимагають активізації подальших розробок у зазначеному сегменті теорії в її публічно-управлінському прояві.

Від аналізу елементів інформаційної безпеки як системи суспільних відносин надалі пропонуємо перейти до дослідження її конкретизованих особливостей, серед яких виділяємо аспект суб'єктної взаємозалежності, громадянської участі, інформаційної грамотності, етики та відповідальності. Надалі розглядатимемо останні більш детально крізь призму наукових напрацювань вітчизняних та зарубіжних науковців.

Так, питання взаємозалежності суб'єктів у якості відмітної риси інформаційної безпеки як системи суспільних відносин у вітчизняному та зарубіжному полі дискурсного аналізу розглядається з позиції взаємного зв'язку держави, громадянського суспільства та бізнесу, а також пов'язаності трьох вищезазначених суб'єктів із міжнародним аспектом регулювання інформаційної безпеки. Такий взаємозв'язок породжує ситуацію, де бізнес технологізує рішення у галузі інформаційної безпеки, держава генерує правила на рівні нормативного впорядкування інформаційно-безпекового простору, а на громадян покладено обов'язок дотримання вищезазначених правил задля повноцінності та ефективності функціонування вищезазначеної системи.

Аспект громадянської участі як елементу інформаційної безпеки у якості системи суспільних відносин переважно зарубіжні вчені та науковці [135, 212] ототожнюють із роллю та місцем громадянського суспільства у культивації норм, правил та стандартів виконання державою парадигм інформаційної безпеки у проєкції ефективності. Компетентнісний складник громадянського суспільства у питаннях інформаційної безпеки як системи суспільних відносин, в свою чергу, має включати в себе такі якісні навички, як обізнаність щодо загроз інформаційного простору, володіння навичками збереження інформації (даних), а також формування відповідальності щодо поведінки в просторі інформації.

Інформаційна грамотність у контексті особливості інформаційної безпеки як системи суспільних відносин, своєю чергою, у парадигмі вітчизняного наукового поля ототожнюється із навчанням детекції дезінформації, обізнаності про кібербезпеку як ідеальний (рамковий) стан інформаційної захищеності та, водночас, кіберзагрозу як негативного антагоніста першої, а також формуванням у індивіда (громадянина, представника громадянського суспільства) паттернів критичного мислення при споживання інформації та перебування в реальному або штучному (цифровому) інформаційному просторі [212].

Наостанок, етика та відповідальність у якості складових частин (елементів) особливостей інформаційної безпеки як системи суспільних відносин може бути розкрита у двох проєкціях.

Перша, котру пропонують деякі вітчизняні дослідники інформаційно-безпекового питання [68], полягає у необхідності підлаштовувати сучасне поле споживання, використання, агрегації та генерації інформаційних даних пропорційно таким тенденціям, як технологічний розвиток, зростання обсягів даних та використання даних у приватному та публічному контекстах одночасно.

Друга, запропонована представниками іноземної доктрини аналізу проблеми інформаційної безпеки у її презентних проявах [238], більшою мірою акцентується на індивідуально-соціальному підході, що вимагає від суспільства підвищення рівня інформаційної культури населення, що включає уміння слідкувати за акцептованим використання власних персональних (особливо – чутливих) даних, відстежувати етичність інформації, що надається для споживання на новинних та інших інтернет-ресурсах, а також розуміння природи та походження фейкових нових.

Проаналізовані підходи до визначення та розуміння особливостей інформаційної безпеки у якості системи суспільних відносин дозволяють говорити про багатогалузевий порядок правовідносин навколо даних як

предмета кооперації. Така кооперація, як правило, виникає між владою (інституціями) та громадянським суспільством, бізнесом, також частково – міжнародними організаціями у контексті дотримання та реалізації законодавчих норм та положень щодо інформаційної безпеки, котрі є неухильними та обов'язковими у питаннях їхнього дотримання.

Елементом та складником формування нормативної рамки правовідносин щодо інформаційної безпеки між суб'єктами є правова охорона останньої. Саме тому вважаємо за доцільне сконцентруватися на огляді феномену інформаційної безпеки як об'єкта правової охорони нижче.

Ідеологічна константа «інформаційна безпека як об'єкт правової охорони є предметом наукових досліджень як вітчизняних, так і іноземних дослідників. Найдоцільніше, на наше переконання, в даному випадку орієнтуватися на праці таких науковців, як О. Пащенко [138, с. 11-17], Л. Демидова [30, с. 354-357], В. Аніщук [285], М. Баран [8, с. 50-56], Р. Карагіоз та О. Вдовиченко [65, с. 34-36]. Серед представників іноземної доктрини, водночас, питання ідеологічної константи «інформаційна безпека як об'єкт правової охорони» розглянули у власних дослідженнях Р. Волтерса [292, 458 с.], Дж. Л. Грами [246, 552 с.] та К. Кіфер [257, 82 с.].

Вітчизняний дослідник О. Пащенко [138, с. 12-13] пропонує розглядати конкретно кримінально-правову характеристику інформаційної безпеки як об'єкта правової охорони крізь призму положень Особливої частини Кримінального кодексу України. Отже, інформаційна-безпека як об'єкт правової охорони, виходячи із матеріалів даного дослідження, знаходить прояв у підтримці конституційного ладу, захищеності державної влади, схоронності даних та інформації, що становить державну таємницю та гарантуванні її нерозповсюдження за межі державного апарату, а також у гарантуванні захищеності та схоронності даних, що стосуються дислокації, готування операцій Збройними Силами України та іншими військовими формуваннями. Зазначені положення логічно виходять із розділу І (Злочини проти основ

національної безпеки України) Кримінального кодексу України, що своєю чергою свідчить про прямий зв'язок інформаційної безпеки як об'єкта правової охорони із державним курсом та політикою.

В той же час, у праці Л. Демидової акцентовано увагу на європейських стандартах кримінально-правової охорони інформаційної безпеки [30, с. 355], насамперед, на основі концептуальної трансформації кримінального права на початку 2000-х років відповідно інформатизації. На основі матеріалів Конвенції про комп'ютерні злочини, прийнятої Радою Європи 23.11.2001 р., вчена дійшла до висновку, що інформаційна безпека як об'єкт правової охорони є в першу чергу станом захищеності суспільства від злочинів у цифрову сферу, що можуть стосуватися як дестабілізації ситуації в державі, так і викрадення персональних даних індивіда, що може загрожувати його індивідуальній безпеці в умовах діджиталізованого середовища. Фактично це означає, що проблема інформаційної безпеки як об'єкта правової охорони розглядається у даному дослідженні у більш широкому форматі, аніж ототожнення безпеки інформації виключно із безпекою держави та населення як соціальної групи.

Праця представника вітчизняної доктрини, В. Аніщук [285], своєю чергою являє собою своєрідну компіляцію між кримінально-правовим та цифровим розумінням безпеки інформації як явища. Так, зазначається, що інформаційна безпека як об'єкт правової охорони перебуває у полі національно-безпекового захисту, котрий, відтак, проявляється у глобальному розумінні даної константи, а саме – використанні правових норм та положень для захисту інформаційного інтересу суспільства, держави та галузі бізнесу. З точки зору нормативно-правової та державно-управлінської теорії, відтак, саме на законодавчі акти покладається обов'язок щодо регулювання інформаційних відносин, включно із сегментом їхнього захисту та відповідальності за порушення таких положень.

Окрім кримінально-правової та цифрової конструкції регулювання та розуміння інформаційної безпеки держави як об'єкта правової охорони,

доцільно також виокремити такий сегмент її конкретизації, як адміністративно-правова регуляція галузі. На переконання вітчизняної дослідниці М. Баран [8, с. 52-53], відсутність конкретизації саме адміністративного регулювання сфери інформаційної безпеки шляхом конкретизації відповідальності за дрібні правопорушення могло б мати статус превентивного регулятора більш ускладнених правопорушень у зазначеній сфері. Станом на зараз, однак, термін адміністративно-правового регулювання інформаційної безпеки у якості об'єкта правової охорони доцільно розглядати як сукупність норм, що прямо або опосередковано доповнюють та реалізовують наявність права громадянина на персональний інформаційний захист, котрий забезпечується інституційно.

Натомість у спільному дослідженні Р. Карагіоза та О. Вдовиченка щодо сегментування дефініції «інформаційна безпека» у її правовому напрямі сутність інформаційної безпеки держави як об'єкта правової охорони розкривається за методологією, що в даному випадку може бути використана [65, с. 35] . На думку дослідників, методичне забезпечення інформаційної безпеки держави як об'єкта правової охорони може проявлятися не лише у нормативній регуляції даного сегмента, котра передбачає правові норми щодо захисту інформації, а й у ліцензуванні та моніторингу (вимоги щодо захисту даних на рівні держави та населення та контроль за їхнім дотриманням) та санкціонуванні – у випадку порушення норм та правил щодо інформаційної безпеки.

Проаналізовані вище вітчизняні дослідження щодо питання ототожнення інформаційної безпеки як об'єкта правової охорони, відтак, концентрується на позиціюванні останньої як своєрідного обопільного зобов'язання держави та населення. Останні першочергово проявляються у обов'язках держави щодо забезпечення безпеки інформації на публічному рівні (ресурси, бази даних, джерела інформації) та захисту інформації як елемента соціального існування громадянина (персональні дані, інформація користувачів тощо), а також обов'язках населення щодо неухильного дотримання норм та положень

законодавства в сегменті ефективного інформаційно-безпекового функціонування державного апарату.

Для повноцінного осмислення проблеми інформаційної безпеки у якості об'єкта правової охорони наразі пропонуємо коротко оглянути іноземні підходи до уніфікації зазначеної конструкції в науковому полі.

На думку Р. Волтерс [292], наприклад, інформаційна безпека як об'єкт правової охорони являє собою систему суспільних відносин, що потребує врегулювання на законодавчому рівні з метою гармонізації правовідносин між суб'єктами інформаційної безпеки та забезпечення сприятливого інформаційного середовища всередині держави. Інформаційна безпека як об'єкт правової охорони розглядається як з точки зору функціонування друкованих джерел інформації в питаннях їхнього розповсюдження, так і з позиції обігу інформації, викладеної в межах мережі Інтернет та електронних джерелах інформації.

Іноземний дослідник Р. Волтерс [292, с. 27] схильний вважати, що інформаційна безпека як об'єкт правової охорони складається із таких елементів, як захист даних, кібербезпека, юридичний механізм регуляції даного питання та адекватність і вмотивованість використання штучного інтелекту (ШІ). Технологізація діяльності держави, а також діджиталізація Інтернет-простору у питаннях зберігання інформації (від новинної до такої, що становить державну таємницю) на цифрових носіях ставить питання не лише щодо правової охорони даних як активу (класичний підхід), але й правової охорони ресурсів, що використовуються для систематизації таких даних, непорушність та цілісність котрих власне і детермінує інформаційну безпеку на партикулярному та глобальному рівнях.

В свою чергу, Дж. Л. Грама [246, с. 77] та К. Кіфер [257, с. 35], розглядаючи інформаційну безпеку як об'єкт правової охорони крізь призму її легального та процедурного управління відмічають, що складниками останньої є нормативна база, інституційна юрисдикційність відповідальних за галузь

органів, а також синхронізація між положеннями законодавства та компетентністю органів державної влади, що реалізують, спрямовують та координують внутрішньодержавну політику в інформаційно-безпековій парадигмі.

Так, іноземний складник розуміння інформаційної безпеки у якості об’єкта правової охорони дозволяє говорити про превалювання державної відповідальності у даній галузі над соціальною (громадянською). На наше переконання, дана позиція заслуговує на увагу в тому сенсі, що покладає саме на органи державної влади, а також легіслативний апарат обов’язок гармонізації внутрішнього інформаційно-безпекового простору держави у руслі його відповідності державному курсу. За таких умов, на наше переконання, слідування законодавчим положенням щодо інформаційної безпеки від громадян є виключно питанням процедурного характеру, адже державний кластер спрямовуватиме інформаційно-безпекову культуру та свідомість останніх.

Проаналізовані вище стандарти ототожнення інформаційної безпеки як об’єкта правової охорони, на наш погляд, потребують певної систематизації за основоположними характеристиками. Останні викладено у табл. 1.1, що розташована нижче.

Сукупність проаналізованої інформації та наукових підходів до розуміння інформаційної безпеки як системи суспільних відносин та об’єкта правової охорони дозволила нам дійти наступних проміжних умовиводів.

По-перше, інформаційна безпека у якості системи суспільних відносин фактично являє собою формат сукупних інтеракцій між суб’єктами державного управління та суспільства, що у процесі взаємодії між собою забезпечують належний рівень координаційного впровадження захисту інформаційного простору від наявних або гіпотетичних загроз галузі.

Таблиця 1.1. Ототожнення інформаційної безпеки як об'єкта правової охорони : вітчизняна та зарубіжна наукові парадигми

Наукова парадигма	**Особливості та концептуальні риси розуміння поняття «інформаційна безпека як об'єкт правової охорони»**
Вітчизняна наукова парадигма (інформаційна безпека як об'єкт правової охорони)	Структура інформаційної безпеки формату «закон-держава-нація». Розуміння інформаційної безпеки як об'єкта правової охорони крізь призму методичного забезпечення останньої в рамках держави як об'єкта правової охорони. Це може проявлятися не лише у нормативній регуляції даного сегмента, котра передбачає правові норми щодо захисту інформації, а й у ліцензуванні та моніторингу (вимоги щодо захисту даних на рівні держави та населення та контроль за їхнім дотриманням) та санкціонуванні – у випадку порушення норм та правил щодо інформаційної безпеки. Інформаційна безпека як об'єкт правової охорони перебуває у полі національно-безпекового захисту, котрий, відтак, проявляється у глобальному розумінні даної константи, а саме – використанні правових норм та положень для захисту інформаційного інтересу суспільства, держави та галузі бізнесу. Сприйняття інформаційної безпеки як об'єкта правової охорони крізь призму її пов'язаності із кримінально-правовим спектром, а саме кримінальним законодавством та потенційним настанням відповідальності в даному сегменті (як злочини проти держави). Інформаційна безпека держави тотожна інформаційній безпеці індивіда.
Зарубіжна наукова парадигма (інформаційна безпека як об'єкт правової охорони)	Інформаційна безпека держави – об'єкт правової охорони саме органів державної влади. Інформаційна безпека держави являє собою систему суспільних відносин, що потребує врегулювання на законодавчому рівні з метою гармонізації правовідносин між суб'єктами інформаційної безпеки та забезпечення сприятливого інформаційного середовища всередині держави, моніторингу друкованих джерел інформації в питаннях їхнього розповсюдження, а також обігу інформації, викладеної в межах мережі Інтернет та електронних джерелах інформації.
Пропозиції ототожнення феномену «інформаційна безпека як об'єкт правової охорони»	Необхідність законодавчого (нормативно-правового) ототожнення термінів «інформаційна безпека держави» та «інформаційна безпека громадянина» (обидві константи є де-факто об'єктами правової охорони інформаційної безпеки як явища). Наявність законодавчого визначення терміну «інформаційна безпека як об'єкт правової охорони» із переліченням відповідальних суб'єктів. Систематизація інформаційної безпеки як системи суспільних відносин та об'єкта правової охорони.

По-друге, розуміння інформаційної безпеки як об'єкта правової охорони крізь призму методичного забезпечення останньої в рамках держави як об'єкта правової охорони проявляється не лише у нормативній регуляції даного сегмента, котра передбачає правові норми щодо захисту інформації, а й у

ліцензуванні та моніторингу (вимоги щодо захисту даних на рівні держави та населення та контроль за їхнім дотриманням) та санкціонуванні – у випадку порушення норм та правил щодо інформаційної безпеки. Інформаційна безпека як об’єкт правової охорони перебуває у полі національно-безпекового захисту, котрий, відтак, проявляється у глобальному розумінні даної константи, а саме – використанні правових норм та положень для захисту інформаційного інтересу суспільства, держави та галузі бізнесу.

По-третє, на наш погляд, задля ефективних трансформацій розуміння феномену «інформаційна безпека як об’єкт правової охорони» доцільно впровадити законодавче (нормативно-правове) ототожнення термінів «інформаційна безпека держави» та «інформаційна безпека громадянина» (обидві константи є де-факто об’єктами правової охорони інформаційної безпеки як явища, нормативно визначити термін «інформаційна безпека як об’єкт правової охорони» із переліченням відповідальних суб’єктів, а також систематизувати інформаційної безпеки як системи суспільних відносин та об’єкта правової охорони.

1.3. Система суб’єктів забезпечення інформаційної безпеки в публічному управлінні

Забезпечення інформаційної безпеки в Україні, як ми зазначали раніше, є багатоскладним процесом та складається із нормативного та, власне, інституційного складника реалізації зазначеної ініціативи, що доповнюють один одного.

Інституційний складник забезпечення інформаційної безпеки України реалізується за допомогою системи суб’єктів, відповідальної за даний напрям пропорційно колу власної компетенції. До таких, як, знову-таки, наголошувалося у п. 2.1 Розділу ІІ даного дисертаційного дослідження, де розглядалися аспекти поняття та принципів побудови механізму правового

регулювання забезпечення інформаційної безпеки в Україні, належать Служба безпеки України (СБУ), Рада національної безпеки і оборони України (РНБО), Міністерство цифрової трансформації України (Мінцифра), Національна поліція України (Нацполіція) та Міністерство культури (Мінкульт).

У даному пункті дисертаційного дослідження пропонуємо зосередити увагу на аналізі ролі та місця кожного у формування інформаційно-гігієнічного та інформаційно-безпекового поля в Україні в умовах глобальних викликів та трансформацій.

Пропонуємо розпочати із дослідження ролі та місце Служби безпеки України (СБУ) у архітектуванні політики інформаційної безпеки України та захисту інформації в сучасних умовах, особливо – в світлі повномасштабної неспровокованої збройної агресії рф проти України від 24.02.2022 р.

Так, законодавча кореляція між діяльністю Служби безпеки України (СБУ) та її компетенцією щодо забезпечення інформаційної безпеки України наявна у ст. 10 Розділу ІІ Закону України «Про службу безпеки України» № 2229-XII [54]. Тут законодавцем зазначено, що центральним управлінням Служби безпеки України у якості одного із елементів системи організації діяльності даного органу може бути здійснено заходи щодо контррозвідувального захисту інтересів держави у сфері інформаційної безпеки. Оскільки законодавець далі за текстом не розкриває повноважень Служби безпеки України (СБУ) у даному контексті більш конкретизовано, здійснимо авторське тлумачення зазначеної нормативної конотації нижче.

Так, категорія «інтереси держави у сфері інформаційної безпеки» може бути розкрита за декількома категоріальними напрямами. Серед них – захист державних інформаційних ресурсів, протидія інформаційним загрозам та, зокрема, дезінформації, а також – координація дотримання законодавства у сфері інформаційної безпеки України задля забезпечення інформаційної обороноздатності держави, що визнається одним зі складників державного (національного) суверенітету. Таким чином, можна зробити висновок про роль

Служби безпеки України в забезпеченні інформаційної безпеки саме за зазначеними пріоритетними профілями, і, окрім того, констатувати, що саме перелічені напрями інтересів держави у сфері інформаційної безпеки, що підлягають захисту Службою безпеки України, власне формують архітектуру державної інформаційної безпеки України на сьогодні.

Ключовим стосовно повноважень Служби безпеки України (СБУ) відносно забезпечення інформаційної безпеки, на наш погляд, є мультифункціональна роль органу щодо контролю та нагляду за елементами формування національної інформаційної політики, підтримання інформаційної гігієни на внутрішньодержавному рівні та створення передумов до мінімізації або нівелювання правопорушень у сфері інформаційної безпеки водночас.

Також потрібно відмітити, що свою діяльність Служба безпеки України (СБУ) як найвищий у ієрархії забезпечення інформаційної безпеки орган державної (публічної) влади провадить не персонально, а у тісному взаємозв’язку та на засадах взаємодії із іншими органами державної влади, а саме – Радою національної безпеки та оборони України (РНБО), Міністерством цифрової трансформації України (Мінцифрою) та Національною поліцією України (Нацполіцією). Пропонуємо розглянути специфіку такої взаємодії у контексті забезпечення системності суб’єктів забезпечення інформаційної безпеки в Україні станом на сьогодні.

Повноваження та компетенція Ради національної безпеки та оборони України (РНБО) у контексті забезпечення інформаційної безпеки України концептуалізуються відповідно до галузевого Закону України «Про Раду національної безпеки та оборони України» № 183/98-ВР [53], що визначає коло компетенції органу в усіх сферах державного спрямування та координації, включно із інформаційною.

Так, згідно із абз. 2 п. 1 ч. 1 ст. 4 Закону України «Про Раду національної безпеки та оборони України» № 183/98-ВР [53], компетенція Ради національної безпеки та оборони України поширюється, зокрема але не виключно, на сферу

протидії порушень стратегічних національних інтересів держави в інформаційній сфері, що є одним зі складників національного благоденства та розвиткової стабільності.

В свою чергу, відповідно до абз. 7 п. 1 ч. 1 ст. 4 Закону України «Про Раду національної безпеки та оборони України» № 183/98-ВР [53], національним законодавцем презюмується опція діяльності Ради національної безпеки і оборони України на засадах проведення (здійснення) заходів інформаційного характеру з метою масштабування потенційних та реальних загроз у даній сфері у їхньому глобальному вимірі.

Сукупність зазначених наукових конотацій щодо розуміння повноважень Ради національної безпеки та оборони України (РНБО) у індивідуальному вимірі та поєднанні із компетенцією Служби безпеки України (СБУ) дозволяє говорити про спрямованість на координацію національного інформаційного простору, проте, якщо Рада національної безпеки та оборони України проводить радше поточні заходи зі стабілізації національної безпекової карти та парадигми держави, то Служба безпеки України здійснює контроль за діяльністю органів, що знаходяться відносно неї нижче за юрисдикцією.

Особливість Ради національної безпеки та оборони України (РНБО) у даному сегментарному співвідношенні полягає в тому, що інформаційна безпека як предмет регулювання, як і у випадку зі Службою безпеки України (СБУ), розглядається крізь призму глобального національного інтересу держави, що полягає у ототожненні національної безпеки із безпекою інформації та, як наслідок, захищеністю державних ресурсів від потенційних атак та нападів (посягань) гібридної генерації.

Сутнісного значення у контексті раніше згаданої взаємодії зі Службою безпеки України (СБУ) набувають положення та компетенція щодо формування підвалин інформаційної безпеки в Україні Міністерства цифрової трансформації України (Мінцифри). Діяльності останньої як суб’єкта забезпечення інформаційної безпеки регламентується безпосередньо

Постановою КМУ № 856 від 18.09.2019 р. Питання Міністерства цифрової трансформації [146]. Нижче розглянемо певні особливості компетенції даного суб'єкта забезпечення інформаційної безпеки як у контексті взаємодії зі Службою безпеки України (СБУ), так і з Радою національної безпеки та оборони України (РНБО).

Першочергово має зауважити, що роль та місце Міністерства цифрової трансформації (Мінцифри) у формуванні національної архітектури інформаційної безпеки формується на основі та підставі необхідності балансування та впорядкування даних та інформаційних систем в умовах глобалізації, інформатизації та діджиталізації. Це стосується як джерел інформації, що мають на меті власне обробку та систематизацію даних приватної ґенези, так і даних, що містять конструктивно важливі для функціонування державного апарату дані (як-от державна таємниця та ін.).

Уже в п. 1 Постанови КМУ № 856 від 18.09.2019 р. Питання Міністерства цифрової трансформації [146] можна знайти концептуальний підхід до формування стратегії залучення Мінцифри до створення засад інформаційної безпеки держави, адже тут національний законодавець згадує про дві інтенційні напрями діяльності органу, пристосовних до даного сегменту – розвиток інформаційного суспільства та національних електронних інформаційних ресурсів. На наше переконання, це є прикладом та фактором чіткого декларування напрямку розвитку державного апарату в контексті інтероперабельності інформаційно-безпекової політики та необхідності формування її гнучкості як з точки зору та позиції органів державної влади та місцевого самоврядування, так і інформаційного суспільства.

Також звертаємо увагу на положення пп. 9-7 п. 4 Постанови КМУ № 856 від 18.09.2019 р. Питання Міністерства цифрової трансформації [146]. Тут сформовано парадигму участі Мінцифри в процесах та процедурах взаємодії органів державної влади (органів публічної влади). Така діяльність, зокрема, стосується ведення інформаційної взаємодії між зазначеними суб'єктами, а

також – функціонування електронних реєстрів публічної формації. Метою та призначенням такого концептуального підходу, на наше переконання, є детінізація діяльності органів державної влади та органів місцевого самоврядування, а також – формування захищеності інформації зазначених інституцій, що кореспондує із національними інтересами та, зокрема, фактором національної (державної) безпеки.

Потрібно також звернути увагу на наявність у діяльності Мінцифри декількох складових реалізації повноважень щодо інформаційно-безпекової координації. Першим з них є культивація політики та культури інформаційної безпеки в Україні на державному та суспільно-громадянському рівні, другим – безпосередня реалізація стандартів інформаційної політики та інформаційно-безпекової політики на практичному рівні, за допомогою формування архітектури схоронності, захищеності критичних даних та чутливої інформації, а також даних, що становлять державну таємницю.

Відтак, взаємозв'язок між повноваженнями та діяльністю Мінцифри, а також Службою безпеки України (СБУ) та Радою національної безпеки та оборони України (РНБО) доцільно виводити за тривимірною архітектурною моделлю.

Першим кластером зазначеного співвідношення, на наш погляд, доцільно визнати кореляційний зв'язок між власне повноваженнями Служби безпеки України (СБУ) в контексті масштабного моніторингу інформаційно-безпекового поля в Україні та, зокрема, повноваження Мінцифри щодо сприяння у проведенні такого моніторингу. Наприклад, видається затребуваною та застосовною опція документування та детекції правопорушень у сфері інформаційної безпеки органами державної влади та органами місцевого самоврядування Мінцифру (враховуючи абсолютне право останньої на організаційне впорядкування державних реєстрів відповідно до пп. 9-7 п. 4 Постанови КМУ № 856 від 18.09.2019 р. Питання Міністерства цифрової трансформації [146], котра підсумково підлягає комплексному доповненню

згідно із повноваженнями Служби безпеки України (СБУ) щодо беззастережного контролю за виконанням приписів відносно уніфікованого формування безпечного та обороноздатного інформаційного простору.

Другим кластером співвідношення, на котрому ми акцентували увагу вище, є уніфікований статус Ради національної безпеки та оборони України (РНБО) щодо формування безпекового національного простору в усіх сферах, зокрема, і у галузі національної інформаційної безпеки. За таких умов, взаємодія зі Службою безпеки України (СБУ) виступає додатковим доповняльним елементом архітектурування простору національної інформаційної безпеки, а діяльність Мінцифри фактично уніфікує можливість впровадження концепцій інформаційної безпеки за допомогою інформаційно-комунікаційних технологій (ІКТ) та ін.

Третім, і заключним, елементом кореляційної взаємодії формату «Служба безпеки України (СБУ), Рада національної безпеки та оборони України (РНБО) та Міністерство цифрової трансформації України (Мінцифра)» функціонування усіх трьох вищезазначених інституцій безпосередньо в інтересах інформаційної безпеки України та, як наслідок, національної безпеки України в генеральному розумінні даного терміну. Вищезазначений аналіз підводить до висновку, що діяльність зазначених органів є механізмом забезпечення інформаційної безпеки України, внаслідок чого зазначені органи публічної влади можуть бути визнані системою суб'єктів, відповідальних за національну інформаційно-безпекову політику.

Радше факультативного значення у контексті огляду суб'єктного складу забезпечення інформаційної безпеки України, водночас, набуває аналіз Національної поліції України (Нацполіції). Зазначимо водночас, що даний орган та його діяльність у контексті формування архітектури інформаційно-безпекового середовища сутнісно доповнюють взаємозв'язок формату «Служба безпеки України (СБУ), Рада національної безпеки та оборони України (РНБО) та Міністерство цифрової трансформації України (Мінцифра)».

Керівним нормативно-правовим актом, котрим визначаються особливості реалізації практичних категорій інформаційної безпеки Національною поліцією України (Нацполіцією) на практиці, є Закон України «Про Національну поліцію України» № 580-VIII [50]. Опосередкований вплив діяльності Національної поліції України (Нацполіції) на реалізаційне забезпечення заходів публічного управління та адміністрування інформаційно-безпекового характеру наявний у ст. 28 Розділу IV зазначеного вище нормативно-правового акту, де національний законодавець відмічає участь Нацполіції у притягненні до відповідальності винних за порушення використання інформаційних ресурсів у випадках, коли це, зокрема, мало наслідком порушення прав, свобод, інтересів людини та ін. Доцільно зауважити, що для цілей даної статті порушення використання інформаційних ресурсів, згідно із диспозицією, полягає у несанкціонованому використанні інформаційних систем, інформаційних ресурсів та інформаційно-комунікаційних систем (ІКТ) водночас. З огляду на вищезазначене, можемо зробити висновок щодо фрагментарності, проте концептуальності ролі Нацполіції у забезпеченні інформаційної безпеки України на рівні притягнення до відповідальності за порушення, що прямим або опосередкованим чином можуть чинити негативний вплив на внутрішнє інформаційне середовище та, відповідно, в підсумку зчинити негативний вплив на інформаційно-безпекову обороноздатність країни на міжнародній арені та у міжнародних відносинах із іншими державами.

На підставі досліджених особливостей ролі та місця Служби безпеки України (СБУ), Ради національної безпеки та оборони України (РНБО), Міністерства цифрової трансформації України (Мінцифри) та Національної поліції України (Нацполіції) у системі забезпечення інформаційної безпеки, можемо сформувати декілька проміжних концептуальних висновків.

Служба безпеки України (СБУ), Рада національної безпеки і оборони України (РНБО), Міністерство цифрової трансформації України (Мінцифри) та Національна поліція України (Нацполіція) є ключовими елементами державної

системи забезпечення інформаційної безпеки, кожен із яких виконує важливу і специфічну роль у цьому процесі. СБУ виступає основним суб'єктом, відповідальним за протидію кіберзагрозам, захист державних інформаційних ресурсів і виявлення деструктивної діяльності у сфері інформації, а також координує заходи з боротьби з дезінформацією та пропагандою. РНБО забезпечує стратегічне планування, формує політику національної безпеки, включно з інформаційною сферою, та координує роботу всіх суб'єктів, задіяних у забезпеченні інформаційної безпеки.

Мінцифра, у свою чергу, є провідним органом, який розвиває інфраструктуру цифрової безпеки, впроваджує сучасні технології захисту даних, забезпечує розвиток кіберграмотності та реалізує державну політику у сфері цифровізації. Національна поліція зосереджена на розслідуванні правопорушень у сфері інформаційної безпеки, зокрема злочинів, пов'язаних із кібератаками, шахрайством та несанкціонованим доступом до інформаційних систем.

Таким чином, діяльність цих органів є взаємодоповнюючою та спрямованою на створення цілісної системи протидії сучасним загрозам в інформаційному просторі України. Координація їх зусиль забезпечує надійний захист національних інтересів у цифровій епосі та зміцнює безпеку держави в умовах гібридних загроз.

На рисунку 1.2 представлено інтегративну модель механізмів реалізації інформаційної безпеки у системі публічного управління України із урахуванням усіх вищеперелічених органів та їхньої ролі у забезпечення національної стійкості

Окрім діяльності органів, компетенція котрих у аспекті забезпечення інформаційної безпеки України полягає у спрямуванні та координації власне державно-управлінського механізму зазначеного процесу, надалі доцільно сконцентруватися на окресленні «соціального» наративу реалізації інформаційно-безпекової моделі крізь призму діяльності Міністерства культури

та стратегічних комунікацій України (Мінкульту).

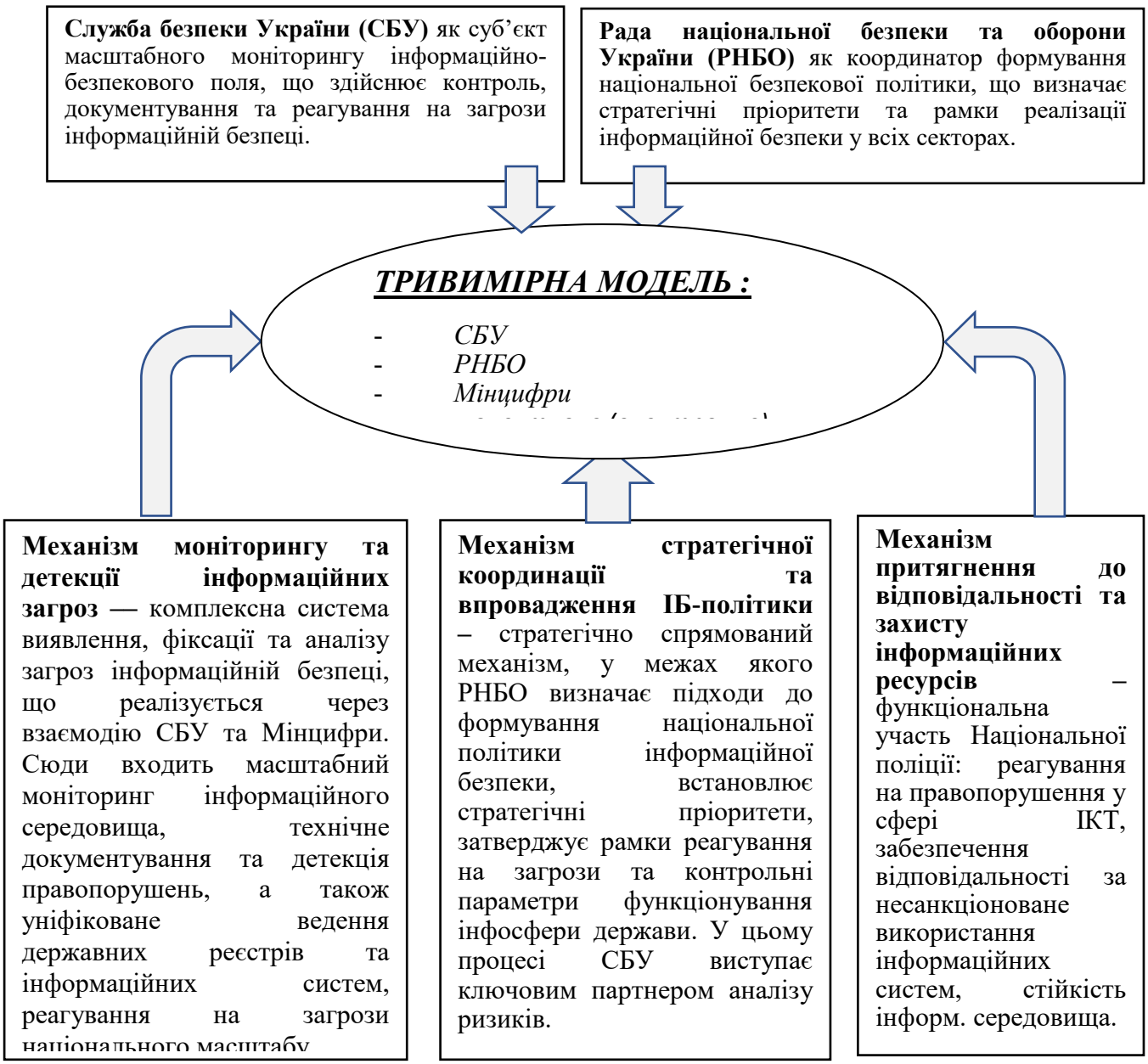

Рисунок 1.2. Інтегративна модель механізмів реалізації інформаційної безпеки у системі публічного управління України

Юридична (нормативно-правова) складова діяльності Міністерства культури та стратегічних комунікацій України (Мінкульту) розглянута та конкретизована національним законодавцем у Постанові КМУ № 885 від

16.10.2019 р. Деякі питання діяльності Міністерства культури та стратегічних комунікацій [147].

Так, у абз. 3 пп. 1 п. 3 Постанови КМУ № 885 від 16.10.2019 р. Деякі питання діяльності Міністерства культури та стратегічних комунікацій [147] до основних цілей, завдань та функцій Мінкульту віднесено культивацію інформаційної політики України та, зокрема, інформаційної безпеки України як її складника.

Також, відповідно до пп. 5 п. 4 Постанови КМУ № 885 від 16.10.2019 р. Деякі питання діяльності Міністерства культури та стратегічних комунікацій [147], до прямих повноважень Мінкульту належить нормативно-правове регулювання у сфері інформаційної політики України. При цьому, у пп. 8 п. 4 Постанови КМУ № 885 від 16.10.2019 р. Деякі питання діяльності Міністерства культури та стратегічних комунікацій [147] національний законодавець відносить до кола компетенції Мінкульту пріоритезацію та перспективне рамкування інформаційно-безпекової галузі України, а пп. 131 п. 4 даного нормативного акту встановлює презумпцію методико-практичної допомоги Мінкульту в галузі архітектування інформаційної безпеки.

Кореляційний зв’язок між інформаційною безпекою та національною безпекою як взаємопов’язаними складниками державного управління, водночас, систематизований у пп. 154 п. 4 Постанови КМУ № 885 від 16.10.2019 р. Деякі питання діяльності Міністерства культури та стратегічних комунікацій [147], де інформаційно-культурні інтереси України віднесені національним законодавцем до структури зміцнення національно-безпекового державного профілю.

На підставі вищезазначеного, можемо зробити висновок про соціальну роль Міністерства культури та стратегічних комунікацій як повноправного суб’єкта забезпечення інформаційної безпеки України в умовах сьогодення. Так, Мінкульт виконує не лише регуляторну, а й стратегічну місію, забезпечуючи гармонійне поєднання культурних, інформаційних та безпекових

інтересів України, що сприяє консолідації суспільства та зміцненню національної ідентичності пропорційно сучасним викликам.

Водночас, сукупність загальнодосліджених особливостей та закономірностей системи суб'єктів забезпечення інформаційної безпеки України дозволяє говорити про те, що СБУ, РНБО, Мінцифру, Нацполіцію та Мінкульт взаємодіють у межах своїх повноважень та нормативних приписів національного законодавста. Так, СБУ координує протидію інформаційним і кіберзагрозам, РНБО визначає стратегічні пріоритети та координує державну політику, Мінцифра впроваджує цифрові технології захисту, Нацполіція розслідує злочини у сфері інформаційної безпеки, а Мінкульт забезпечує культурно-інформаційну стійкість та нормативно-правове регулювання. Їх спільна діяльність створює комплексний підхід до захисту інформаційного простору України.

Висновки до розділу 1

1. Обґрунтовано та розроблено інтегративну модель механізмів реалізації інформаційної безпеки у системі публічного управління України, яка, на відміну від існуючих, ґрунтується на міжсекторальному та комунікаційно-стратегічному підходах та включає: удосконалену інституційно-правову конструкцію ключових суб'єктів забезпечення інформаційної стійкості (РНБО, Центр протидії дезінформації; Міністерство культури); критерії функціональної діагностики управлінських обмежень в умовах воєнного стану; комплексну концепцію стратегічного управління інформаційною безпекою, що забезпечує синергію між захистом критичної інфраструктури та підтримкою інформаційної гігієни громадянського суспільства.

2. Поглиблено теоретико-методологічні засади дослідження інформаційної безпеки у системі публічного управління шляхом системного аналізу її подвійної природи та авторського структурування її ключових

елементів: інформаційна безпека як система суспільних відносин: Здійснено комплексне розмежування та структурування її елементів (суб’єкти: держава, громадянське суспільство, бізнес; об’єкт: інформаційне середовище; регулювання; інститути; цілі), а також ідентифіковано її ключові особливості (суб’єктна взаємозалежність, громадянська участь, інформаційна грамотність, етика та відповідальність), що дозволяє перейти від статичного опису до динамічного управління процесами; інформаційна безпека як об'єкт правової охорони: Проаналізовано та систематизовано вітчизняні та зарубіжні наукові парадигми (кримінально-правова, цифрова, адміністративно-правова) та запропоновано науково-обґрунтовані рекомендації щодо її ефективної правової охорони, які включають необхідність законодавчого ототожнення термінів «інформаційна безпека держави» та «інформаційна безпека громадянина» як де-факто об’єктів правової охорони.

3. Удосконалено підходи до інституційного механізму забезпечення інформаційної безпеки в системі публічного управління шляхом: розробки та обґрунтування мультифункціональної архітектурної моделі взаємодії ключових суб’єктів — Служби безпеки України (СБУ), Ради національної безпеки та оборони України (РНБО) та Міністерства цифрової трансформації України (Мінцифри) — виведеної за тривимірним кластерним співвідношенням (моніторинг-координація-впровадження), що дозволяє перейти від лінійного переліку функцій до системного розуміння механізму забезпечення національної інформаційної стійкості; концептуалізації соціальної ролі Міністерства культури та стратегічних комунікацій України (Мінкульт) як повноправного суб’єкта забезпечення інформаційної безпеки, який виконує стратегічну місію із забезпечення культурно-інформаційної стійкості та нормативно-правового регулювання інформаційної політики, доповнюючи техніко-правовий та правоохоронний сегменти (СБУ, Нацполіція)

).

РОЗДІЛ 2
МЕТОДОЛОГІЧНІ ЗАСАДИ МЕХАНІЗМІВ РЕАЛІЗАЦІЇ ІНФОРМАЦІЙНОЇ БЕЗПЕКИ У СИСТЕМІ ПУБЛІЧНОГО УПРАВЛІННЯ

2.1. Концептуальні засади дослідження інформаційної безпеки у системі публічного управління

Інформаційна безпека на сучасному етапі, в умовах інтернаціональної мінливості, нестабільності та подекуди – слабкої адаптивності міжнародної політики є чутливим та вразливим аспектом державно-управлінського апарату управління. Виходячи з цього, комплексне та конкретизоване дослідження методології, за допомогою якої здійснюватиметься аналіз даного феномену, набуває додаткового рівня затребуваності та актуальності.

Актуальність та значення методології у дослідженні інформаційної безпеки найпершим чином варто розкривати крізь призму наявності сучасних викликів – глобалізації, цифровізації, підвищення рівня згубності та ефективності кібератак та появи інваріацій кіберзагроз, котрі виступають чинником дестабілізації локально-управлінської та міжнародної державно-управлінської парадигми в умовах сьогодення.

Більш сегментовано аналізуючи питання загроз інформаційній безпеці в сучасних умовах, вітчизняний учений Т. Ткачук [169, с. 184] зазначив, що, окрім їхнього власне технічного прояву (DDoS-атаки, злами, віруси, шкідливе ПЗ та інші, похідні порушення інформаційного суверенітету держави), останні мають також соціально-психологічний та політико-економічний прояви. Соціально-психологічний виявляється у маніпулюванні громадською думкою та дестабілізації ситуації всередині країни за допомогою інформаційного оснащення ззовні, тоді як політико-економічний складник передбачає

здійснення заходів кібершпигунства та кібертерору, призначенням котрих є систематизація даних про державу та її «чутливі» дані для подальших дій проти інформаційно-безпекового середовища останньої та внесення хаосу у діяльність державних інституцій [169, с. 184].

Проаналізовані вище підходи до розуміння проблеми загроз інформаційній безпеці в сучасних умовах дозволяють зробити висновок про її прямий вплив на політико-соціальну об'єктивну дійсність держави. Із урахуванням факту впливу загроз інформаційній безпеці на національну (фінансова, транспортна, енергетична сфери), міжнародну (кібершпигунство та загрози глобальній економіці) та соціальну (незахищеність персональних даних громадян та ризик понесення збитків через кібеаратаки або негативна опція стати жертвою шахрайства) парадигми стабільності, дослідження інформаційної безпеки потребує чітких методологічних засад, заснованих на категоріях системності, міждисциплінарності та комплексного аналізу.

Системність як методологічна складова процесу дослідження інформаційної безпеки являє собою кластер комплексного аналізу зазначеного феномену у його багатовимірному форматі. Як зазначається у дослідженні іноземного вченого К. М. Паананена [267, с. 21-22], саме системна складова дослідницької діяльності може дозволити ефективним способом проаналізувати характерні особливості технічного, соціального, правового та організаційного спектрів ототожнення останньої з позиції наявних проблем та протиріч у науковому полі розуміння. У тому-таки дослідження науковець відзначає, що за допомогою системного підходу інформаційна безпека може бути проаналізована як впорядкована структура сталих елементів (суб'єктів, об'єктів, загроз та механізмів захисту), що сукупно формують сталу модель підтримки сталості у інформаційній галузі [267, с. 22].

Можемо погодитися із запропонованим нижче підходом до розуміння системності як методологічної складової процесу дослідження інформаційної безпеки, проте, на наш погляд, до цілей та особливостей даної кластерної

категорії доцільно додати аналіз взаємного доповнення між вищепроаналізованими елементами (суб'єкти, об'єкти, загрози та механізми захисту) та прогностично-моделювальне застосування імовірного (гіпотетичного) розвитку ситуації у локальному та міжнародному інформаційно-безпековому середовищі.

В свою чергу, міждисциплінарність у якості методологічної складової процесу дослідження інформаційної безпеки являє собою інтегрованих підхід до залучення знань із різних галузей з метою комплексності, повноцінності, безсторонності та всебічності аналізу зазначеного феномену. Предметом застосування міждисциплінарної методології дослідження інформаційної безпеки є першочергово аналіз інформації як активу державно-управлінської, політичної та юридичної дійсності [267, с. 135].

Необхідно зауважити, що необхідність застосування міждисциплінарного підходу детермінована потребою в урахуванні складності проблеми забезпечення інформаційної безпеки (технічні, правові аспекти та вплив на суспільну думку), динамізмі появи кіберзагроз (глобальність кіберзагроз та поширення ролі штучного інтелекту в аспектах дестабілізації інформаційно-безпекових ситуацій), а також – урахуванні явища глобалізації (контекст міжнародного досвіду, юридичних стандартів та норм щодо нівелювання гіпотетичного негативного впливу останньої на формування інформаційно-безпекової локальної та міжнародної карти сьогодення).

До сфер знань, що можуть бути інтегровані до процесу вивчення та аналізу інформаційної безпеки як дефініції, явища та феномену водночас, доцільно віднести технічну, правову, соціальну, економічну, міжнародну та психологічну концептуальні складові[267, с 144-146].

Технічна сфера знань у контексті застосування міждисциплінарного підходу до розуміння та дослідження інформаційної безпеки має на меті акцентуацію на розробці кібербезпекових застосунків та технологій зберігання та збереження інформації на засадах використання мережевих систем

(програмного забезпечення) [267, с.144].

Правова сфера знань у аспекті використання міждисциплінарного підходу до розуміння та дослідження інформаційної безпеки покликана аналізувати міжнародне та локально-правове розуміння кібербезпеки як явища об'єктивної дійсності, висувати пропозиції щодо теоретичного усунення негативних проявів інформаційної узурпації на рівні держав та кіберзлочинності на рівні міжнародного права, де інформаційна безпека розглядається як частина суверенітету держави [267, с. 144-145].

Соціальна сфера знань та соціальні науки у контексті використання міждисциплінарного підходу в аналізі інформаційної безпеки, в свою чергу, полягає у аналізі та вивченні громадської думки щодо інформаційної безпеки, а також – поведінки користувачів у цифровому середовищі [267, с 145.].

Економічні знання у контексті використання міждисциплінарного підходу під час дослідження інформаційної безпеки, водночас, створюють плацдарм для розуміння зв'язків інформаційної безпеки із економічної стабільністю та, в той же час, для розуміння характеру та розміру збитковості від кібератак в цифрову епоху [267, с 145.].

Напрацювання та теоретичні розробки у розрізі міжнародних відносин та міжнародного права в розрізі дослідження особливостей інформаційної безпеки дозволяють виокремити, розробити та концептуалізувати роль безпеки інформації (даних) у контексті глобально-політичного кластеру та можливості (опції) коригування негативного впливу кібератак та попередження кіберзагроз [267, с.145-146].

Дослідження у галузі психології можуть бути застосовані для вивчення підходів щодо дезінформації користувачів в епоху глобалізації, цифровізації та інформатизації, а також пошуку інструментів формування кіберграмотності на даній основі [267, с 146.].

Комплексність аналізу як одна з вихідних методологічних парадигм дослідження інформаційної безпеки є узагальненою категорією, що певним

чином логічно та ідеологічно продовжує концепцію мультинаукового підходу до розуміння даного феномену. На переконання українського авторського колективу на чолі з Г. Ситником [160, с. 4], інформація як об'єкт та предмет аналізу (дослідження) у контексті науки державного управління концентрується, систематизується на концептуалізується на взаємозалежності системного, міждисциплінарного та власне комплексно-аналітичного підходів. Сукупно останні означають, що аналіз та синтез інформації (даних), пов'язаних із феномен інформаційної безпеки, з метою його об'єктивності, логічності, критичності та всебічності дослідження зазначеної категорії дискурсно-наукового інтересу повинен досліджуватися не лише в межах науки державного управління, але й із залучення суміжних полей наукового інтересу та наукової періодики задля встановлення ролі та місця останньої не лише у теоретичному, але й соціально-політичному, політико-економічному, політико-інформаційному, політико-інфраструктурному та ін. форматах життя держави [160, с. 5].

Аналіз вихідних методологічних засад дослідження інформаційної безпеки в контексті даного дисертаційного дослідження потребує не лише узагальнення, але й використання методології концентрації на тематиці даної праці, що передбачає акцент на теоретико-методологічних засадах забезпечення інформаційної безпеки в умовах глобалізації, аналізі структури механізму правового забезпечення інформаційної безпеки в Україні, міжнародних норм та практик забезпечення інформаційної безпеки, сучасних загроз інформаційній безпеці України та, водночас, формуванні стратегії реалізації механізму протидії зовнішнім і внутрішнім інформаційним впливам у сучасних умовах.

Методологічну основу проведеного дослідження становить сукупність взаємопов'язаних загальнонаукових і спеціалізованих підходів, серед яких застосовано системний, історико-ретроспективний, компаративний, структурно-функціональний методи, а також методи аналізу й синтезу, узагальнення та класифікації, індуктивного й дедуктивного мислення,

принципи взаємозв’язку частини та цілого, проблемного і прогностичного аналізу. Застосування історико-ретроспективного методу дало змогу здійснити концептуалізацію термінологічного та категоріального апарату поняття «інформаційна безпека» в межах системи національної безпеки [параграф 1.1]. У свою чергу, через узагальнення й систематизацію вітчизняних наукових джерел було проаналізовано інформаційну безпеку як багатовимірну систему суспільних відносин і водночас — як об’єкт правової охорони [параграф 1.2], а також виокремлено ключові методологічні орієнтири для подальшого дослідження даного феномену [параграф 1.3].

Системний та структурно-функціональний підходи надали можливість розкрити сутність та принципи побудови механізму правового регулювання забезпечення інформаційної безпеки, концептуалізувавши нормативні особливості такого процесу та систему суб’єктів забезпечення інформаційної безпеки [параграф 2.1; параграф 2.2; параграф 2.3]. Використання емпіричних методів, індукції й дедукції забезпечило розкриття сутності, мети та особливостей стратегічного управління забезпеченням інформаційної безпеки [параграф 3.1]. Завдяки проблемному й прогностичному підходам проаналізовано глобальний характер інформаційної безпеки крізь призму інституційних можливостей та ризиків, а також комунікаційну стратегію як складову національного управління інформаційною безпекою [параграф 3.2; параграф 3.3] та, на додаток, класифіковано загрози інформаційній безпеці України і систематизовано методичні підходи протидії загрозам інформаційній безпеці України [параграф 4.1; параграф 4.2].

Задля реалізації зазначеної мети, котру ми визначили вище, у контексті розуміння та опрацювання власне вихідних методологічних засадах дослідження інформаційної безпеки пропорційно встановленим завданням дисертації, водночас, доцільно зосередити власну увагу на принципах, філософських та правових основах дослідження безпеки інформації. Специфіку аналізу деяких із даних кластерів означимо нижче більш детально.

Принципами дослідження інформаційної безпеки як сталої категоріальної теоретичної, державно-управлінської та соціально-дійснісної величини, котрі застосовуються у даній праці, доцільно називати комплексність, прогнозованість та глобальність.

Комплексність як концепція-принцип дослідження інформаційної безпеки походить власне від системності, міждисциплінарності та комплексності аналізу як методологічних засад аналізу інформаційно-безпекового простору. До прикладу, у праці М. Гончарова [25, с. 35] зазначається, що виключно «комплексне дослідження інформаційної безпеки, засноване на визначенні її місця у політичному житті держави, суспільних відносинах державного управління та специфіці правової охорони» здатне виступити об'єктивним та дієвим джерелом наукового осмислення зазначеного феномену. Виходячи із наших попередніх напрацювань, розуміння інформаційної безпеки у комплексній парадигмі також передбачає урахування таких її складників, як зв'язок із технікою та технологіями, а також – окреслення впливу останніх на розвиток інформаційно-безпекової карти сьогодення та, водночас, негативного прояву цифрового прогресу у контексті порушення інформаційного суверенітету держав.

Комплексне дослідження інформаційної безпеки, на наш погляд, у контексті нашого дисертаційного дослідження також знаходитиме свій прояв у кореляції між загальними підходами до розуміння феномену інформаційної безпеки у теорії та доктрині, міжнародними концепціями забезпечення інформаційної безпеки та дослідженням особливостей забезпечення і проблематики інформаційної безпеки в Україні в період державотворчого руху та євроінтеграційного поступу.

Прогнозованість у якості принципу дослідження інформаційної безпеки, в свою чергу, має на меті орієнтацію на майбутні виклики та загрози у інформаційно-безпековому полі. На основі наявної проблематики у галузі інформаційної безпеки (кіберзагрози, кібератаки, порушення безпеки даних

користувачів та незахищеність персональних даних (інформації), дезінформація як джерело гібридного політико-соціального та політико-мілітарного впливу тощо) та пропозицій, котрі будуть застосовані у даній праці, вбачаємо за доцільне розробити індивідуальні підходи до нівелювання наявних протиріч та інформаційно-безпекових неузгодженостей, котрі в подальшому можуть бути апропріативно застосовані на практиці. У даному дисертаційному дослідженні зазначеному завданню присвячено Розділ V, де буде розглянуто стратегію реалізації механізму протидії зовнішнім і внутрішнім інформаційним впливам у сучасних умовах.

Контекст глобальності як елемент-принцип дослідження інформаційної безпеки опосередковується із урахування міжнародних підходів, стандартів, тенденцій управління, спрямування та координації інформаційно-безпекового простору. Як відмічає В. Шемчук у власній монографічній праці «Забезпечення інформаційної безпеки як функція сучасних держав : порівняльно-правовий аналіз» [197, с. 73-75], усвідомлення глобального правопорядку та безпеки у міжнародних відносинах, локального забезпечення безпеки країни, громадян, населення та критичних аспектів функціонування апарату управління створюють прецедент повноцінного, комплексного та галузевого підходу до дослідження інформаційної безпеки та таких її особливостей, як багатовимірність, залежність від цифрових інструментів та соціальний характер.

Водночас, на наше суб’єктивне переконання, глобальність як принцип дослідження інформаційної безпеки у контексті тематики та архітектури даної дисертаційної праці може розкриватися через потенційну рецепцію підходів до спрямування та координації інформаційної безпеки на міжнародному та теоретичному рівні в національно-правове та національно-інституційне поле в Україні.

Маємо зауважити, що до вихідних методологічних основ аналізу інформаційно-безпекового простору доцільно відносити не лише власне

наукові різногалузеві підходи, але й філософський складник осмислення інформаційної безпеки – т.зв. «філософію інформаційної безпеки», адже остання встановлює причинно-наслідкові зв'язки між елементами інформаційно-безпекового середовища не на рівні статики, а на рівні практичної тотожності.

Так, філософія інформаційної безпеки насамперед визначає останню з позиції її наданням інформації статусу ресурсу, а також – із конкретизацією ціннісної парадигми інформації (даних) у сучасному суспільстві. Щодо розкриття даного методологічного підходу, нам імпонує наукова позиція К. Захаренка [56, с. 47-48], що пропонує ввести у дослідницьку модель інформаційної безпеки термін «філософія інформації», що розкривається за цивілізаційним визначником суспільного розвитку та технічного прогресу, де місце інформації має статус активу, котрий, водночас, формує нові виклики перед суспільством та світовою спільнотою – адже надлишок і надмірність даних та фактів може стати «джерелом хаосу».

Також, у контексті розуміння концептуальної моделі філософії інформаційної безпеки у розрізі її застосування як методологічного складника її аналізу, доцільно означити кластер діалектичного співставлення за її допомогою категорій «безпека» та «свобода». Інноваційне наукове моделювання даного співвідношення в даному випадку запропонував американський дослідник Г. Г. Фостер [241, с. 333-334], на думку котрого «інформаційна безпека є проявом свободи, адже включає в себе можливість індивіда вільно та на власний розсуд споживати дані із різних джерел, власноручно аналізуючи їх на предмет доцільності, компетентності та застосовності». Можна стверджувати, що вищенаведений підхід відсилає до права людини та громадянина на інформацію, котре є абсолютним, не підлягає обмеженню та, водночас, є конституційно гарантованим проявом демократичної, людиноцентриської державної політики. Відповідно, застосування такої концептуальної підмоделі загальної моделі «філософія

інформаційної безпеки» у даному дисертаційному дослідженні може розглядатися як затребуване.

Правові основи дослідження безпеки інформації, в свою чергу, у контексті вихідних методологічних основ інформаційної безпеки, за допомогою яких може бути проведено аналіз пропорційно тематиці дисертаційної роботи, полягають у опрацюванні законодавства України у сфері інформаційної безпеки та окресленні основних положень міжнародних стандартів, дотичних до галузі інформаційно-правового забезпечення (Будапештська конвенція про кіберзлочинність, General Data Protection Regulation (GDPR), ISO/IEC 27001 та ін.).

Аналіз юридичної складової забезпечення інформаційної безпеки, водночас, повинен бути здійснений у пристосуванні до інституційної складової реалізації даної кластерної категорії. Таким чином, дослідженню та аналізу підлягають особливості діяльності Єврокомісії, Європарламенту (ЄС) у контексті інформаційно-безпекового забезпечення, а також діяльності Міжнародної організації стандартизації та Міжнародної електротехнічної комісії (органів, що брали безпосередню участь у розробці міжнародного стандарту інформаційної безпеки ISO/IEC 27001).

На підставі зазначених опрацьованих особливостей вихідних методологічних засад дослідження інформаційної безпеки можемо сформувати наступні умовиводи.

Так, дослідження інформаційної безпеки є складною міждисциплінарною проблемою, яка потребує інтеграції знань з технічних, правових, соціальних, економічних і філософських сфер. Вихідні методологічні засади формують основу для комплексного аналізу та розробки ефективних рішень у цій галузі.

Методи дослідження інформаційної безпеки мають базуватися на поєднанні аналізу й синтезу, моделювання загроз, системного підходу та порівняльного аналізу міжнародного досвіду. Важливим є також інтеграція прогнозування та аналізу ризиків із врахуванням соціальних і технологічних

змін.

Таким чином, вихідні методологічні засади дослідження інформаційної безпеки ґрунтуються на системності, міждисциплінарності, етичному підході та адаптивності до динамічних змін сучасного світу, а їхнє застосування дозволяє формувати комплексні та ефективні стратегії для забезпечення безпеки інформації, що є критично важливим для сталого розвитку суспільства у цифрову епоху.

2.2. Принципи реалізації механізмів інформаційної безпеки у системі публічного управління

Перш ніж переходити до тематичного осмислення особливостей механізму правового регулювання забезпечення інформаційної безпеки безпосередньо в Україні, пропонуємо надати теоретичне розуміння явищу «механізм правового регулювання забезпечення інформаційної безпеки».

У праці «Інформаційна безпека : принципи та практики» британські вчені М. М. Мерков та Дж. Брітгаупт [266, с. 223] зауважили, що під механізмом правового регулювання забезпечення інформаційної безпеки доцільно називати систему правових, нормативних та інституційних засобів, за допомогою яких формується захисна парадигма інформаційного середовища, що включає захист державних органів, суспільства та окремих осіб від загроз, пов’язаних із обробкою, зберіганням, передачею та використанням інформації.

Узагальнено, на переконання дослідників, механізм правового регулювання забезпечення інформаційної безпеки являє собою впорядковану взаємодію органів законодавчої, виконавчої та судової влади, що може підлягати контролю та нагляду від громадянського суспільства в рамках демократично-правової побудови державності. Метою функціонування механізму правового регулювання забезпечення інформаційної безпеки як сталої публічно-управлінської категорії у дослідженні визначено безпечне

інформаційно-інфраструктурне національне поле [266, с. 225].

Натомість, у рамках вітчизняного дослідницького поля механізм правового регулювання забезпечення інформаційної безпеки розглядався радше не з теоретичного, а з теоретико-нормативного наукового спектру.

Корисним у даному контексті вбачаємо напрацювання Т. Перун [139, с. 119-120], у якому було розглянуто структурні чинники механізму інформаційної безпеки держави.

Визначаючи феноменологію трактування та наукового аналізу поняття «механізм правового регулювання забезпечення інформаційної безпеки», науковець запропонував розглядати останній як сукупність способів, засобів та механізмів, за допомогою яких відбувається забезпечення інформаційного суверенітету держави на нормативно-правовому рівні [139, с. 120]. Саме від нормативно-правового рівня врегулювання проблеми забезпечення механізм правового регулювання забезпечення інформаційної безпеки, на переконання вченого, залежить успішність, ефективність та послідовність забезпечення схоронності даних та інформації, в тому числі – державної та такої, що становить державну таємницю.

Розширюючи цю тезу, можна зауважити, що механізм правового регулювання інформаційної безпеки включає в себе як формальні, так і функціональні компоненти, які визначають чітку послідовність дій державних органів, відповідальних за безпеку інформаційного середовища. До формальних компонентів відносяться нормативні акти, закони, постанови та інструктивні документи, що закріплюють правила обробки, зберігання та поширення інформації на державному рівні. Функціональні компоненти, у свою чергу, визначають конкретні процеси контролю, аудиту, моніторингу і реагування на загрози, включно з оперативним втручанням у випадку виявлення інформаційних порушень.

Важливо підкреслити, що успішність механізму залежить не лише від наявності нормативної бази, а й від її практичного впровадження та адаптації

до швидко змінюваного інформаційного середовища. Іншими словами, ефективне регулювання інформаційної безпеки передбачає не стати формальним набором документів, а трансформуватися у динамічну систему, яка здатна передбачати, запобігати і оперативно реагувати на нові загрози, включно із технологічними, кібератаками та соціально-психологічними маніпуляціями.

Крім того, науковець наголошує на значенні інтеграції механізму правового регулювання із іншими підсистемами національної безпеки. Йдеться про тісну взаємодію з військовою, економічною, соціальною та кібернетичною інфраструктурою держави, що дозволяє створювати комплексну систему захисту інформації. Така інтеграція забезпечує одночасне дотримання балансу між суворим контролем за державними даними та необхідністю відкритості і прозорості у доступі до публічної інформації, що становить фундамент демократичного управління інформаційною сферою [139, с. 120].

Не менш важливою є роль людського фактору в реалізації механізму правового регулювання. Ефективність його функціонування значною мірою залежить від кваліфікації та підготовки кадрів, здатних не лише імплементувати нормативні вимоги, а й прогнозувати розвиток загроз та формувати превентивні стратегії. Тому сучасні підходи до управління інформаційною безпекою передбачають створення систем безперервного навчання, перепідготовки фахівців, а також залучення експертів з академічного і приватного секторів для підвищення адаптивності та стійкості механізму.

Таким чином, механізм правового регулювання забезпечення інформаційної безпеки виступає не лише як статична сукупність законів і правил, а як динамічна, багаторівнева система, що поєднує нормативне, організаційне, технологічне та кадрове забезпечення. Його ефективність визначає здатність держави забезпечити безпеку інформаційного середовища, запобігати кібератакам і дезінформації, а також підтримувати довіру громадян до державних інститутів, що є невід’ємним елементом загальної національної

безпеки.

Водночас, конкретизовані аналітичні погляди на проблему понятійно-категоріального апарату терміну «механізм правового регулювання забезпечення інформаційної безпеки» буде приведено нижче.

Наприклад, вітчизняна дослідниця В. Талімончик у дослідженні для іноземного видання під назвою «Правові аспекти міжнародної інформаційної безпеки» [281] зауважила, що механізми правового забезпечення інформаційної безпеки в Україні, на відміну від європейських держав та держав західної демократії, здебільшого будуються на нормативній реалізації даного процесу через нормативні акти. Це означає зменшення ролі, наприклад, соціально-політичних дискусій в питаннях побудови належної інформаційно-безпекової архітектури та зосереджує увагу насамперед на інституційно-юридичному захисті інформаційного простору. Такий підхід, хоча і є декларативним, страждає від статики застосування та нерідко не в змозі вирішити питання появи нових інформаційних загроз, як-от кібератаки та порушення інформаційного простору засобами дезінформації.

Окрім того, даний підхід має низку суттєвих наслідків. По-перше, він сприяє чіткому юридичному закріпленню ролей та обов’язків державних органів у сфері інформаційної безпеки, визначенню механізмів відповідальності за порушення та створенню формальної системи контролю. Це забезпечує стабільність і передбачуваність державного реагування на відомі загрози, що важливо для підтримання базового рівня інформаційного суверенітету. По-друге, зосередження уваги на нормативно-правовому регулюванні водночас обмежує інтеграцію ширших соціально-політичних та міжсекторальних ініціатив. Тобто питання формування колективної інформаційної культури, стимулювання проактивної поведінки громадян у сфері кібергігієни, взаємодії з приватним сектором та громадськими організаціями часто опиняються поза межами формального нормативного поля, що ускладнює реалізацію комплексної та адаптивної стратегії інформаційної безпеки.

Крім того, підкреслено, що такий механізм, хоча і формально захищає інформаційний простір, часто виявляється недостатньо ефективним у випадку появи нових та нетипових загроз, зокрема кібератак, технологічно складних шкідливих впливів, гібридних кампаній дезінформації або маніпуляцій із масовою свідомістю. Формальна нормативність не завжди здатна оперативно адаптуватися до динамічних змін у кіберпросторі, що робить систему уразливою перед швидко еволюційними загрозами.

Важливо також відзначити, що така структура інформаційно-безпекового механізму, орієнтована на декларативну нормативність, потребує додаткового розвитку інституційного, технологічного та кадрового потенціалу для забезпечення реальної ефективності. Це включає в себе створення оперативних підсистем моніторингу загроз, аналітичних центрів прогнозування інформаційних ризиків, а також інтеграцію новітніх технологій штучного інтелекту та систем автоматизованого аналізу даних у державні структури.

Таким чином, позиція В. Талімончик демонструє, що українська практика правового забезпечення інформаційної безпеки, незважаючи на формальну законодавчу системність, потребує глибшої інтеграції між нормативними, технологічними, громадськими та міжнародними компонентами для формування справді стійкого та адаптивного національного інформаційно-безпекового середовища [281]. Відповідно, тільки за умови поєднання жорсткого нормативного підґрунтя з динамічними управлінськими та інноваційними підходами держава може забезпечити комплексний захист інформаційного простору та підвищити стійкість суспільства до сучасних гібридних загроз.

В свою чергу, український авторський колектив на чолі зі М. Бондар та ін. [10] схиляється до думки, що механізм правового регулювання забезпечення інформаційної безпеки як стала конструкція повинна розумітися насамперед через сукупність елементів забезпечення останньої. До таких у даній праці віднесено нормативну, суб’єктну, правову та стратегічну бази, функціонування

котрих спрямовується Україною на рівні національної державної політики.

Функціонування зазначених баз у комплексі формує цілісну систему, де кожен елемент взаємопов'язаний із іншими, створюючи ефект синергії та забезпечуючи стійкість державного інформаційного середовища. Такий підхід передбачає, що державна політика в сфері інформаційної безпеки не обмежується формальними нормами чи ізольованими заходами, а реалізується через взаємодію всіх рівнів управління та структур, залучення громадянського суспільства, приватного сектору та міжнародних партнерів.

Надання пріоритету стратегічній базі дозволяє прогнозувати появу нових загроз, розробляти превентивні заходи та адаптувати національну політику до швидких технологічних і соціальних змін. У цьому контексті важливою є інтеграція аналітичних центрів і науково-дослідних інституцій, які здатні своєчасно оцінювати ризики, моделювати сценарії розвитку інформаційних загроз та пропонувати практичні рекомендації для державних органів.

Не менш важливим є включення у механізм інформаційної безпеки елементів комунікаційної стратегії, що забезпечує прозорість, довіру та координацію між державою, громадянами та міжнародними партнерами. Це дозволяє не лише ефективно протидіяти дезінформації та маніпуляціям, а й формувати активну громадянську позицію щодо захисту національної інформаційної безпеки.

Таким чином, механізм правового регулювання інформаційної безпеки, як його розглядає С. Бондаренко та колектив, виступає не лише нормативно-юридичною конструкцією, а й інтегрованою системою, де стратегічні, суб'єктні, правові та нормативні бази взаємодіють для створення ефективного, гнучкого та адаптивного інформаційно-безпечного середовища. Його функціонування забезпечує надійність, цілісність та ефективність захисту державного суверенітету в інформаційній сфері, одночасно створюючи передумови для безпечного та свідомого інформаційного середовища для громадян [10].

Особливу увагу слід приділити тому, що кожна складова механізму має як автономні, так і взаємозалежні функції. Наприклад, нормативна база не лише регламентує дії суб'єктів, але й визначає рамки використання стратегічної бази та межі правових інструментів у контексті інформаційної безпеки. Стратегічна база, у свою чергу, інтегрує результати діяльності суб'єктної та правової бази, забезпечуючи узгодженість і послідовність державної політики у довгостроковій перспективі.

Завдяки такому підходу механізм стає здатним оперативно реагувати на внутрішні та зовнішні загрози, підтримувати баланс між нормативною регламентацією та практичною реалізацією заходів, а також забезпечувати комплексний захист інформаційного простору держави. Важливим аспектом є також формування гнучких процедур моніторингу, контролю та оцінки ефективності застосування правових і стратегічних інструментів, що дозволяє своєчасно коригувати політику та впроваджувати інноваційні рішення у сфері інформаційної безпеки.

У підсумку, механізм правового регулювання забезпечення інформаційної безпеки держави, представленого у дослідженні, можна розглядати як багаторівневу, системну та динамічну конструкцію. Ключова цінність останнього полягає у здатності поєднувати нормативно-правову основу, суб'єктну активність, стратегічне планування та практичне управління у єдину інтегровану систему, що гарантує не лише формальну захищеність даних і інформаційного простору, а й реальну стійкість держави та її громадян у сучасних умовах глобальних інформаційних викликів.

Нормативна парадигма механізму правового регулювання забезпечення інформаційної безпеки, відповідно матеріалів даного дослідження, реалізується через такі акти законодавства, як Закон України «Про інформацію» № 2657-XII, Закон України «Про доступ до публічної інформації» № 2939-VI, Закон України «Про основні засади забезпечення кібербезпеки України» № 2163-VIII та ін. нормативно-правові акти.

Суб’єктна складова механізму правового регулювання забезпечення інформаційної безпеки, згідно матеріалів даного дослідження, в Україні забезпечується за допомогою діяльності таких органів, як Служба безпеки України (СБУ), Рада національної безпеки і оборони України (РНБО), Міністерство цифрової трансформації України (Мінцифра), Міністерство культури України (Мінкульт) та Національна поліція України (Нацполіція) [10].

Правова складова впливу на механізм нормативного регулювання забезпечення інформаційної безпеки в Україні, на переконання С. Бондаренко та ін. [10], підлягає впровадженню за допомогою : 1) розробки стандартів інформаційного захисту; 2) інформаційно-системної сертифікації; 3) санкційної діяльності відносно осіб, що порушують інформаційно-просторову стабільність та суверенітет держави ззовні (переважно – шляхом блокування Інтернет-доступу до таких ресурсів).

Стратегічний складник механізму правового регулювання забезпечення інформаційної безпеки України, відповідно матеріалів даного дослідження, реалізується на концептуалізується за допомогою інтеграції стратегічної інформаційно-безпекової документації – Указу Президента України «Про рішення Ради національної безпеки і оборони України від 14 травня 2021 року "Про Стратегію кібербезпеки України» № 447/2021 та Указу Президента України № 685/2021 «Про рішення Ради національної безпеки і оборони України від 15 жовтня 2021 року «Про Стратегію інформаційної безпеки» [174]. Конкретні особливості нормативно-правового забезпечення інформаційної безпеки у контексті державного управління та державного регулювання інформаційної безпеки в Україні, водночас, буде проведено у п. 2.2 Розділу ІІ даного дисертаційного дослідження.

У контексті розуміння понятійно-проблемного питання механізму правового регулювання забезпечення інформаційної безпеки як публічно-управлінської величини, що потребує уточненого та конкретизованого дефінціювання, пропонуємо також дослідити такий теоретичний конструкт, як

«призначення механізму правового регулювання забезпечення інформаційної безпеки» шляхом аналізу наукових підходів до його гіпотетичного трактування.

Раніше згаданий у контексті визначення характерних особливостей структурності механізму інформаційної безпеки держави український науковець Т. Перун [139, с. 121] пропонує ототожнювати призначення механізму правового регулювання забезпечення інформаційної безпеки крізь призму створення умов ефективного та взаємовигідного, юридичного рівного функціонування таких суб'єктів інформаційного простору, як держава, засоби масової інформації та громадяни (переважно у контексті розуміння громадянського суспільства). Сутнісний складник призначеннєвої функції механізму правового регулювання забезпечення інформаційної безпеки може визначатися, згідно позиції вищеназваного науковця, у форматі захисту своїх прав, інтересів та ресурсів від загроз за допомогою стабільного, безпекового та розвитково орієнтованого інформаційного простору в парадигмі слідування та респонденції глобалізації, цифровізації та ризиково-технологічним процесам у якості невід'ємних складових діджиталізаційного прогресу.

На наше переконання, сутність (призначення) функції механізму правового регулювання забезпечення інформаційної безпеки, зазначене та запропоноване у зазначеній дефініції, є концептуальним, проте може потребувати подальшого розширення. Наприклад, такі константи інформаційно-безпекового середовища, як регулювання інформаційної діяльності та розвиток інформаційного середовища можуть бути визнані якраз-таки частинами призначеннєвої парадигми розуміння функціонального наповнення інформаційно-безпекового юридичного спрямування.

Наукові позиції, контекстно пов'язані із запропонованими нами видозмінами у трактуванні питання призначення механізму правового регулювання забезпечення інформаційної безпеки, можна знайти, зокрема, у праці Н. Грабар «Механізми інформаційної безпеки України в умовах інформаційного глобалізму» [26, с. 170-171]. Розглядаючи зазначене питання на

стикові державно-управлінської та юридико-правової теорії, дослідниця пропонує розширювати концептуальне розуміння регулювання інформаційної діяльності, формуючи його модель не лише на рівні директивного управління інформаційними правами громадян шляхом нормотворення, але й на рівні обов'язку державних органів дотримуватися інформаційного та інформаційно-безпекового законодавства. Крім того, у її праці знаходимо пропозицію нового контексту механізму правового регулювання забезпечення інформаційної безпеки, котрий полягає у розвитковій інформаційній діяльності, що повинна торкатися середовища, де здійснюється обіг інформації, із його акцентом на інтеграцію інноваційних, цифрових нововведень з метою створення категорії «інформаційне суспільство».

У цьому контексті важливо відзначити, що запропонована Н. Грабар концептуалізація механізму правового регулювання інформаційної безпеки дозволяє вийти за межі традиційного нормативно-правового підходу та інтегрувати практичні аспекти державного управління із сучасними інформаційно-технологічними процесами [26, с. 170-171]. Такий підхід передбачає не лише фіксоване регулювання, а й активне прогнозування загроз та планування превентивних заходів у динамічному інформаційному середовищі, що включає як внутрішньодержавні, так і міжнародні аспекти взаємодії.

Важливим компонентом є врахування принципу відповідальності органів державної влади за дотримання стандартів інформаційної безпеки, який включає як формальні, так і процедурні інструменти контролю, моніторингу та оцінки ефективності виконання встановлених норм, що дозволяє створювати середовище, де інформаційна діяльність не тільки регламентована, а й підлягає постійному оцінюванню з точки зору її відповідності стратегічним цілям національної безпеки.

Розширення механізму за рахунок інтеграції цифрових інновацій і технологій є ключовим для формування інформаційного суспільства, яке

характеризується високим рівнем доступності, прозорості та ефективності інформаційного обміну. Впровадження таких елементів дозволяє державі адаптуватися до швидких змін у глобальному інформаційному середовищі, зменшувати ризики кібератак, інформаційних маніпуляцій та дезінформаційних кампаній, а також підвищувати довіру громадян до державних інституцій та процесів управління.

Крім того, механізм правового регулювання повинен передбачати комплексну взаємодію суб'єктів, залучених до забезпечення інформаційної безпеки, включаючи державні органи, громадські інституції, академічні центри та приватний сектор. Така інтеграція дозволяє формувати багаторівневу систему протидії загрозам, де кожен учасник має визначені функції та відповідальність, що сприяє оперативному реагуванню на інформаційні ризики та узгодженому впровадженню стратегічних рішень.

Завдяки комплексному підходу, запропонованому Н. Грабар, механізм правового регулювання забезпечення інформаційної безпеки набуває характеру живої системи, здатної до саморегуляції та адаптації до нових викликів [26, с. 170-171]. Це, у свою чергу, створює передумови для реалізації принципу безперервності захисту інформаційного простору та забезпечує сталу стійкість державного суверенітету в умовах глобалізації та цифрової трансформації суспільства.

Особливої уваги заслуговує концептуальне поєднання нормативного, стратегічного та інноваційного аспектів. На практиці це означає, що державна політика у сфері інформаційної безпеки повинна поєднувати створення чітких нормативних рамок із можливістю оперативного реагування на нові загрози, використанням сучасних цифрових технологій для прогнозування та моделювання ризиків, а також забезпеченням прозорості та відкритості інформаційних процесів для громадян.

Таким чином, підхід Н. Грабар дозволяє сформулювати механізм правового регулювання як цілісну, інтегровану і динамічну систему, яка здатна

не лише захищати інформаційний простір, а й стимулювати розвиток інформаційного суспільства, підвищувати ефективність державного управління та посилювати взаємодію між державою, суспільством і міжнародними партнерами [26, с. 170-171]. Ця модель стає не лише теоретичною основою, а й практичним орієнтиром для формування національної стратегії інформаційної безпеки, здатної враховувати сучасні виклики та динаміку глобального інформаційного середовища.

Проаналізований підхід до розуміння та наукового ототожнення кластерів «регулювання інформаційної діяльності» та «розвиток інформаційного середовища» як складових частин понятійної парадигми «призначення правового регулювання забезпечення інформаційної безпеки» дозволяють зробити декілька проміжних висновків.

По-перше, категорія «призначення правового регулювання забезпечення інформаційної безпеки» потребує подальшого розгляду у полі державного управління та юридичної науки одночасно. Таким чином відбуватиметься забезпечення балансу між реалізаційним (інституційна діяльність) та координаційним (нормативні категорії, що детермінують, зокрема, забезпечення моделей інформаційної безпеки інституціями у межах правового поля) впровадженням теорій середовища безпекового споживання інформації на практиці.

По-друге, механізм правового регулювання забезпечення інформаційної безпеки має і повинен мати демократичний, людиноцентристський характер, спрямований на забезпечення права людини на інформацію, що має конституційний підтекст генерації.

Надалі, якраз-таки, пропонуємо сконцентрувати власну увагу на особливостях доктринального трактування механізму правового регулювання забезпечення інформаційної безпеки крізь призму кореляції із правом людини і громадянина на інформацію, задекларованим у ст. 5 Закону України «Про інформацію» № 2657-XII.

Наперед зауважимо, що саме право людини і громадянина на інформацію, на наш погляд, детермінує можливість запровадження механізму правового регулювання забезпечення інформаційної безпеки у глобальній проєкції, адже першочерговим завданням держави є реалізація концепцій забезпечення безпеки громадян, включно із інваріаціями останньої, де безпека даних та інформації займає чільне місце.

Дослідження О. Задувайла [40] щодо розуміння механізму правового регулювання забезпечення інформаційної безпеки крізь призму аналізу права людини та громадянина на інформацію в розрізі приватності та секретності дозволяє говорити про багатоканальність даної кореляції. Так, процеси одержання, використання, поширення, зберігання та захисту даних та інформаційних потоків, котрі існують в системі забезпечення (реалізації) прав та свобод людини у даному дослідженні визнаються складовою частиною механізму формування інформаційно-суверенного простору всередині держави [40]. При цьому, факт реалізації права на інформацію людиною та громадянином, пропорційно матеріалів даного дослідження [40], можливий виключно за умови повноцінної та всескладної кореляції із громадськими, політичними, економічними, соціальними, духовними, екологічними та іншими правами, свободами і законними інтересами громадян, правами та інтересами юридичних осіб.

Позиція О. Задувайла є концептуально вагомою, оскільки вона не лише зводить механізм правового регулювання забезпечення інформаційної безпеки до нормативно-правового рівня, але й демонструє його як інтегральну частину загальної системи прав людини. Автор пропонує розглядати інформаційне право не ізольовано, а у зв’язку з іншими фундаментальними правами, такими як право на гідність, на свободу думки та слова, на таємницю особистого життя, на власність, а також право на безпечне інформаційне середовище. Такий підхід дозволяє говорити про формування нової доктрини — доктрини «інформаційного суверенітету особи», де захист прав людини і громадянина

стає первинною основою державної інформаційної політики.

Важливим у цьому контексті є те, що О. Задувайло фактично пропонує поєднання індивідуального і колективного вимірів інформаційної безпеки. Індивідуальний вимір полягає у визнанні права кожного громадянина на доступ до достовірної інформації, її використання та захист власних персональних даних, тоді як колективний — у формуванні правових механізмів, що гарантують стабільність і цілісність інформаційного простору держави. Це дозволяє досягати гармонії між публічним і приватним інтересом у сфері інформаційних відносин, зокрема через баланс між відкритістю інформації та необхідністю забезпечення національної безпеки.

Крім того, О. Задувайло акцентує на важливості дотримання принципу пропорційності у сфері інформаційної безпеки: будь-які обмеження доступу до інформації, моніторинг або контроль з боку держави повинні мати законну мету, бути чітко визначеними, обґрунтованими і співмірними з тими правами, які вони потенційно зачіпають. Це положення, з одного боку, підтверджує необхідність існування нормативного контролю, а з іншого — унеможливлює надмірне втручання у приватне життя, що є однією з головних проблем сучасних демократичних систем у цифрову епоху.

Таким чином, у роботі О. Задувайла [40] механізм правового регулювання забезпечення інформаційної безпеки постає не лише як система формальних юридичних процедур, а як багаторівневий інструмент реалізації загальних принципів верховенства права, правової визначеності, поваги до людської гідності та недоторканності приватного життя. У цьому аспекті науковець фактично розширює традиційне уявлення про інформаційну безпеку, розглядаючи її не тільки як елемент державного захисту, а як правову гарантію безпеки людини в інформаційному суспільстві.

З точки зору сучасної доктрини, така позиція є надзвичайно прогресивною, оскільки підкреслює взаємозалежність інформаційної безпеки й прав людини, що стає особливо актуальним у світлі тенденцій цифровізації,

глобальної мережевої взаємодії та зростання впливу інформаційних технологій на політичні, економічні та соціальні процеси. Інформаційна безпека, у трактуванні Задувайла, не може розглядатися без урахування правової культури користувачів, рівня цифрової грамотності, етичних стандартів поводження з інформацією та відповідальності суб'єктів владних повноважень за забезпечення прозорості інформаційних процесів.

У підсумку, дослідження О. Задувайла формує важливий теоретичний орієнтир для переосмислення механізму правового регулювання забезпечення інформаційної безпеки в Україні. Його змістовна спрямованість дозволяє говорити про необхідність інтеграції гуманістичного підходу у сферу інформаційного права, що, своєю чергою, забезпечує реалізацію принципу людиноцентризму в інформаційній політиці держави та підсилює гарантії конституційного права громадян на інформацію як фундаментального елементу демократичного суспільства.

Також доцільно відзначити, що у даному дослідженні формат механізму правового регулювання забезпечення інформаційної безпеки крізь призму права людини на інформацію як абсолютного та повноцінного розкритий не повною мірою. Враховуючи, що інших підходів до формування кореляційного зв'язку між категоріями «механізм правового регулювання забезпечення інформаційної безпеки» та «право людини та громадянина на інформацію» у системі вітчизняного дослідницького поля знайти не вдалося, пропонуємо власний підхід до розуміння даного взаємозв'язку.

Форматом останнього доцільно визнати взаємне забезпечення прав, де право людини на інформацію забезпечується шляхом послідовної діяльності органів та інституцій інформаційно-безпекової парадигми, а інформаційна безпека як конструкт державно-управлінської діяльності має на меті реалізацію якраз-таки крізь призму забезпечення прав населення (громадянського суспільства) на інформацію та конституційної непорушності такого права. На нашу думку, за таких умов не створюватиметься конфліктологічне трактування

двох вищенаведених конструкцій і, водночас, максимально забезпечуватиметься концептуальний складник розуміння безпеки інформації як детермінанти суверенітету держави та формуляра конструювання державності зокрема.

Проаналізовані вище підходи та положення до розуміння поняття, категорії та явища механізму правового регулювання забезпечення інформаційної безпеки у структурі механізму правового забезпечення інформаційної безпеки в Україні дозволяють говорити про багатовимірність зазначеної категорії у контексті наукового інтересу. Саме тому пропонуємо надалі звернути увагу на аналіз принципів побудови механізму правового регулювання забезпечення інформаційної безпеки України крізь призму науково-доктринального розуміння даної сегментованої категорії.

Насамперед, звертаємо увагу на матеріали праці К. Юдкової [200, с. 75], котра розглянула модель побудови інформаційної безпеки в Україні з позиції права та державного управління. На її переконання, під принципами побудови механізму правового регулювання забезпечення інформаційної безпеки в Україні в рамках сучасних викликів доцільно розуміти ті засади, за допомогою котрих відбувається впровадження практичної реалізації засад, напрямів, підходів та способів створення, функціонування зазначеної кластерної категорії із урахуванням її суб'єктів – держави, державних органів та установ, засобів масової інформації та громадянського суспільства, що виступає основним чинником реалізації нововведень інформаційної політики та інформаційної безпеки на державно-управлінському рівні.

Не дивлячись на досить повноцінне та конкретизоване розуміння понятійно-категоріального призначення принципів побудови механізму правового регулювання забезпечення інформаційної безпеки в системі державно-управлінської теорії, допрацювання, на наш погляд, потребує аспектна складова розгляду кінцевої мети діяльності в рамках даної ініціативи. Такою, на наш погляд, можна вважати потребу в спрямованості на балансуванні

між захистом інформаційно-просторової безпеки, інформаційної гігієни, а також – прав та свобод людей і громадян у інформатизаційному, діджиталізованому цифровому суспільстві сьогодення, що живе в рамках сучасних викликів, як-от повномасштабна військова агресія рф проти України від 24.02.2022 р. та політика дезінформації, котру остання продукує задля дестабілізації ситуації всередині Української держави.

Надалі перейдемо до більш детального трактування власне принципів побудови механізму правового регулювання забезпечення інформаційної безпеки. Відповідно матеріалів декількох вітчизняних досліджень проблематики інформаційної безпеки з позиції права та публічного управління та адміністрування [200], до останніх доцільно відносити принцип законності, принцип захисту прав та свобод людини, принцип національного суверенітету, принцип прозорості, принцип превентивності, принцип технологічної адаптивності, принцип міжвідомчої координації, принцип співпраці та інтеграції, принцип пропорційності, принцип відповідальності, принцип безперервності. Надалі пропонуємо здійснити більш деталізований огляд зазначених принципів як складових механізму правового регулювання забезпечення інформаційної безпеки в Україні.

Принцип законності як елемент побудови механізму правового регулювання забезпечення інформаційної безпеки базується на концепції, згідно з якою правове регулювання інформаційної безпеки повинно мати законний характер. Законність процедури правового регулювання інформаційної безпеки має два виміри – внутрішній та міжнародний. Внутрішній полягає у виконанні положень Основного закону – Конституції України – у розрізі забезпечення прав та свобод людини і громадянина у інформаційній галузі, міжнародний (зовнішній) – у слідуванні положенням міжнародного права під час забезпечення прав та свобод людини і громадянина у інформаційній сфері, а також – інтересів держави у даній сфері водночас [200].

У такому контексті принцип законності виступає своєрідною базовою передумовою для функціонування всього правового механізму, адже саме на ньому ґрунтується довіра до державної політики у сфері інформаційної безпеки, її стабільність та передбачуваність. Дотримання цього принципу гарантує, що будь-які дії, спрямовані на регулювання інформаційних процесів, здійснюються виключно в межах, визначених чинним законодавством, а прийняття рішень у цій сфері відбувається із чітким дотриманням процедур правотворчості та правозастосування. Законність, у даному випадку, не зводиться лише до формального аспекту – вона охоплює й змістовний вимір, передбачаючи, що норми права повинні мати узгоджений характер, бути внутрішньо несуперечливими та відповідати принципам справедливості, пропорційності й правової визначеності.

Водночас, принцип законності виконує функцію системоутворювального чинника, що поєднує нормативні засади інформаційної безпеки з практичною діяльністю органів державної влади, органів місцевого самоврядування, а також суб’єктів господарювання та громадянського суспільства. У цьому аспекті його реалізація забезпечує баланс між правами особи, інтересами суспільства та обов’язками держави. Застосування принципу законності у сфері інформаційної безпеки уможливлює створення цілісного нормативного середовища, у якому забезпечується відповідність дій державних інституцій конституційним положенням, а діяльність суб’єктів інформаційних відносин перебуває під правовим контролем, що запобігає проявам свавілля, маніпуляцій чи зловживань.

Змістовно принцип законності у цій сфері також відображає необхідність належного нормативного закріплення усіх етапів інформаційної діяльності — від збору та зберігання даних до їх обробки, передачі, поширення й захисту. Це означає, що кожен елемент інформаційного циклу повинен бути врегульований на рівні закону або підзаконного акта з урахуванням вимог Конституції України, міжнародних договорів та загальновизнаних принципів міжнародного

права. З огляду на це, реалізація принципу законності у сфері інформаційної безпеки виступає індикатором зрілості правової системи держави та рівня її інтегрованості до європейського і світового правового простору.

У міжнародному вимірі принцип законності набуває особливого значення як інструмент гармонізації національного законодавства із нормами та стандартами міжнародного права. Йдеться насамперед про дотримання універсальних документів, що регулюють питання свободи вираження поглядів, права на доступ до інформації, захисту персональних даних, а також відповідальності держави за неправомірне втручання в інформаційні процеси. Виконання цих зобов'язань є показником того, що держава дотримується міжнародно-правових стандартів у сфері інформаційної безпеки, забезпечуючи при цьому легітимність і правомірність своєї діяльності у глобальному інформаційному просторі.

Крім того, принцип законності у сфері правового регулювання інформаційної безпеки слугує основою для формування правосвідомості та правової культури суб'єктів інформаційних відносин. Він вимагає, щоб не лише держава, але й усі учасники інформаційних процесів – громадяни, юридичні особи, засоби масової інформації, оператори електронних комунікацій – діяли виключно у межах чинного правового поля. Такий підхід забезпечує сталість функціонування інформаційного середовища, знижує рівень правових конфліктів та сприяє формуванню атмосфери правової визначеності і взаємної довіри між державою та суспільством.

Отже, принцип законності у механізмі правового регулювання забезпечення інформаційної безпеки є не лише формально-юридичною вимогою, але й фундаментальною основою для стабільності, передбачуваності та ефективності всієї системи правового забезпечення. Його дотримання створює умови для узгодженості внутрішніх і зовнішніх правових процесів, забезпечує взаємозв'язок між правотворчою та правозастосовною діяльністю, а також гарантує, що інформаційна безпека розвиватиметься у рамках правового

поля, з урахуванням національних інтересів та міжнародних зобов'язань держави.

Принцип захисту прав та свобод людини у контексті однієї із складових частин побудови механізму правового регулювання забезпечення інформаційної безпеки, в свою чергу, полягає у забезпеченні останньої на засадах демократизму [200]. Людиноцентристські цензи даного процесу можуть бути розкриті у ст. 3 Конституції України, що визнає людину найвищою соціальною цінністю, а також – у ст. 2 Закону України «Про інформацію» № 2657-XII та ст. 3, ст. 4 Закону України «Про доступ до публічної інформації» № 2939-VI, котрими гарантується право громадян на отримання інформації загалом та, зокрема, право на отримання достовірної та об'єктивної інформації (даних) громадянами про обставини, що стосуються схоронності їхніх прав та інтересів.

Принцип національного суверенітету як один із чинників категорії реалізації призначення механізму правового регулювання забезпечення інформаційної безпеки, водночас, доцільно розглядати крізь призму чинної та особливої за статусом ролі держави у контролі та координації національного інформаційного простору. Така діяльність, при цьому, повинна перебувати на межі спрямування внутрішнього інформаційного простору та забезпечення захисту національного інформаційного суверенітету від внутрішніх втручань та загроз дезінформаційного та дестабілізаційного характеру [200].

Тобто доцільно констатувати, що у межах сучасного публічно-управлінського та юридико-правового дискурсу принцип національного суверенітету в інформаційній сфері постає не лише як теоретико-правова конструкція, але як реальний інструмент забезпечення незалежності держави у процесі формування, контролю й захисту власного інформаційного простору. Його сутність полягає у визнанні державою своєї виключної компетенції щодо визначення стратегічних напрямів розвитку інформаційної політики, створення нормативно-правових гарантій збереження цілісності інформаційної

інфраструктури та недопущення зовнішнього або внутрішнього втручання у механізми формування суспільної думки, комунікаційних процесів і державних інформаційних ресурсів.

Змістовно ж, принцип національного суверенітету в контексті інформаційної безпеки охоплює комплекс явищ, що забезпечують здатність держави діяти як автономний суб'єкт у глобальному інформаційному середовищі. Це передбачає спроможність формувати власну інформаційну політику без нав'язування зовнішніх моделей, підтримувати незалежність інформаційних систем і мереж, а також гарантувати захист стратегічних державних інформаційних ресурсів. Такий підхід набуває особливої ваги в умовах зростання кількості інформаційних загроз, кібератак, операцій впливу та маніпуляцій, які можуть мати як транснаціональний, так і внутрішньополітичний характер.

Виходячи з цього, можна визначити, що практичній площині принцип національного суверенітету передбачає, що держава має не лише право, але й обов'язок забезпечувати збереження інформаційного простору від деструктивних впливів, формувати ефективні системи реагування на загрози, створювати інституційні механізми для підтримання інформаційної гігієни суспільства. Водночас, реалізація цього принципу повинна відбуватися в межах міжнародно-правових зобов'язань, що гарантують дотримання прав і свобод людини у сфері інформації, забезпечують баланс між безпекою та відкритістю, між контролем і свободою комунікації.

Фактично, принцип національного суверенітету у сфері інформаційної безпеки також є основою для визначення державою пріоритетів у розвитку цифрової інфраструктури, управлінні стратегічними даними, технологічною модернізацією інформаційних систем і формуванні національної стратегії кіберстійкості. Його дотримання сприяє зміцненню національної ідентичності, підтриманню інформаційного балансу у суспільстві та формуванню єдиного комунікаційного простору, що діє в межах правового поля та на засадах

демократичних цінностей.

Окрім того, принцип національного суверенітету визначає межі взаємодії держави з іншими суб'єктами міжнародних відносин у сфері інформаційної безпеки. Тут говоримо про участь у розробленні міжнародних документів, що регламентують порядок обміну інформацією, запобігання кіберзлочинності, боротьбу з пропагандою та гібридними загрозами. Дотримання цього принципу дозволяє державі відстоювати власні інтереси на глобальній арені, зберігаючи при цьому стабільність і незалежність внутрішнього інформаційного середовища.

Таким чином, принцип національного суверенітету у механізмі правового регулювання забезпечення інформаційної безпеки виконує роль концептуальної основи державної політики у цій сфері, оскільки саме через нього реалізується взаємозв'язок між національними інтересами, правовими гарантіями, публічним управлінням та безпосередньою практикою забезпечення інформаційного суверенітету. Він утверджує автономність держави у здійсненні інформаційної політики, формує підґрунтя для ефективного реагування на сучасні інформаційні загрози та сприяє утвердженню правової моделі, у якій інформаційна безпека виступає не лише елементом безпекового середовища, а й ключовим чинником державної стійкості.

Принцип прозорості як категорія реалізації призначення механізму правового регулювання забезпечення інформаційної безпеки базується на необхідності прозорого, відкритого та гласного їхнього функціонування в інтересах населення, громадянського суспільства. Також, зазначений принцип передбачає опцію проведення громадського та парламентського контролю за діяльністю органів, що здійснюють таку діяльність [200] (в Україні до таких належать Служба безпеки України (СБУ), Рада національної безпеки і оборони України (РНБО), Міністерство цифрової трансформації України (Мінцифра), Міністерство культури України (Мінкульт) та Національна поліція України (Нацполіція). Повноважна складова діяльності останніх в рамках забезпечення

інтересу громадянського суспільства буде розглянута у п. 2.2 та п. 2.3 Розділу ІІ даного дисертаційного дослідження.

Принцип превентивності у якості складової механізму правового регулювання забезпечення інформаційної безпеки спрямований на акцент запобігання інформаційним загрозам, а не лише протидію останнім після їхньої появи [200]. Зазначена модель має більшою мірою теоретичне призначення, концептуально базуючись на необхідності формування такої інформаційно-безпекової карти та гігієни всередині країни, котра забезпечуватиме інтереси державних органів у виконанні ними безпосередніх публічного (державного) управління, а також інтереси засобів масової інформації у висвітлення обставин об'єктивної дійсності без запобігань даному процесу та зловживань (узурпації) влади органами та інституціями, відповідальними за сектор власне інформації та публічної діяльності. Чільне місце серед забезпечення інформаційних прав та свобод громадян у структурі принципу превентивності займають права та свободи людей і громадян, котрі підлягають державній охороні на засадах постійності та всебічності [200].

Принцип технологічної адаптивності у структурі механізму правового регулювання забезпечення інформаційної безпеки спрямований на необхідність послідовного підлаштування вітчизняного апарату управління під реалії видозмін цифрового, інформаційного та діджитал-простору [200]. Інституційне забезпечення такого принципу як сегментарного у концепції забезпечення інформаційної безпеки України у часи геополітичної та геоглобальної нестабільності покладено на Міністерство цифрової трансформації України (Мінцифру) та Кіберполіцію.

Принцип міжвідомчої координації, що використовується з метою повного та всебічного впровадження механізму правового регулювання забезпечення інформаційної безпеки у предметну дію на рівні інституційно-правової парадигми, своєю чергою базується на взаємодії між акторами (учасниками, від англ. «actor») інформаційного простору, себто його суб'єктами, як-от держава у

особі органів державної влади, громадянське суспільство (громадяни, особливо проактивна частина населення) та бізнесом, що прямим або опосередкованим чином детермінує та передвизначає особливості формування безпеково-інформаційної карти держави [200]. В Україні потребує подальшої сегментації та розвитку саме складова частина впливу громадянського суспільства на інформаційну політику держави, адже остання формує модель інформаційної безпеки (вона залежить від досконалості, дієвості та ефективності державної інформаційної політики). Певного переосмислення у даному контексті також вимагає сегментація діяльності Міністерства культури та інформаційної політики України (Мінкульту), діяльність котрого забезпечується Постановою КМУ № 885 від 16.10.2019 р. Деякі питання діяльності Міністерства культури та стратегічних комунікацій (редакція від 24.09.2024 р.).

Принцип співпраці та інтеграції як керівна структурна парадигма побудови механізму правового регулювання забезпечення інформаційної безпеки базується насамперед на взаємодії із міжнародними організаціями, обміні досвідом та рецепції досвіду від країн-членів ЄС та державам, що визнаються для України стратегічними партнерами, у галузі інформаційної політики та інформаційної безпеки [200]. З точки зору інституційного забезпечення, тут варто говорити про запозичення стандартів таких органів у інформаційній галузі, як Європейська агенція з кібербезпеки (European Union Agency for Cybersecurity (ENISA)), а також Єврокомісії, Європарламенту та Ради Європи (до питання створення нормативно-правового інструментарію регулювання інформаційно-безпекового простору такими законодавчими документами, як Європейська стратегія безпеки 2006 р. та Європейська стратегія кібербезпеки 2020 р.)

Принцип пропорційності у системі побудови механізму правового регулювання забезпечення інформаційної безпеки в Україні, в свою чергу, виходить із необхідності реалізації інформаційно-безпекових наративів на засадах помірного втручання у діяльність суб’єктів інформаційного простору та

пропорційності (відповідності) заходів, спрямованих на забезпечення інформаційної безпеки, загальному рівню загроз, що генеруються у даній галузі відповідно до політичної, економічної та загальнополітичної (геополітичної) ситуації, в якій перебуває держава.

Крізь призму теорії та практики державного управління, тут маємо говорити про діяльність органів (інституцій), що забезпечуються безпеку в інформаційній сфері – Служби безпеки України (СБУ), Ради національної безпеки і оборони України (РНБО), Міністерства цифрової трансформації України (Мінцифри), Міністерства культури та стратегічних комунікацій України (Мінкульту) та Національної поліції України (Нацполіції) в межах правового поля, що визначається нормативними документами, котрі спрямовують, координують та систематизують діяльність останніх. Особливості діяльності останніх як суб'єктів забезпечення інформаційної безпеки в Україні означуватимемо у п. 2.3 Розділу ІІ даного дисертаційного дослідження.

Принцип відповідальності у якості структурної парадигми побудови механізму правового регулювання забезпечення інформаційної безпеки заснований на тому, що кожен із суб'єктів інформаційного простору відповідальний за дотримання норм, положень та правил інформаційно-безпекового середовища [200]. До таких суб'єктів можна віднести власне державу, засоби масової інформації, приватні компанії (що генерують інформаційно-безпекову парадигму та існують в інформаційно-безпековому просторі водночас) та громадян (громадянське суспільство).

Тобто, у цьому контексті принцип відповідальності не обмежується лише формальним дотриманням законодавчих норм, а набуває рис багаторівневої етичної, інституційної та технологічної взаємодії між суб'єктами інформаційних відносин. Кожен із них, діючи у власних межах компетенції, виконує функцію носія інформаційної культури, що передбачає як свідоме дотримання принципів достовірності, відкритості та безпеки інформації, так і

формування належних практик поводження з нею у цифровому середовищі. Зокрема, держава має виступати гарантом дотримання інформаційного законодавства, створюючи належні правові, організаційні та технічні умови для реалізації права на інформацію та захисту персональних даних.

Медіа, у свою чергу, покликані забезпечувати баланс між свободою слова та відповідальністю за точність і достовірність переданої інформації, утримуючись від поширення матеріалів, що можуть загрожувати публічній безпеці, репутації осіб або національним інтересам. Приватні компанії, особливо ті, що здійснюють діяльність у сфері ІТ, телекомунікацій, кібербезпеки, повинні дотримуватись норм захисту інформаційних систем і сприяти формуванню безпечного цифрового середовища. Громадяни ж, як безпосередні споживачі та поширювачі інформації, несуть моральну та правову відповідальність за власну інформаційну поведінку, що виражається у дотриманні вимог щодо поширення персональних даних, уникненні маніпуляцій та недопущенні розповсюдження неправдивої або шкідливої інформації.

Таким чином, принцип відповідальності постає не лише як складова юридичного механізму регулювання, але й як елемент соціального партнерства у сфері інформаційної безпеки, що забезпечує взаємозалежність прав і обов’язків усіх учасників інформаційного процесу. Його реалізація сприяє побудові стійкої інформаційної культури суспільства, формуванню довіри до державних інституцій та медіа, а також створенню правових передумов для запобігання інформаційним загрозам і мінімізації їх наслідків у межах національного інформаційного простору.

Наостанок, принцип безперервності як елемент побудови механізму правого регулювання забезпечення інформаційної безпеки в Україні базується на постійності даного процесу [200]. Водночас, останній повинен враховувати фактори ризику та змінності інформаційно-безпекового середовища, пов’язані із внутрішньо- та зовнішньополітичними аспектами, як-от збройна агресія рф

проти України від 24.02.2022 р. та загрози, що походять від даного факту.

Отже, безперервність у цьому контексті виступає не лише як характеристика часової тяглості правового регулювання, але й як засадничий принцип системності, що забезпечує стійкість інформаційного простору до динамічних викликів глобалізованого світу. Йдеться про необхідність розуміння інформаційної безпеки як процесу, який ніколи не може бути завершеним або статичним — він є постійно діючим механізмом, який адаптується, трансформується та самовідтворюється відповідно до змін технологічних, політичних і соціальних реалій. У цьому сенсі принцип безперервності формує правову доктрину, де інформаційна безпека постає не як реакція на загрозу, а як стратегічна готовність до неї.

З позицій теорії права безперервність означає необхідність підтримання постійного правового моніторингу, оновлення нормативно-правових актів, адаптації стратегій кіберзахисту, інформаційної політики та засобів контролю за дотриманням інформаційних прав громадян. В умовах збройної агресії рф, цей принцип набуває особливої актуальності, оскільки інформаційна безпека перетворюється на складову обороноздатності держави, а її забезпечення стає не лише технічним чи адміністративним завданням, а — питанням національного виживання. Безперервність у таких умовах передбачає постійне вдосконалення правових механізмів, оперативне реагування на зміни у характері загроз — від кібератак до маніпуляцій масовою свідомістю — та адаптацію державної політики до нових форматів гібридних впливів.

Крім того, принцип безперервності має і стратегічний вимір — він охоплює питання сталості інституцій, спроможності держави забезпечувати ефективну взаємодію між усіма суб’єктами інформаційного простору: державними структурами, бізнесом, науковими центрами, громадянським суспільством. Його реалізація передбачає формування сталої комунікаційної екосистеми, у якій процеси інформаційного обміну, збирання, обробки та захисту даних здійснюються на основі постійного оновлення технологій,

правових рішень та етичних стандартів.

Таким чином, принцип безперервності визначає не лише часовий вимір функціонування механізму правового регулювання забезпечення інформаційної безпеки, але й його якісний потенціал — здатність до саморозвитку, стійкості та адаптивності. Його сутність полягає у тому, що правове забезпечення інформаційної безпеки не може бути одноразовим актом чи набором фрагментарних заходів, а має формувати цілісну, еволюційну систему, яка постійно оновлюється у відповідь на зміни середовища. В умовах сучасних гібридних загроз і глобальної інформаційної конкуренції такий підхід є не просто бажаним, а життєво необхідним для збереження національного інформаційного суверенітету, забезпечення стабільності держави та захисту фундаментальних прав і свобод людини в інформаційній сфері.

Ми також маємо розуміти, що, окрім власне теоретико-доктрнального, класифікаційного розуміння поняття та принципів побудови механізму правового регулювання забезпечення інформаційної безпеки, існує також і методологічний контекст його класифікації, дослідницького осмислення та ґенерації, котрий і буде розглянуто нижче.

Насамперед, маємо виходити з того, що, у контексті стрімкого поширення цифрових технологій, гібридних конфліктів та розмивання традиційних меж національного суверенітету забезпечення інформаційної безпеки постає як ключове завдання сучасної державної політики. Проблематика правового регулювання у цій сфері характеризується високим ступенем міждисциплінарності, що передбачає залучення не лише суто юридичних, а й управлінських, інформаційно-технологічних та філософських категорій. У такому контексті традиційні механізми правового впливу потребують перегляду з урахуванням динаміки інформаційного середовища та його специфічних характеристик: децентралізованості, швидкості обміну даними, технологічної адаптивності.

В свою чергу, актуальність методологічного підходу до аналізу правового

механізму забезпечення інформаційної безпеки полягає у необхідності сформувати системне бачення не лише юридичних конструкцій, а й логіки управлінської дії у цифрову добу. Без такого бачення неможливо ані окреслити межі державного втручання у сферу інформаційного обігу, ані забезпечити баланс між безпекою та правами людини. Саме тому важливим кроком у межах дисертаційного дослідження є вивчення понятєво-категоріального апарату та принципів, які мають лягати в основу правового регулювання інформаційної безпеки в державотворчих практиках.

Розгляд правового регулювання забезпечення інформаційної безпеки вимагає складного методологічного інструментарію, оскільки це явище охоплює не лише нормативно-правову площину, але й соціальні, технологічні, антропологічні та ризикологічні параметри. Саме тому подальший аналіз побудований на системному поєднанні загальнонаукових, спеціально-правових та міждисциплінарних підходів, що забезпечує багаторівневе бачення предмету дослідження.

Так, до групи загальнонаукових методів, застосованих у дослідженні, належать аналіз, синтез, індукція, дедукція, моделювання та абстрагування. Метод аналізу дозволяє розчленувати складний феномен правового забезпечення інформаційної безпеки на окремі компоненти: нормативну базу, суб'єктний склад, інституційний механізм, контрольні процедури тощо. Синтез, у свою чергу, уможливлює реконструкцію цих елементів у цілісну систему, придатну для аналітичної інтерпретації.

Індуктивний підхід застосовується при узагальненні практики правового регулювання в окремих державах (Україна, США, Китай) для формування висновків щодо універсальних закономірностей. Дедукція забезпечує екстраполяцію фундаментальних положень теорії держави і права на конкретику сфери інформаційної безпеки. Метод абстрагування використовується для виведення загальних категорій (зокрема, «інформаційна загроза», «безпекова політика», «інформаційний суверенітет»), які становлять

основу поновлюваного поновлюваного поновлюваного глосарію термінів.

В свою чергу, у межах спеціально-правової методології провідну роль відіграють формально-юридичний, порівняльно-правовий, системно-структурний та інституційний методи. Формально-юридичний метод дає змогу аналізувати законодавчі акти, концепції, доктрини в їхньому текстуальному вираженні, виявляючи логічні прогалини, суперечності та потенціал нормативного моделювання.

Порівняльно-правовий метод дозволяє дослідити підходи до правового забезпечення інформаційної безпеки в різних юрисдикціях — зокрема, в умовах Європейського Союзу (з опорою на EU Cybersecurity Act 2019 р.), США (з аналізом Cybersecurity Information Sharing Act), Китаю та, власне, України. Системно-структурний підхід уможливлює розгляд правового механізму як багаторівневої ієрархічної системи, що включає нормативну основу, суб'єктів, процедурні регламенти, механізми реалізації й контролю.

Інституційний підхід дозволяє дослідити роль державних органів (зокрема, органів спеціального призначення: Служби безпеки України (СБУ), Державної служби спеціального зв’язку та захисту інформації (ДССЗЗІ), Національного координаційного центру кібербезпеки (НКЦК) у формуванні та реалізації політики інформаційної безпеки. Також він допомагає виявити взаємозв’язок між політико-адміністративними структурами та спеціалізованими регуляторами у сфері кібербезпеки.

На додаток до вищезазначеного, міждисциплінарність є визначальною рисою дослідження. Найбільш релевантними у цьому контексті виступають кібернетичний, інформаційно-антропологічний, етичний та ризикологічний підходи, що застосовуються для науково-методологічного аналізу механізмів реалізації інформаційної безпеки у системі публічного управління.

Кібернетичний підхід дозволяє тлумачити правове регулювання як механізм обробки, передачі та зворотного зв’язку інформації в системі «держава — суспільство — особа». Останній застосовується для опису процесів

управління ризиками, загрозами, інцидентами, а також для формалізації процедурної логіки реагування на кіберінциденти. Застосування цього підходу збагачує дослідження категорії механізмів інформаційної безпеки, оскільки дає змогу описати логіку реагування на ризики, загрози та інциденти у вигляді формалізованих процесів управління.

Інформаційно-антропологічний підхід дозволяє враховувати роль людини як одночасно об’єкта, суб’єкта та середовища інформаційного впливу, що особливо важливо при розробці політик у сфері маніпулятивних технологій, дезінформації, когнітивної безпеки.

Етичний підхід має особливе значення у сфері правового регулювання в інформаційному середовищі, оскільки багато рішень у сфері кібербезпеки лежать на межі правової допустимості й моральної виправданості (питання масового спостереження, контролю контенту, обмеження свободи слова). У цьому контексті вивчаються міжнародні підходи до інформаційної етики (наприклад, напрацювання згаданого Т. Фітцджеральда [66 , с. 79].

Ризикологічний підхід, натомість, у рамках використання даного методологічного конструкту забезпечує розуміння й моделювання імовірнісного характеру інформаційних загроз, їхньої системної природи та необхідності адаптивного управління на основі сценаріїв і мультифакторного аналізу.

Одночасно із вищезазначеним та вищезапропонованим, ураховуючи складну, динамічну та міжгалузеву природу об’єкта дослідження, нами також обґрунтовується застосування комбінованої методології, яка поєднує в собі переваги перелічених вище підходів. Такий синтез дає змогу уникнути редукціонізму, що властивий суто юридичному аналізу, і водночас забезпечити практичну застосовність напрацьованих теоретичних моделей у площині державного управління.

Комбінована методологія, зокрема та виключно, дозволяє:

побудувати багаторівневу модель правового регулювання з урахуванням

змін цифрової реальності;

здійснювати системний аналіз загроз і відповідей на них у межах існуючого правового поля;

окреслити ціннісно-етичні межі допустимого у сфері інформаційного впливу;

проектувати нормативні інтервенції на основі міждисциплінарного бачення безпеки.

Сукупно, ідеологічно та конвенційно, на рівні окреслення категорій, закономірностей та конструкцій дослідження поняття та принципів побудови механізму правового регулювання забезпечення інформаційної безпеки, ми наразі маємо змогу сформувати також індивідуалізоване, впорядковане бачення дисертанта щодо власного моделювання дослідження зазначеного предмету розвідки, котре, знову-таки, представляємо нижче.

Таким чином, власна методологічна модель дисертанта ґрунтується на адаптації системно-комплексного підходу, у межах якого дослідження здійснюється із урахуванням кількох взаємопов’язаних аналітичних рівнів.

Зокрема, концептуальний рівень дослідження передбачає вивчення змісту інформаційної безпеки як категорії правової, управлінської та безпекової науки, що відображає трансформацію уявлень про суверенітет, контроль і ризик в епоху цифрових викликів [66, с. 89].

В той же час, нормативно-правовий рівень фокусується на аналізі структури та внутрішньої логіки нормативного забезпечення інформаційної безпеки, при цьому особливу увагу приділено взаємозв’язку між рівнями законодавства, спеціальних актів та підзаконного регулювання [66, с. 89].

Інституційно-управлінський аспект, на додаток, передбачає вивчення ролі державних органів і спеціальних суб’єктів, зокрема, їх здатності до адаптивного управління інформаційними загрозами в умовах високої турбулентності [66, с. 89].

У межах механізмового підходу, зрештою, аналізуються практичні

інструменти правового регулювання — індикатори, регулятивні алгоритми, санкційні моделі, а також процедури екстреного реагування. Тоді як ціннісний вимір дослідження дозволяє оцінити легітимність державного втручання в інформаційне середовище крізь призму етичних меж, прав людини та принципу пропорційності [66 , с. 89].

На основі проаналізованих особливостей механізму правового регулювання забезпечення інформаційної безпеки в Україні з точки зору теорії та доктрини, а також методологічного оснащення останнього ми дійшли деяких проміжних умовиводів, котрі викладаємо нижче.

Так, у процесі дослідження поняття та принципів побудови механізму правового регулювання забезпечення інформаційної безпеки було визначено, що цей механізм є комплексною системою нормативно-правових актів, інституцій, процедур і засобів, спрямованих на захист національного інформаційного простору від загроз. Його основною метою є забезпечення стабільності та безпеки інформаційної інфраструктури, захист прав і свобод громадян, а також протидія інформаційним загрозам у контексті глобалізації та цифровізації.

В основу побудови механізму закладено такі фундаментальні принципи, як законність, національний суверенітет, захист прав і свобод людини, технологічна адаптивність, прозорість та підзвітність, превентивність, пропорційність, міжвідомча координація та публічно-приватне партнерство. Особливе значення має інтеграція з міжнародними стандартами та співпраця із закордонними партнерами для протидії глобальним інформаційним загрозам.

Принципи побудови механізму правового регулювання забезпечення інформаційної безпеки визначають орієнтири для гармонійного розвитку правової бази, яка дозволяє ефективно реагувати на виклики сучасного інформаційного середовища, зберігаючи при цьому баланс між захистом національних інтересів і дотриманням демократичних цінностей. Це створює основу для впровадження інноваційних рішень, посилення кіберзахисту та

забезпечення безпеки інформаційного простору України в умовах зростаючих глобальних викликів.

Також, здійснене методологічне осмислення правового регулювання інформаційної безпеки дозволило виокремити кілька концептуально значущих напрямів. Нами з'ясовано, що сама сфера інформаційної безпеки виходить за межі традиційної правової доктрини, інтегруючи технічні, соціальні, філософські та управлінські компоненти. Зазначене, своєю чергою, зумовлює потребу у мультидисциплінарному підході до її дослідження, що базується на поєднанні загальнонаукових і спеціально-правових методів із урахуванням новітніх підходів з кібернетики, ризикології, етики та інформаційної антропології.

До того ж, проведений аналіз джерел засвідчив, що сучасні наукові концепції у сфері інформаційної безпеки не обмежуються тільки технічними або нормативними розробками. У фокусі міжнародного і вітчизняного правового дискурсу все частіше опиняються питання легітимності, дотримання прав людини, забезпечення інформаційної автономії, а також прозорості процесів обробки та захисту даних. Як наслідок, розуміння інформаційної безпеки потребує переходу від інфраструктурного до ціннісно-регулятивного виміру.

Наостанок, сформована дисертантом методологічна модель базується на системно-інституційному підході, доповненому елементами механізмового, ціннісного та функціонального аналізу. Це дозволяє оцінити не лише ефективність існуючих нормативних рішень, а й виявити прогалини в регулюванні, зумовлені як нормативною інерцією, так і швидкими змінами інформаційного середовища. Застосування комбінованої методології уможливлює створення цілісної аналітичної рамки для вивчення механізмів правового забезпечення інформаційної безпеки.

Таким чином, запропонована система принципів і визначення механізму правового регулювання є важливим кроком до формування дієвого

інструментарію для реалізації державної політики в сфері інформаційної безпеки, а обрана методологія дослідження не лише забезпечує всебічність і наукову обґрунтованість, але й створює основу для подальшого розроблення ефективних правових механізмів, адаптованих до викликів цифрової доби, адже поєднує критичний аналіз нормативної бази з емпіричним досвідом реалізації інституційних практик, що дає змогу здійснити глибоку реконструкцію предмета дослідження у межах державно-управлінської парадигми.

2.3. Правове регулювання забезпечення інформаційної безпеки у системі публічного управління

Феномен правового регулювання забезпечення інформаційної безпеки у контексті державного управління та державного регулювання інформаційної безпеки є комплексним та багатоаспектним, тому потребує аналізу у декількох, пов’язаних між собою проте сутнісно відмінних, структурно-ідеологічних форматах.

Так, на наш погляд, останній доцільно розглядати у теоретичному вимірі (погляди науковців та дослідників на проблему правового регулювання та державного регулювання забезпечення інформаційної безпеки в Україні) та нормативно-практичному вимірі (аналіз деяких нормативно-правових актів, що є основою спрямування та координації інформаційної безпеки в Україні як сталої політичної та публічно-управлінської конструкції) водночас.

Підходи-концепції до розуміння особливостей правового регулювання забезпечення інформаційної безпеки у контексті її державного управління та державного регулювання можемо прослідковувати у працях А. Крупнової [113, 7 с.], О. Каплі [64, с. 16-20], В Цимбалюка [188, с. 22-30], І. Лопатченка [120, с. 14-24]. Пропонуємо конкретизувати науково-доктринальні погляди останніх на проблему юридичного забезпечення інформаційно-безпекового простору в Україні.

У дослідженні А. Крупнової, присвяченому розгляду та критичному аналізу правового регулювання сфери забезпечення інформаційної безпеки в Україні [113, с. 4-5], останнє розглядається радше з теоретико-доктринальної, аніж з юридико-концептуальної точки зору. Так, на переконання авторки, в Україні основами правового регулювання сфери забезпечення інформаційної безпеки як процесу є аналіз сутності інформаційної безпеки, розуміння ролі права у забезпеченні інформаційної безпеки та глобального контекстного виміру інформаційної безпеки водночас.

Аналіз сутності інформаційної безпеки у якості елемента теоретичного виміру розуміння феномену правового регулювання сфери забезпечення інформаційної безпеки в Україні, згідно матеріалів вищенаведеного дослідження [113, с. 4], являє собою процес, що формує необхідність національного законодавця дотримуватися таких постулатів під час нормотворчої діяльності, як збереження цілісності та доступності інформаційних ресурсів, захист прав на приватність, свободу слова та доступ до інформації та протидія кібератакам, дезінформації, шпигунству та іншим загрозам.

Розуміння ролі права у забезпеченні інформаційної безпеки у якості складника правового регулювання сфери забезпечення інформаційної безпеки в Україні у згаданій праці А. Крупнової [113, с. 4] розглядається з позиції необхідності урахування балансу між свободою інформації та необхідністю захисту національних інтересів, формування концепції відповідальності за порушення інформаційно-безпекових стандартів (приписів) та, водночас, регулювання суб’єктів інформаційного простору, що критично та ідеологічно повинно враховувати інтерес громадянського суспільства та держави водночас.

Глобальний контекст розуміння інформаційної безпеки як заключна модель, розглянута у вищезазначеному дослідженні [113, с. 5], проаналізована крізь призму неухильної необхідності у кореляційному взаємозв’язку між нормативними підходами до регулювання інформаційної безпеки

безпосередньо в Україні та, водночас, у ЄС та інших країнах, включно із європейськими стандартами, наявними у законодавстві країн-членів.

Розвиваючи ідеї, запропоновані А. Крупновою, варто підкреслити, що дослідження набуває особливого значення в контексті формування сучасної української доктрини інформаційної безпеки, яка має подвійний характер — як теоретико-правовий, так і прикладний. Авторка фактично підводить до висновку, що ефективність національного механізму правового регулювання у цій сфері визначається не стільки кількістю прийнятих законів, скільки якістю концептуальних засад, які лежать в основі законодавчої архітектури. Тобто йдеться про створення цілісної системи, у якій право не просто встановлює правила поведінки у цифровому чи медійному середовищі, а й формує ціннісні орієнтири для функціонування держави, суспільства та індивіда у нових умовах інформаційної взаємодії.

Підхід А. Крупнової демонструє спробу вийти за межі традиційного правового дискурсу, у якому інформаційна безпека розглядається як технічна категорія. Вона пропонує розуміти її у системному вимірі — як феномен, що охоплює не лише сферу державного управління, а й соціальну, культурну, комунікативну площину. Таке трактування надає праву гуманітарного змісту, адже безпека інформаційного простору стає не просто завданням державних інституцій, а справою кожного члена суспільства, який є одночасно споживачем і творцем інформації.

У цьому контексті особливої ваги набуває виявлена авторкою необхідність збереження балансу між принципом свободи інформації та принципом державного захисту. З одного боку, право повинно гарантувати громадянам безперешкодний доступ до інформації та вільне висловлення думок, з іншого — запобігати використанню інформаційних технологій для підриву національної безпеки, поширення ворожої пропаганди, маніпулювання масовою свідомістю. Саме такий баланс є фундаментом демократичного інформаційного суспільства, де свобода не переходить у хаос, а контроль не

вироджується у репресію.

Крім того, у логіці А. Крупнової, важливо підкреслити багатовимірність відповідальності у сфері інформаційної безпеки. Йдеться не лише про юридичну чи адміністративну відповідальність за порушення інформаційного законодавства, а й про етичну, соціальну, професійну відповідальність усіх учасників інформаційного процесу — від журналістів і державних посадовців до пересічних користувачів цифрових платформ. Такий підхід відображає тенденцію до формування нової культури правової свідомості, в основі якої — розуміння інформації як спільного ресурсу, що потребує дбайливого ставлення.

Не менш важливим є третій — глобальний — вимір, який А. Крупнова виводить як завершальний етап у структурі осмислення інформаційної безпеки. Вона слушно зазначає, що в умовах цифрової глобалізації, коли інформаційні потоки перетинають державні кордони, жодна країна не може гарантувати власну інформаційну стабільність ізольовано. Це вимагає від України активного включення до міжнародних ініціатив, координації політики з державами-партнерами, адаптації національного законодавства до стандартів Ради Європи, ЄС, НАТО та інших міжнародних інституцій.

Водночас, авторка обґрунтовує, що імплементація іноземних моделей регулювання не повинна мати механічного характеру. Україна повинна виробляти власну гібридну модель — гнучку, адаптивну і водночас укорінену у національну правову традицію. Це означає, що правове забезпечення інформаційної безпеки має бути водночас універсальним і локальним — таким, що здатне відповідати на глобальні виклики (кіберзлочинність, гібридні війни, інформаційний тероризм) і водночас враховувати внутрішні соціальні реалії.

Таким чином, науковий внесок А. Крупнової полягає не лише у систематизації ключових елементів правового регулювання інформаційної безпеки, а й у формуванні нового типу мислення — інтегративного, міждисциплінарного, стратегічного. Її підхід поєднує юридичну методологію з філософією права, соціологією інформації, теорією держави та управління, що

дозволяє створити розгорнуту доктрину інформаційної безпеки, орієнтовану не лише на сьогодення, а й на перспективу — у напрямку побудови правової, безпечної та етично відповідальної інформаційної держави.

Водночас, проблеми теорії та практики правового (юридичного) регулювання інформаційної безпеки як окремої категорії не завжди є предметом розгляду виключно з позиції тих аспектів, котрі повинні бути враховані під час нормотворчої діяльності.

У праці В. Цимбалюка та А. Бабінської, де останні розглядають проблеми теорії та практики нормативного регулювання інформаційної безпеки в Україні [188, с. 27], увагу спрямовано на дослідження питання упорядкування (унормування) складових реалізації інформаційно-безпекового профілю. Так, власне нормативний кластер розглядається у його взаємозв'язку із інституційним на засадах пошуку оптимальних механізмів реалізації зазначеного співвідношення. Під час останнього, за матеріалами даного дослідження, підлягають урахуванню такі положення та нормативи, як конституційні гарантії громадянина України щодо невтручання в особисте життя та свободу слова (ст. 32, 34 Основного закону) за принципом інтегративної пов'язаності зі сферою інформаційної безпеки, а також – діяльність органів, що покликані забезпечувати інформаційну безпеку України насамперед на внутрішньому рівні – Служби безпеки України (СБУ), Ради національної безпеки і оборони України (РНБО), Міністерства цифрової трансформації України (Мінцифра), Міністерства культури та стратегічних комунікацій України (Мінкульт) та Національної поліції України (Нацполіції).

Розширене осмислення підходів, закладених у зазначеній роботі, дає підстави стверджувати, що автори фактично окреслюють спробу сформувати концептуальну модель багаторівневої взаємодії правових і організаційних інструментів у системі забезпечення інформаційної безпеки. Ідеться не лише про опис функцій відповідних державних інституцій, а й про спробу виявити певну закономірність у співвідношенні нормативних актів, стратегічних

документів і практик їх застосування в умовах динамічної трансформації інформаційного простору. Такий підхід дозволяє розглядати правове регулювання не як замкнену систему норм, а як живий, еволюційний механізм, здатний реагувати на появу нових викликів – від кібератак до інформаційних диверсій, гібридних загроз, маніпуляцій громадською думкою та поширення дезінформації.

Особливої уваги в цьому контексті набуває положення про «інтегративну пов'язаність» конституційних гарантій зі сферою інформаційної безпеки. Воно не лише підкреслює необхідність дотримання основоположних прав людини навіть у межах спеціальних інформаційно-безпекових режимів, а й вказує на потребу в концептуальному узгодженні між безпекою держави та правами громадянина. Інакше кажучи, будь-яка політика чи стратегія інформаційної безпеки повинна виходити з презумпції пріоритету людини як суб'єкта права, що реалізує себе в інформаційному суспільстві. Це накладає додаткову відповідальність на державу як гаранта не лише безпеки, але й довіри до інформаційного простору, у якому громадянин функціонує.

Водночас, наголошується на багатовекторності суб'єктного складу забезпечення інформаційної безпеки. Перелік органів, поданий у дослідженні, демонструє, що сучасна модель інформаційної безпеки в Україні має комплексний характер: вона включає як силовий і аналітичний компоненти (СБУ, РНБО), так і технологічний (Мінцифра), культурно-ціннісний (Мінкульт) та правоохоронний (Нацполіція). Такий підхід можна охарактеризувати як системно-комплементарний, коли кожен із суб'єктів виконує специфічну, але взаємопов'язану роль у структурі загальної безпекової архітектури. Зокрема, СБУ здійснює контррозвідувальні та превентивні заходи щодо кіберзагроз і шпигунства, РНБО координує державну політику в цій сфері, Мінцифра формує цифрову інфраструктуру та впроваджує стандарти кіберзахисту, Мінкульт реалізує гуманітарно-комунікаційний вектор через протидію дезінформації, а Нацполіція забезпечує оперативно-правовий механізм

реагування на порушення.

Крім того, у межах інституційної логіки зазначеного підходу варто розглядати питання міжвідомчої синергії та обміну даними, що стає особливо актуальним в умовах гібридної війни. Інформаційна безпека більше не є сферою, обмеженою технічними чи юридичними параметрами; вона поступово перетворюється на основу національної стійкості, інтегруючи в собі правову, технологічну, політичну та соціальну складові. Звідси випливає потреба у формуванні гнучких, але водночас узгоджених нормативних механізмів, які б дозволили уникнути дублювання повноважень, правової невизначеності чи міжінституційних колізій.

З огляду на зазначене, праця В. Цимбалюка та А. Бабінської становить значний внесок у сучасну доктрину правового регулювання інформаційної безпеки, адже не лише описує поточний стан нормативного поля, а й закладає теоретичні передумови для його подальшого розвитку. Автори фактично окреслюють необхідність переходу від суто формального, декларативного трактування інформаційної безпеки до її концептуального осмислення як цілісної системи, у якій право виступає не лише засобом регламентації, а й інструментом гармонізації суспільних і державних інтересів у межах цифрової епохи.

Повинні зазначити, що особливості правового регулювання забезпечення інформаційної безпеки у контексті державного управління та державного регулювання інформаційної безпеки в Україні станом на сьогодні потребують розгляду не лише за статичним (ідеальним), але й за предметно-реальним виміром координації. Одним із фактів, що прямо та опосередковано детермінує необхідність розгляду проблеми публічного управління українським інформаційно-безпекововим простором, є повномасштабна військова агресія рф проти України від 24.02.2022 р.

Затребуваним та концептуально цінним, на наш погляд, у даному контексті можна вважати аналітичне дослідження О. Каплі [64, с. 17-18], в

якому останній, розглядаючи закономірності регулювання інформаційної безпеки громадянина під час дії воєнного стану в Україні, вивів основні закономірності процесу управління національним інформаційним простором. До таких науковець пропонує відносити пріоритетність загальнонаціональних інтересів на засадах балансування між правами та власне безпекою громадян, превенцію дезінформації та встановлення і запровадження механізмів відповідальності за останню, інституціоналізацію управління інформаційним простором, а також – оперативність управління національним інформаційним простором.

Пріоритетність національних інтересів як фактор-концепцію державного управління та державного регулювання сектору інформаційної безпеки України в умовах протидії неспровокованій російській військовій агресії від 24.02.2022 р. вчений пропонує розглядати з позиції орієнтиру на забезпечення безпеки держави, що, своєю чергою, може призводити до часткових обмежень конституційних прав та гарантій громадян, як-от свобода слова, принцип невтручання в особисте життя тощо [64, с. 18]. Подібна концептуалізація наявна у позиціях законодавця в Указі Президента України № 64/2022 від 24.02.2022 р. Про введення воєнного стану в Україні, про що нами буде означено в другій частині п. 2.2 Розділу ІІ даного дисертаційного дослідження.

В свою чергу, превенцію дезінформації та встановлення і запровадження механізмів відповідальності за останню науковець у вищезазначеному дослідженні розглядає у якості інструмента потенційного контролю за дотриманням інформаційної гігієни в Україні в умовах протидії ворожим російським наративам, політиці дезінформації та ІПСО, що рф активно використовує як елемент дестабілізації внутрішньополітичної та внутрішньосоціальної ситуації в Українській державі [64, с. 18].

Від себе додамо, що наразі даний принцип належним чином не врегульований на законодавчому рівні, адже відповідальність за поширення неправдивих відомостей в Україні наразі не встановлена (ані адміністративна,

ані кримінальна), а єдиним фактом регуляції інформаційного простору з точки зору негативного впливу дезінформаційних даних на останній можемо вважати Проект Закону «Про внесення змін до деяких законодавчих актів України щодо забезпечення національної інформаційної безпеки та права на доступ до достовірної інформації» від 28.01.2020 р., котрий не був схвально сприйнятий засобами масової інформації, а, відтак, залишений на стадії першочергового розгляду.

В той же час, інституціоналізація управління інформаційним простором у праці вищезазначеного дослідника [64, с. 18] пристосовно до протидії російській неспровокованій військовій агресії розглядається як процедура розширення повноважень з контролю за медіа, соціальних мереж, доступу до інформації та комунікаційних каналів державними органами, що відповідають за даний напрям і про які ми зазначали раніше – Служба безпеки України (СБУ), Рада національної безпеки і оборони України (РНБО), Міністерство цифрової трансформації України (Мінцифра), Міністерство культури України (Мінкульт) та Національна поліція України (Нацполіція).

Заключне місце серед перелічених та оглянутих особливостей основних закономірностей процесу управління національним інформаційним простором в Україні в умовах воєнного стану у вищенаведеному дослідженні [64, с. 18] відіграє оперативність управління національним інформаційним простором. Даний сегмент тут розглядається у якості швидкого реагування на інформаційно-просторові виклики та оперативного управління останніми, що базуються на здійснення нормативно-правових (законодавчих) та спеціально-розпорядницьких дій, котрі покликані забезпечувати та реалізовувати основні положення щодо інформаційної стійкості України у період внутрішніх та міжнародних викликів водночас.

Здійснюючи теоретизування та всебічний аналіз особливостей правового регулювання забезпечення інформаційної безпеки у контексті державного управління та державного регулювання інформаційної безпеки крізь власне

нормативну призму, доцільним буде також звернути увагу на публічно-управлінський вимір даного питання на рівні доктринального розуміння. Надалі пропонуємо звернути увагу на наукову позицію А. Русакевича [152, с 178-179], котрий у власному дослідженні сутнісно проаналізував державне регулювання у сфері інформаційної безпеки України в умовах воєнного стану як окремий конструкт. На основі розуміння даного термінологічного феномену ми в подальшому зможемо перейти до висвітлення особливостей правового регулювання забезпечення інформаційної безпеки у контексті державного управління та державного регулювання інформаційної безпеки на законодавчому рівні (аналіз нормативно-правових актів, що забезпечують формування локальної концепції інформаційної безпеки в Україні).

Так, у праці зазначеного науковця під назвою «Інформаційна безпека в умовах воєнного стану у аспекти забезпечення інформаційних прав громадян» [152, с. 179], даний процес розглядається як безпосередньо погоджені та синхронізовані між органами влади дії, спрямовані на захист національного суверенітету, громадянської безпеки та суспільної стабільності одночасно. Інструментарно, зазначений процес здійснюється за допомогою нормативного регулювання, контролю за інформаційним простором, кіберзахисної діяльності та протидії дезінформації та забезпеченню надійної координації між державними органами та суспільством, що сукупно є завданням органів та установ, що виконують та забезпечують державно-владні повноваження та представляють державу у правовідносинах із засобами масової інформації та громадянським суспільством на рівні внутрішньодержавної інформаційно-безпекової політики [152, с. 179-180].

Позиція А. Русакевича має фундаментальне значення, оскільки вперше вітчизняна доктрина розглядає державне регулювання інформаційної безпеки не лише як адміністративно-управлінський процес, а як динамічну, багатокомпонентну систему публічного управління, в якій злиті воєдино політична воля, нормативна база, комунікаційні стратегії та інституційна

практика. Йдеться про перехід від лінійного розуміння «захисту інформації» до цілісної концепції управління інформаційною стійкістю суспільства, де головним критерієм ефективності виступає не обсяг заборон чи контролю, а ступінь гармонізації між безпековими пріоритетами держави та свободами її громадян.

У цьому аспекті, важливо наголосити, що у період воєнного стану інформаційна безпека перестає бути виключно технологічною або нормативною категорією — вона набуває характеру стратегічного ресурсу публічного управління. Держава в таких умовах змушена здійснювати складну балансувальну політику між оперативною потребою обмеження деструктивного контенту й збереженням демократичних стандартів комунікації. Саме тому ключовими інструментами реалізації інформаційно-безпекової політики стають не лише правові акти, але й управлінські рішення, засновані на принципах ризик-орієнтованого підходу, прогнозування та адаптивного реагування.

Також А. Русакевич, на відміну від багатьох попередників, фактично формує новий підхід до розуміння співвідношення державного управління і правового регулювання у сфері інформаційної безпеки: перше визначається ним як організаційно-координаційний механізм, що забезпечує дієвість другого. Іншими словами, право виступає «каркасом» системи, а управління — її «динамічним елементом», здатним забезпечити узгодження між нормами і реальними загрозами, які мають часто асиметричний характер.

Показово, що у наведеній науковій конструкції чітко простежується елемент публічної відповідальності держави перед громадянином — відповідальності не лише за захист, але й за комунікацію, пояснення та залучення суспільства до процесів забезпечення інформаційної безпеки. Це свідчить про зміщення акцентів у сучасному розумінні даної сфери — від авторитарного контролю до демократичного партнерства, від «захисту від» до «захисту через співучасть».

У контексті сучасної України, що перебуває у стані постійного інформаційного протистояння з агресором, наведена концепція набуває особливої актуальності. Вона дозволяє осмислити інформаційну безпеку як складову публічного управління, спрямовану не лише на реагування на загрози, а й на формування стійкої інформаційної культури, що базується на довірі, критичному мисленні та правовій обізнаності громадян. Саме такий підхід забезпечує не тимчасову «обороноздатність» інформаційного простору, а його довгострокову стабільність, що є визначальним чинником національної безпеки загалом.

Зрештою, наукова позиція А. Русакевича відкриває простір для подальшої ревізії доктринального підґрунтя державної інформаційної політики: необхідним є перехід до моделі, у якій державне регулювання не заміщує публічне управління, а виступає його функціональною складовою. Така взаємодія забезпечить реалізацію принципів транспарентності, підзвітності та участі, без яких неможливо побудувати сучасну, демократично легітимну систему забезпечення інформаційної безпеки.

Даний підхід, водночас, не дивлячись на його структурну уніфікованість та узагальнену затребуваність, недостатньою мірою впроваджує механізми задіяння громадянського суспільства у процес моніторингу та регулювання інформаційної безпеки громадян, що потенційно може спричинити недовіру суспільства до державних ініціатив та сприяти поширенню недостовірної інформації – особливо небезпечна модель в умовах воєнного стану та консолідації суспільства на реалізацію та виконання функцій інформаційної та, відповідно, державної (загальнодержавної) безпеки.

Способами, за допомогою яких можна розвинути та належним чином концептуалізувати запропонований А. Русакевичем підхід щодо розуміння державного регулювання у сфері інформаційної безпеки України в умовах воєнного стану саме у сегменті суспільної участі, не дивлячись на певні обмеження прав та свобод, що генерує правовий режим воєнного стану, на наш

погляд, можуть стати інтеграція механізмів громадського контролю, підвищення і прозорість державних заходів у зазначеній сфері та, водночас, залучення незалежних експертів з метою розбудови організаційно-структурного забезпечення даного інформаційно-безпекового сегменту.

Відтепер пропонуємо перейти до безпосереднього аналізу та дослідження особливостей правового регулювання забезпечення інформаційної безпеки у контексті державного управління та державного регулювання інформаційної безпеки з точки зору нормативно-правового інструментарію. В даному випадку, на наш погляд, доцільно брати до уваги положення таких нормативно-правових актів, як Закон України «Про інформацію» № 2657-XII, Закон України «Про доступ до публічної інформації» № 2939-VI, Закон України «Про основні засади забезпечення кібербезпеки України» № 2163-VIII, а також Указ Президента України № 187/2021 «Питання Центру протидії дезінформації», Указ Президента України «Про рішення Ради національної безпеки і оборони України від 15 жовтня 2021 року "Про Стратегію інформаційної безпеки» № 685/2021 та Указ Президента України «Про рішення Ради національної безпеки і оборони України від 14 травня 2021 року "Про Стратегію кібербезпеки України» № 447/2021.

Пропонуємо оглянути положення даних нормативно-правових актів у контексті правового регулювання забезпечення інформаційної безпеки у контексті державного управління та державного регулювання інформаційної безпеки нижче. Так, загальні положення даного законодавчого документа відносно забезпечення інформаційної безпеки України з точки зору спрямування та координації даного процесу на легіслативному рівні відбувається за декількома напрямами – захист національних інтересів, контроль інформаційного простору, протидія дезінформації та правове регулювання моделі інформаційної безпеки України. При цьому, за кожен із вищезазначених напрямів «відповідає» окремо нормативно-правове положення конкретного нормативного документа,, увагу на котрих буде зосереджено

надалі.

Розпочнемо із Закону України «Про інформацію» № 2657-XII [47]. Відповідно до абз. 7 ч. 1 ст. 3 Закону України «Про інформацію» № 2657-XII [47], пріоритетним полем державної інформаційної політики України вітчизняний законодавець визначає забезпечення інформаційної безпеки на національному рівні. У дійсності, зазначена юридична конотація першочергово спрямована на декларування генеральних концептуальних підходів до публічного управління та адміністрування сфери інформації та, як наслідок, обігу даних, проте доцільно відзначити, що вищенаведеним підходом декларується і право, і обов'язок держави здійснювати прямі та поточні дії косметичного та генерального характеру із метою архітектурування внутрішньобезпекової моделі суверенітету. Останній, окрім іншого, має власним складником і інформаційне поле.

Крім цього, концептуалізація захисту національних інтересів як однієї із основоположних інтенцій державної політики у сфері інформаційної безпеки України у Законі України «Про інформацію» № 2657-XII розкривається не лише за предметною, але й за аналогово-правовою структурою. Наприклад, згідно із ч. 1 ст. 5 Закону України «Про інформацію» № 2657-XII [47], котрою де-факто декларовано опцію безальтернативного, повного та всебічного обігу даних всередині держави на засадах відкритості з метою реалізації прав, свобод та законних інтересів як держави, так і громадян, право на інформацію є комплексною феноменологічною категорією, котра передбачає дотримання прав усіх акторів (від англ. actor – учасник), як держава, громадянське суспільство, громадяни, засоби масової інформації та ін.

Враховуючи вищезазначене, можемо говорити про те, що захист національних інтересів в рамках положень Закону України «Про інформацію» № 2657-XII крізь призму формування інформаційної політики підлягає забезпеченню крізь призму контролю та нагляду за політикою інформаційної безпеки України та визначення інформаційної безпеки пріоритетним полем,

зокрема, державного інтересу, що реалізується органами державної влади та органами місцевого самоврядування у рамках власних повноважень.

В свою чергу, такий аспект забезпечення інформаційної безпеки України з точки зору спрямування та координації даного процесу на легіслативному рівні, як контроль інформаційного простору забезпечується одразу двома нормативно-правовими актами – згаданим Законом України «Про інформацію» № 2657-XII та Законом України «Про доступ до публічної інформації» № 2939-VI. Детальніше зупинимося на конкретних положеннях зазначених документів відносно предметного поля нашого дослідження.

Зокрема, відповідно до абз. 5 ч. 1 ст. 6 Закону України «Про інформацію» № 2657-XII [47], гарантування права на інформацію має джерелом та варіацією власного забезпечення, окрім іншого, здійснення державного контролю та громадського контролю за додержанням законодавства про інформацію. Фактично це означає, що інформаційний простір не існує «у відриві» від публічно-управлінських (відповідно, і законодавчих) положень та концепцій, що декларують можливість та реальну опцію залучення громадянського суспільства до процесу формування інформаційного та інформаційно-гігієнічного поля держави.

Доцільно конкретизувати, що здійснення державного контролю та громадського контролю за додержанням законодавства про інформацію як ідеологічно та законодавчо декларований процес не має поширення на узурпацію інформаційного простору та інформаційної політики в Україні. Такі висновки можна зробити на підставі положень ч. 2 ст. 24 Закону України «Про інформацію» № 2657-XII [47], котрими декларується заборона на втручання у діяльність журналістів, діяльність засобів масової інформації та, водночас, встановлюється неприпустимість контролю за змістом інформації, що поширюється, за винятком випадків, коли контроль за поширенням відповідної інформації може мати на меті забезпечення державних інтересів, питань безпеки держави, реалізації її права на державний суверенітет та ін.

В свою чергу, у ст. 3 Закону України «Про доступ до публічної інформації» № 2939-VI [43] встановлено презумпцію, семантичну із зазначеною у ч. 2 ст. 24 Закону України «Про інформацію» № 2657-XII, проте гарантування права на доступ до публічної інформації тут конкретизоване законодавцем шляхом здійснення парламентського, громадського та державного контролю за дотриманням прав на доступ до публічної інформації).

Більш детальне розуміння контролю за забезпеченням доступу до публічної інформації як елементу (складової) контролю за інформаційним простором викладено у ст. 17 Закону України «Про доступ до публічної інформації» № 2939-VI [43].

Відповідно до ч. 1 ст. 17 нормативно-правового акту, контроль за забезпеченням права людини на доступ до інформації в межах парламентської діяльності здійснюється Уповноваженим Верховної Ради України з прав людини, тимчасовими слідчими комісіями парламенту, а також народними депутатами України [43].

Згідно із ч. 2 ст. 17 даного законодавчого документу, забезпечення доступу до публічної інформації розпорядниками перебуває під наглядом громадськості, який реалізується через діяльність депутатів місцевих рад, громадських об’єднань, консультативно-дорадчих органів, а також безпосередньо громадянами, і цей контроль здійснюється шляхом організації громадських слухань, проведення експертних оцінок та інших форм залучення суспільства до моніторингу [43].

Наостанок, у ч. 3 ст. 17 згаданого нормативного документу встановлено презумпцію здійснення державного контролю за забезпеченням розпорядниками інформації доступу до інформації на підставі виключно законодавства та презумпцій, встановлених законодавчими нормами [43].

Отже, на підставі проаналізованих вище особливостей гарантування права на доступ до публічної інформації згідно із Законом України «Про доступ до публічної інформації» № 2939-VI, можемо зробити висновок про

багаторівневість підходу до забезпечення доступу до публічної інформації, що, в свою чергу, дозволяє ефективно поєднати парламентський, громадський та державний контроль, сприяючи реалізації права громадян на інформацію. На наш погляд, даний механізм є ключовим елементом підтримки відкритості, прозорості та підзвітності державних інституцій, що, у свою чергу, посилює демократичні процеси в Україні.

Більш загальні особливості проміжного розуміння контролю інформаційного простору у контексті забезпечення інформаційної безпеки України з точки зору спрямування та координації даного процесу на легіслативному рівні, в свою чергу, включають в себе визначення останнього інструментом забезпечення прозорості й підзвітності суб'єктів інформаційних відносин, що має на меті детінізацію інформації та даних як потенційного активу демократичних видозмін та трансформацій у державі.

Необхідно зазначити, що захист національних інтересів та контроль інформаційного простору як складові частини правового регулювання забезпечення інформаційної безпеки у контексті державного управління та державного регулювання інформаційної безпеки з точки зору нормативно-правового інструментарію не існують окремо від інших кластерних категорій та доповнюються такими процедурними частинами, як протидія дезінформації та правове регулювання моделі інформаційної безпеки України. Відтак, нижче сконцентруємося на дослідженні кореляційного взаємозв'язку між зазначеними елементами вищеокресленої структури формування інформаційно-правової політики в Україні.

Реалізація принципу протидії дезінформації у якості частини правового регулювання забезпечення інформаційної безпеки у контексті державного управління та державного регулювання інформаційної безпеки крізь призму нормативного регулювання являє собою частину національної інформаційної політики України. Юридичне забезпечення зазначеної парадигми формування інформаційного суверенітету національним законодавцем здійснюється на

підставі Закону України «Про основні засади забезпечення кібербезпеки України» № 2163-VIII, а також Указу Президента України № 187/2021 «Питання Центру протидії дезінформації».

У Законі України «Про основні засади забезпечення кібербезпеки України» № 2163-VIII питання протидії дезінформації займає чільне місце та розглядається у декількох проєкціях [51].

По-перше, у п. 9 ч. 1 ст. 7 Закону України «Про основні засади забезпечення кібербезпеки України» № 2163-VIII [51] національним законодавцем презюмовано можливість протидії кіберзагрозам на внутрішньому та міжнародному рівнях шляхом, зокрема, запровадження стандартів інтернаціонального та транскордонного співробітництва у інформаційній сфері. Подібне бачення спрямоване на декларування законодавцем призначення та першочергових інтенцій протидії дезінформації у різних, в тому числі кіберпросторових (цифрових) вимірах, враховуючи динамічність та змінність розвитку джерел інформації та важливість їхнього контролю, нагляду та захищеності для цілей схоронності державного суверенітету станом на сьогодні.

Відповідно до п. 1 ч. 2 ст. 8 Закону України «Про основні засади забезпечення кібербезпеки України» № 2163-VIII [51], однією зі складових забезпечення національної системи кібербезпеки України є протидія зовнішній агресії у кібепросторі. На наше переконання, агресія у кібепросторі є інваріацією агресії проти суверенітету держави, спрямована на розхитування та дестабілізацію внутрішньополітичної ситуації, тому можемо говорити про розуміння кібербезпеки як складової безпеки інформації в державі. Окрім того, кібербезпека держави є проявом та індикатором протидії дезінформації, що здійснює держава за допомогою нормативно-правових та, водночас, інституційних елементів впливу.

У п. 21 ч. 3 ст. 8 та п. 24 ч. 3 ст. 8 Закону України «Про основні засади забезпечення кібербезпеки України» № 2163-VIII [51] зазначено, водночас,

військово-мілітарне призначення протидії дезінформації як акту державно-управлінської діяльності, спрямованого на захист національних інтересів України. Так, протидію кіберзлочинності тут розглянуто у контексті запобігання «розвідувально-підривній, терористичній та іншій діяльності у кіберпросторі, що завдає шкоди інтересам України, використанню мережі Інтернет у воєнних цілях», тоді як нівелювання кібепросторових ризиків за допомогою системи контррозвідувального забезпечення названо елементом забезпечення «внутрішньої та зовнішньої безпеки України». Фактично це означає, що національний законодавець наразі визначає кібербезпеку однією із опорних галузей протидії повномасштабній російській військовій неспровокованій агресії від 24.02.2022 р., а забезпечення даного процесу покладає на національний кібербезпековий апарат (останній у якості суб'єктної складової регулювання інформаційної безпеки в Україні детально розглядатимемо у п. 2.3 Розділу ІІ даного дисертаційного дослідження).

Таким чином, протидія дезінформації як частина державної інформаційної політики, конкретизована у положеннях Закону України «Про основні засади забезпечення кібербезпеки України» № 2163-VIII, має кібербезпековий вимір конкретизації та, відтак, концептуалізується за принципом переходу від частини до цілого, де частиною є власне протидія дезінформації як нормативно-правовий та державотворчий процес, а цілим – національна політика інформаційної безпеки України, однією із частин формування котрої є кіберпростір.

В той же час, реалізація принципу протидії дезінформації як складник правового регулювання забезпечення інформаційної безпеки у контексті державного управління та державного регулювання інформаційної безпеки відповідно до Указу Президента України № 187/2021 «Питання Центру протидії дезінформації» [175] має більшою мірою узагальнений, статично-декларативний характер, проте конкретизує певну «дорожню карту» даного процесу як політичного, публічно-управлінського, ідеологічного та, власне,

нормативного в Україні в умовах сучасних викликів.

У даному випадку сегментарної важливості для цілей нашого дослідження набуває положення п. 1 зазначеного Указу, де протидію дезінфомації крізь призму діяльності Центру протидії дезінформації (ЦПД) ототожнено із запобіганням поточним та прогнозованим загрозам у сфері інформаційної безпеки, що, водночас, становлять інтерес для національних інтересів України [175]. Зазначена законодавча конотація демонструє взаємний зв'язок таких елементів, як протидія дезінформації, інформаційна безпека та національні інтереси України.

Конкретизувавши на авторському рівні дані підходи на предмет встановлення меж та концептуальних особливостей такого поєднання, можемо зазначити наступне : протидія дезінформації є процесом державно-управлінської діяльності, що передбачає законодавчий та інституційний вплив на боротьбу зі спробами зовнішнього ворога дестабілізувати інформаційний фон, інформаційну гігієну в Україні та ін.; інформаційна безпека є сталою константою, результатом діяльності в галузі протидії дезінформації та державного спрямування (координації) інформаційного простору, що визнається частиною державної (національної) безпеки; національні інтереси України є категорією, що систематизує та накопичує в собі елементи національної безпеки, такі як незалежність, суверенітет, територіальна цілісність та, окрім іншого, інформаційна безпека, котра підлягає реалізації та забезпеченню якраз-таки через концептуальний підхід протидії дезінформації.

Заключним елементом формування правового регулювання забезпечення інформаційної безпеки у контексті державного управління та державного регулювання інформаційної безпеки, відповідно поданої нами класифікації, доцільно вважати правове регулювання моделі інформаційної безпеки України. Останнє здійснюється на підставі положень таких нормативно-правових актів, як Указ Президента України «Про рішення Ради національної безпеки і оборони України від 15 жовтня 2021 року "Про Стратегію інформаційної

безпеки» № 685/2021 [174] та Указ Президента України «Про рішення Ради національної безпеки і оборони України від 14 травня 2021 року "Про Стратегію кібербезпеки України» № 447/2021 [173].

Так, в Указі Президента України «Про рішення Ради національної безпеки і оборони України від 15 жовтня 2021 року "Про Стратегію інформаційної безпеки» № 685/2021 [174] в загальному викладено потребу у необхідності формування внутрішньодержавної моделі інформаційної безпеки, здатної реагувати та ефективно кореспондувати на внутрішні та зовнішні інформаційно-безпекові виклики, детерміновані та спровоковані гібридними та прямими втручанням в інформаційну сфері збоку агресора – рф. Таким чином, національний законодавець визначає саме протидію дезінформаційним кампаніям одним із функціональних завдань та функціонально-призначеннєвих елементів управління національним полем безпеки даних, безпеки інформації та, як наслідок, безпеки внутрішнього інформаційного поля.

В той же час, інформаційна безпека у контексті моделювання інформаційно-безпекової архітектури управління на внутрішньодержавному рівні в Україні не існує окремо від власних підвидів, одним із яких, в умовах глобалізації, діджиталізації та інформатизації, доцільно визнати кібербезпеку та її стратегізацію. Нормативно-правовим документом, що здійснює точкову регуляцію даного питання, є Указ Президента України «Про рішення Ради національної безпеки і оборони України від 14 травня 2021 року "Про Стратегію кібербезпеки України» № 447/2021 [173] – у даному законодавчому акті, окрім іншого, концептуалізовано виклики та проблеми, з якими стикається національний кіберпростір в умовах сталого розвитку та, відповідно, запропоновано орієнтири формування моделі інформаційної безпеки України. До неї нележить впровадження інформаційно-технічної кіберзахисної моделі (п. 3 Стратегії), моделі дієвої кібероборони (п. 5 Стратегії) та моделі відносин у кібербезпековій сфері (п. 5 Стратегії).

Інформаційно-технічна кіберзахисна модель та модель дієвої

кібероборони передбачає впровадження інноваційних рішень у Е-галузі, що дозволить максимізувати захищеність державних реєстрів та державних веб-сайтів, офіційних представництв органів державної влади та органів місцевого самоврядування з метою захисту інформації, що становить державну таємницю та має стратегічну важливість для провадження функціонування національної системи державного управління на усіх рівнях та ланках [173].

В свою чергу, модель відносин у кібербезпековій сфері як один із пріоритетних напрямів діяльності у сфері інформаційно-безпекового моделювання передбачає формування та перерозподіл відповідальності між акторами (учасниками) інформаційних та інформаційно-безпекових відносин в Україні на засадах їхньої ефективізації та нівелювання тіньового елементу (сегменту) [173], що є джерелом посилення обороноздатності країни та її інформаційної захищеності як від зовнішніх, так і від внутрішніх загроз.

На підставі вищеопрацьованих даних та юридичних фактів можемо зробити висновок про пов’язаність між інформаційно-безпековою та кібербезпековою стратегізацію як елементами впорядкування та моделювання розвитку інформаційного простору в Україні. У більш генеральному розумінні, усі складові правового регулювання забезпечення інформаційної безпеки у контексті державного управління та державного регулювання інформаційної безпеки перебувають у тісному доповняльному законодавчому та інституційно-доповняльному взаємозв’язку.

На рисунку 2.1 наведено ключові наративи сутнісного взаємозв’язку між зазначеними елементами.

На підставі вищезазначених проаналізованих особливостей та концептуальних підходів до наукового та законодавчого розуміння феномену правового регулювання забезпечення інформаційної безпеки у контексті державного управління та державного регулювання інформаційної безпеки в Україні можемо дійти висновку щодо багатоскладності даного процесу.

Так, повинні відмічати різницю у трактуванні інформаційної безпеки як

складової правового регулювання та теоретичному та, власне, практичному (нормативному) рівні.

Складові правового регулювання забезпечення інформаційної безпеки України : питання співвідношення

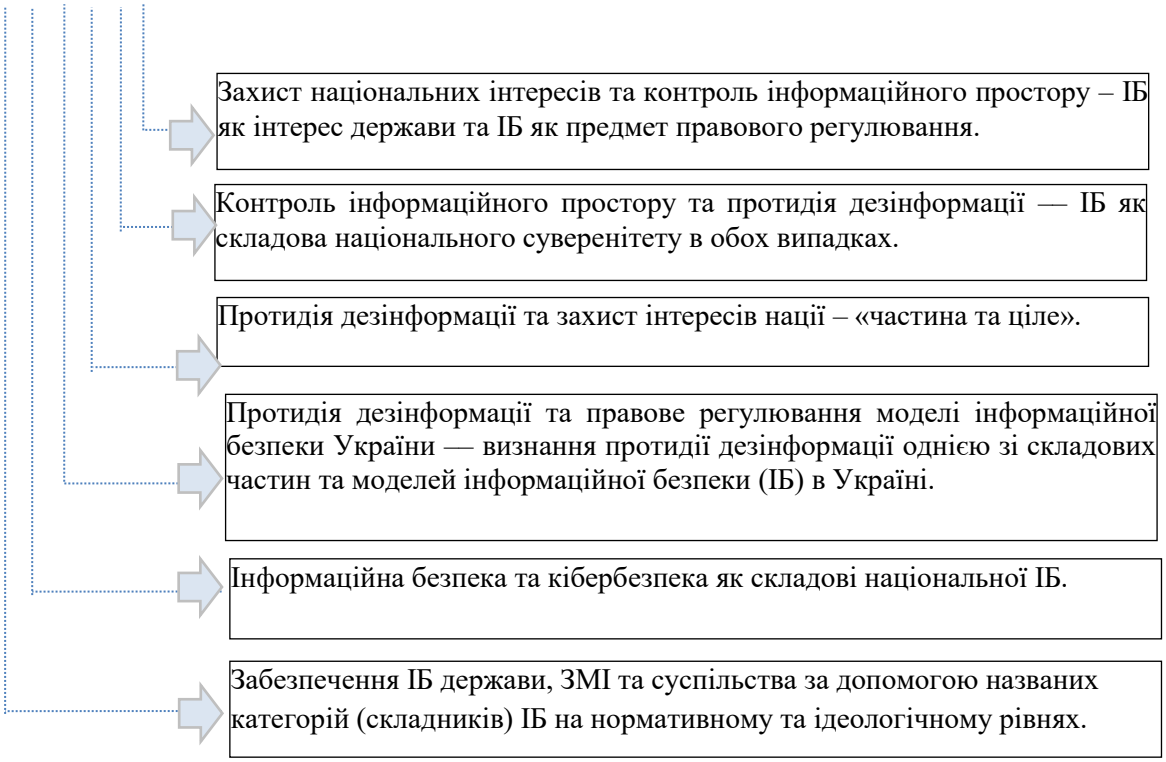

Рисунок 2.1. Складові правового регулювання забезпечення інформаційної безпеки України : питання співвідношення

На теоретичному рівні остання визначається як процес, що формує необхідність національного законодавця дотримуватися таких постулатів під час нормотворчої діяльності, як збереження цілісності та доступності інформаційних ресурсів, захист прав на приватність, свободу слова та доступ до інформації та протидія кібератакам, дезінформації, шпигунству та іншим загрозам.

В цей же час, у нормативно-правовій парадигмі інформаційна безпека та конкретно – інформаційна безпека України розглядається крізь призму таких

складників, як захист національних інтересів, контроль інформаційного простору, протидія дезінформації та правове регулювання моделі інформаційної безпеки України, а легіслативними мірилами забезпечення даних конотацій на нормативно-правовому рівні та, відповідно, агрегаторами становлення культури інформаційної безпеки в Україні та інформаційно-безпекової обороноздатності держави є такі законодавчі документи, як Закон України «Про інформацію» № 2657-XII, Закон України «Про доступ до публічної інформації» № 2939-VI, Закон України «Про основні засади забезпечення кібербезпеки України» № 2163-VIII, а також Указ Президента України № 187/2021 «Питання Центру протидії дезінформації», Указ Президента України «Про рішення Ради національної безпеки і оборони України від 15 жовтня 2021 року "Про Стратегію інформаційної безпеки» № 685/2021 та Указ Президента України «Про рішення Ради національної безпеки і оборони України від 14 травня 2021 року "Про Стратегію кібербезпеки України» № 447/2021.

З огляду на вищенаведене, вбачаємо за доцільне комплексно дослідити підходи протидії загрозам інформаційній безпеці України в розрізі діагностики сучасного стану механізмів реалізації інформаційної безпеки у системі публічного управління України, що і буде здійснено у п. 3.1 Розділу ІІІ даного дисертаційного дослідження.

Висновки до розділу 2

1. Концептуалізовано сутнісне призначення механізму правового регулювання ІБ через: 1) інтеграцію двох ключових функціональних кластерів: регулювання інформаційної діяльності (включно з обов'язком державних органів дотримуватись ІБ-законодавства) та розвиток інформаційного середовища (орієнтація на інновації та формування "інформаційного суспільства"); 2) теоретичне обґрунтування власного підходу до кореляції між

механізмом правового регулювання ІБ та правом людини на інформацію як взаємного забезпечення прав, де реалізація права на інформацію громадян детермінує діяльність інституцій ІБ-парадигми, а інформаційна безпека має на меті конституційну непорушність цього права; 3) систематизації та початкового опису дванáдцяти ключових принципів побудови механізму правового регулювання забезпечення інформаційної безпеки в Україні, які інтегрують правовий, управлінський та технологічний аспекти (законності, захисту прав та свобод людини, національного суверенітету, прозорості, превентивності, технологічної адаптивності, міжвідомчої координації, співпраці та інтеграції, пропорційності, відповідальності, безперервності); 4) концептуалізацію моделі державного управління ІБ в умовах воєнного стану через систематизацію його основних закономірностей (пріоритетність загальнонаціональних інтересів, превенція дезінформації, інституціоналізація та оперативність управління), а також запропоновано шляхи його розвитку шляхом інтеграції механізмів громадського контролю та підвищення прозорості державних заходів для посилення суспільної довіри.

2. Систематизовано та концептуалізовано методологічні засади дослідження інформаційної безпеки у системі публічного управління, що дозволило: розширити та уточнити зміст таких ключових методологічних підходів (системність, міждисциплінарність, комплексність) шляхом додавання до них прогностично-моделювального та кореляційно-взаємодоповнювального елементів, що є критично важливим для аналізу ІБ в умовах динамічних гібридних загроз; науково обґрунтувати та ввести до наукового обігу принципи дослідження інформаційної безпеки (комплексність, прогнозованість та глобальність) у контексті публічного управління, розкривши їхню суть через орієнтацію на майбутні виклики (принцип прогнозованості) та потенційну рецепцію міжнародних стандартів і досвіду (принцип глобальності) у національно-правове та інституційне поле України; актуалізувати застосування філософських основ дослідження ІБ, зокрема, через призму ціннісної

парадигми інформації як активу та діалектичного співставлення категорій «безпека» та «свобода» як конституційно гарантованого прояву інформаційної політики.

3. Поглиблено теоретичні та нормативні засади правового регулювання інформаційної безпеки (ІБ) у системі публічного управління.

Удосконалено доктринальний підхід до розуміння правового регулювання ІБ шляхом виділення та розширення його трьох ключових елементів: аналіз сутності ІБ, розуміння ролі права (через баланс свободи інформації та захисту національних інтересів, а також формування багатовимірної відповідальності) та глобальний контекст (з акцентом на виробленні національної гібридної моделі, що адаптує міжнародні стандарти до внутрішніх реалій).

Концептуалізовано модель державного управління ІБ в умовах воєнного стану через систематизацію його основних закономірностей (пріоритетність загальнонаціональних інтересів, превенція дезінформації, інституціоналізація та оперативність управління), а також запропоновано шляхи його розвитку шляхом інтеграції механізмів громадського контролю та підвищення прозорості державних заходів для посилення суспільної довіри.

Проведено комплексний нормативно-правовий аналіз законодавства України (Закон «Про інформацію», Закон «Про доступ до публічної інформації») у контексті державного управління ІБ, що дозволило чітко розмежувати легіслативні механізми за такими напрямами, як захист національних інтересів та контроль інформаційного простору (зокрема, його багаторівневість: парламентський, громадський, державний контроль) та визначити їхню роль як декларативного права та обов'язку держави на архітектуру внутрішньобезпекової моделі суверенітету.

Обґрунтовано необхідність переходу від суто формального, декларативного трактування правового регулювання до його концептуального осмислення як цілісної, системно-комплементарної архітектури, що інтегрує

силовий, аналітичний, технологічний, культурно-ціннісний та правоохоронний компоненти суб'єктного складу ІБ.

РОЗДІЛ 3
ДІАГНОСТИКА СУЧАСНОГО СТАНУ МЕХАНІЗМІВ РЕАЛІЗАЦІЇ ІНФОРМАЦІЙНОЇ БЕЗПЕКИ У СИСТЕМІ ПУБЛІЧНОГО УПРАВЛІННЯ УКРАЇНИ

3.1. Аналіз підходів протидії загрозам інформаційній безпеці України

Концепції, засоби, методи та механізми протидії загрозам, що виникають в інформаційному просторі України внаслідок цілеспрямованих дій агресора, спрямованих на дестабілізацію функціонування критичних вузлів державного значення (економіка, власне інформаційна галузь, енергетичний сектор) набувають особливої актуальності сьогодні – в умовах великої війни з рф та питань, що ставить перед вищим політичним керівництвом України повоєнна відбудова.

Загалом, методичні підходи до протидії загрозам інформаційній безпеці України можна розподілити, залежно від специфіки застосування останніх вітчизняним публічно-управлінським апаратом, на декілька незалежних, проте взаємодоповнюваних кластерних категорій. Серед них виділяємо використання нормативно-правових та організаційних механізмів забезпечення інформаційної безпеки, застосування технічних засобів та методології кіберзахисту, дбання про інформаційно-психологічну безпеку та протидію дезінформаційним загрозам, використання освітніх ініціатив та підвищення цифрової грамотності населення України та, водночас, інтеграцію міжнародної співпраці у сфері інформаційної безпеки у якості екстрактивного складника національної інформаційної та інформаційно-безпекової політики. Надалі пропонуємо сконцентрувати увагу на особливостях підвищення публічно-управлінської та державної респонсивності до імовірних інформаційних загроз та протидію

останнім пропорційно зазначеним наративним конструкціям.

Ключовим сегментом методичних підходів протидії загрозам інформаційній безпеці України є використання нормативно-правових та організаційних механізмів забезпечення інформаційної безпеки. Даний контекст передбачає, в першу чергу, належне правове регулювання та ефективну роботу відповідних державних інституцій у контексті реалізації (забезпечення) даної мети. Нормативною основою такого процесу є ст. 1 та ст. 17 Закону України «Про національну безпеку України» № 2469-VIII, в яких встановлюються ключові засади та напрями державної політики у сфері захисту національних інтересів, презумпція збереження суверенітету, територіальної цілісності, демократичного устрою країни, а також протидія актуальним і потенційним загрозам; також зазначено, що кібербезпека є невід'ємною складовою загальної системи безпеки держави, а також окреслено функції та відповідальність органів влади, які здійснюють її гарантування та забезпечення.

До додаткового нормативного інструментарію, що являє собою основу формування парадигми державної політики в галузі та сегменті методології підходів протидії загрозам інформаційній безпеці України, також доцільно відносити положення ст. 5 Закону України «Про основні засади забезпечення кібербезпеки України» № 2163-VIII. Тут зазначається, що основні суб'єкти забезпечення кібербезпеки – Кабінет Міністрів України; Рада національної безпеки і оборони України; центральні органи виконавчої влади, що забезпечують формування та реалізацію державної політики у сферах оборони, національної безпеки, захисту інформації та телекомунікацій; Служба безпеки України; Національна поліція України; Національний банк України.

Крім того, відповідно до ст. 10 Закону України «Про основні засади забезпечення кібербезпеки України» № 2163-VIII, визначається необхідність державно-приватного партнерства у сфері кібербезпеки, що має бути інтегрована у контекстах співпраці між державними органами та приватними підприємствами для обміну інформацією про кіберзагрози та спільного

реагування на них у контексті забезпечення інформаційно-безпекових здатностей та респонсивної можливості протидії появі таких.

Однак, не дивлячись на усе вищенаведене, попри наявність законодавчої бази, актуальним залишається питання підвищення ефективності її практичного застосування. Це вимагає розробки підзаконних нормативних актів, що детально регламентують порядок взаємодії суб'єктів, відповідальних за кібербезпеку, а також запровадження дієвих механізмів контролю та оцінки рівня дотримання встановлених норм. Важливим аспектом є зміцнення співпраці між державними структурами, такими як Рада національної безпеки і оборони України, Служба безпеки України, Державна служба спеціального зв'язку та захисту інформації України, Міністерство внутрішніх справ України, що дозволить забезпечити своєчасний обмін критичною інформацією та ефективне реагування на кіберінциденти.

Наступним контекстом реалізації методологічних приписів протидії загрозам інформаційній безпеці України, що потребує нашого аналізу, є, як зазначалося раніше, аспект застосування технічних засобів та методології кіберзахисту. Зазначений кластер носить більшою мірою теоретичний характер, адже не має конкретизованої нормативно-правової регламентації. Тому тут-таки варто говорити радше про методологію, використання котрої може бути застосовним для формування захищеного інформаційного простору в Україні.

Аналізуючи зазначену проблему, українська дослідниця У. Коруц [275, с. 85] зазначила, що компонентом технологічної протидії інформаційним загрозам та загрозам інформаційній безпеці України може бути визначено системи моніторингу та аналізу кіберзагроз, до яких належать рішення класу SIEM (Security Information and Event Management), засновані на здійсненні централізований збір, аналіз та кореляцію подій безпеки в реальному часі, що дозволяє швидко виявляти аномальну активність у корпоративних та державних інформаційних мережах, запобігаючи можливим атакам. Додатковою складовою забезпечення інформаційної безпеки та інформаційної

захищеності можна визначати також застосування систем виявлення та запобігання вторгненням (IDS/IPS), які аналізують трафік та блокують шкідливу активність, захищаючи критично важливі інфраструктурні об’єкти – особливої актуальності це може набувати надалі, в контексті превенції можливих вторгнень чи атак від держави-агресора навіть після виходу воєнних дій в Україні із активної фази воєнного зіткнення, якщо така матиме місце.

У контексті зазначених інтеракційних складників використання Україною аспекту застосування технічних засобів та методології кіберзахисту доцільно говорити про активне розширення міжнародної співпраці у сфері кіберзахисту. Тут наводимо приклади кооперації із такими структурами, як Центр передових технологій кібероборони НАТО (NATO CCDCOE) та команда реагування Microsoft DART (Detection and Response Team), що сутнісно та організаційно сприяє впровадженню передових практик у сфері кібербезпеки, завдяки чому і українські фахівці отримують доступ до новітніх технологій, аналітики щодо актуальних загроз та підтримки у протидії кібератакам (що не було можливим, наприклад, на етапі гібридної та інформаційної війни рф проти України від 2014 р. до 2022 р., – із прикладами, що надавали вище , як НЕК «Укренерго» та кібератаки на енергетичний сектор).

Дбання про інформаційно-психологічну безпеку та протидію дезінформаційним загрозам у якості одного із методів забезпечення інформаційної безпеки України, в свою чергу, концентрується на боротьбі з маніпуляціями та пропагандою, які використовуються для дестабілізації політичної ситуації та зниження довіри до влади. Такий процес, як ми зазначали раніше, може і повинен передбачати у прогностичному розрізі підвищення медіаграмотності населення через освітні програми, а також дії державних органів та установ, що відповідають в Україні за забезпечення інформаційного простору та інформаційної безпеки відповідно – Міністерство культури України, Центр протидії дезінформації (тобто установи, що відання яких належить забезпечення ідеологічного складника інформаційної

стабільності не непідвладності соціального сектору потенційним негативним впливам від держави-агресора). Також, у контексті реалізації зазначеного припису буде доцільним відмітити та нагадати про необхідність матеріального та матеріально-технічного забезпечення функціонування Центру протидії дезінформації та виконання останнім покладених на нього завдань та функцій щодо спростування неправдивої (фейкової) інформації, що вкидається у національний інформаційний простір державою-агресором – інноваційними методами, що можуть бути використані у даному розрізі, доцільно називати програмне забезпечення VoxCheck та StopFake, призначеннєвою функцією котрого є спростування недостовірної інформації, що публікується в режимі онлайн.

Не дивлячись на ідеологічну важливість реалізації та втілення методу дбання про інформаційно-психологічну безпеку та протидію дезінформаційним загрозам у якості одного зі складників інформаційної безпеки України, не менш важливого, на наш погляд, значення у розрізі реалізації інформаційних інтересів України у сегменті протидії та боротьби із наявними чи потенційними загрозами в умовах сьогодення набуває впровадження освітніх ініціатив з метою підвищення цифрової грамотності населення та уміння останнього належним чином обробляти, опрацьовувати та систематизувати наявну інформацію, що пропонується особі до аналізу або котру вона зустрічає на теренах Інтернет-мережі.

Наразі на рівні практичної реалізації у розрізі даного питання в Україні наявна ініціатива, запроваджена у 2021 р. Міністерством цифрової трансформації України – «Дія. Цифрова освіта». Метою останньої є навчання громадян основам цифрової безпеки та основам інформаційної безпеки відповідно у контексті її ґенерування. Стратегічне спрямування таких курсів для широкого кола громадян, в свою чергу, дозволяє мінімізувати ризики, пов’язані з шахрайством в інтернеті, персональними даними, банківськими операціями та інформаційною гігієною.

Водночас, крім узагальненого контексту застосування соціальної орієнтації під час реалізаційного забезпечення методу дбання про інформаційно-психологічну безпеку та протидію дезінформаційним загрозам у якості одного зі складників інформаційної безпеки України, варто говорити про безпосередній навчально-процесний. Останній, зокрема, повинен передбачати певні ініціативні стартапи щодо інтеграції медіаграмотності та цифрової грамотності у якості навчальних дисциплін у закладах вищої освіти (ЗВО) та, зокрема, школах, чого наразі, на жаль, не наявно у достатніх обсягах.

Водночас, застосовним та ефективним концептуальним підходом, що наразі використовується у системі закладів вищої освіти України та потребує подальшого експансіювання з метою захисту національного інформаційного простору, є моніторинг останнього закладами вищої освіти на засадах його спрямування та координації. Наприклад, блокування месенджера «Telegram» у якості основного джерела обміну інформації даними серед науково-педагогічних працівників університету було запроваджено у низці закладів вищої освіти, таких як Київський національний університет імені Т. Шевченка, Київський авіаційний інститут (раніше – Національний авіаційний університет), що узагальнено свідчить про роботу над висвітленням інформаційної відкритості та позбавленням інформаційної незахищеності, зокрема, на рівні освітнього сектору. Поміж тим, вищенаведений підхід відзначається також яскравим ідеологічним наповненням, адже у такий спосіб Міністерство освіти і науки України та безпосередньо заклади освіти дбають про збереження інформаційної автентичності та недопущення толерування студентством як проактивно-розвитковим кластером майбутнього Української держави, неправдивих (фейкових) новин та інформації.

Розглядаючи питання використання методологічного інструментарію в Україні з метою позитивного впливу на інформаційний простір та, зокрема, забезпечення його здатності реагувати на виклики та подразники у вигляді внутрішньо-, зовнішньополітичних, безпекових та економічних фактів,

доцільно звертати увагу не лише на локальну політику забезпечення інформаційної стабільності, а й на інтеграцію міжнародної співпраці у сфері інформаційної безпеки у якості екстрактивного складника національної інформаційної та інформаційно-безпекової політики України.

Нормативною рамкою для реалізації концепції інтеграції міжнародної співпраці у сфері інформаційної безпеки у якості екстрактивного складника національної інформаційної та інформаційно-безпекової політики України у її міжнародному вимірі є положення Угоди про асоціацію з ЄС від 21.03.2014 р. (із подальшими змінами). Відповідно до пп. f) п. 2 ст. 22 Розділу III (Юстиція, свобода та безпека) зазначеного документу, злочинність у інформаційному просторі та, зокрема, прояви кіберзлочинності є предметним об'єктом взаємодії України із країнами-членами ЄС [405]. Фактично це означає, що інформаційна безпека та методи її забезпечення в Україні в умовах євроінтеграційного поступу, що, окрім іншого, включає інкорпоративне вирішення безпеково-інформаційних питань, має полем власної ґенерації постійне співробітництво та взаємодію із європейськими партнерами для рецепції дієвих, застосовних у інформаційно-правовому вимірі практик, спрямованих на протидію посяганням на національну інформаційну інфраструктуру.

Окрім власне нормативно-правової рамки та деяких раніше розглянутих проявів взаємодії України у даному сегменті на міжнародно-правовому рівні із Центром передових технологій кібероборони НАТО (NATO CCDCOE) та команда реагування Microsoft DART (Detection and Response Team), також звертаємо увагу на використання у даному розрізі додаткових елементів забезпечення національної інформаційної стабільності.

Так, у 2022 році Українська держава офіційно долучилася до європейської ініціативи щодо кіберзахисту Cyber Rapid Response Teams and Mutual Assistance in Cybersecurity (CRRTs), що передбачає залучення висококваліфікованих фахівців для надання допомоги у разі масштабних кібератак. Зазначена ініціативна робота, на додаток, доповнюється інтеграцією

в EU Cybersecurity Competence Network, яка об’єднує провідні дослідницькі установи та експертів з кібербезпеки у Європі з метою консолідації процедури обміну досвідом та впровадженню передових технологій захисту.

В свою чергу, окремим стратегічним напрямом міжнародної взаємодії України у розрізі забезпечення інформаційної сталості та інформаційної безпеки в сегменті протидії наявним загрозам є співробітництво з провідними світовими IT-компаніями, як-от Google, Amazon, Microsoft, Cisco. Завдяки останній Україна отримує доступ до інноваційних рішень у сфері кіберзахисту, зокрема до інструментів моніторингу загроз, передових аналітичних систем та хмарних технологій, котрі сприяють убезпеченню державних інформаційних ресурсів від незаконних посягань та протиправних інформаційно-кібернетичних атак. Наприклад, Microsoft забезпечує надання технологічної підтримки, допомагаючи ідентифікувати та аналізувати потенційні кібератаки, Google реалізовує проєкти, спрямовані на підвищення стійкості кіберінфраструктури державних органів та засобів масової інформації, тоді як компанія Amazon Web Services (AWS) у 2022 році сприяла перенесенню критично важливих українських даних у хмарні сховища, що дозволило запобігти їхній втраті через російські кібератаки.

Ще одним важливим аспектом міжнародного партнерства є інтеграція України в глобальні системи обміну даними про кіберзагрози. Одним із ключових інструментів у цій сфері стала платформа MISP (Malware Information Sharing Platform), яка забезпечує оперативний обмін інформацією про новітні кіберінциденти та вразливості, що можуть бути використані, зокрема, державою-агресором під час конструювання потенційних кібератак. Відмітимо, що до даного співробітництва залучається профільний орган забезпечення інформаційної стійкості та інновацій у галузі інформаційного простору – Міністерство цифрової трансформації України (Мінцифра), що сукупно дозволяє створити прецедент координації національної інформаційної респонсивностіу світлі протидії відповідного рівня та ґенерації загрозам.

Використання цього ресурсу сприяє підвищенню ефективності реагування на загрози, вдосконаленню методів нейтралізації атак та посиленню загальної кіберстійкості держави.

У процесі систематизації та конкретизації методичних підходів протидії загрозам інформаційній безпеці України доцільно, окрім власне контекстів забезпечення даного процесу як феномену та явища (розглянуті вище), побічно акцентувати увагу на проблематиці даного питання, що потребує подальших розробок та напрацювань задля його врегулювання.

Зокрема, ефективній нейтралізації загроз інформаційній безпеці України бракує комплексного підходу, що охоплює правове регулювання, технічні рішення, організаційні стратегії та освітні ініціативи. Повинні констатувати, що сучасна система кіберзахисту України має низку недоліків, які вимагають системного вдосконалення на ідеологічному, процедурному та практично-прикладному рівнях.

Передусім, хоча нормативно-правова база в Україні розвинена, вона залишається неповною та недостатньо адаптованою до швидко змінюваного характеру кіберзагроз. Відсутність ефективних механізмів імплементації окремих норм Законів України «Про національну безпеку» № 2469-VIII та «Про основні засади забезпечення кібербезпеки України» № 2163-VIII ускладнює координацію між відповідальними державними структурами. Необхідно розробити деталізовані підзаконні акти, які регламентуватимуть алгоритми реагування на кіберінциденти та порядок взаємодії між Радою національної безпеки і оборони України (РНБО), Службою безпеки України (СБУ), Держспецзв’язку та Міністерством внутрішніх справ України (МВС).

Крім того, технічний рівень захисту критичної інфраструктури потребує суттєвої модернізації. Використання застарілих рішень, відсутність широкого впровадження технологій штучного інтелекту для моніторингу загроз, автоматизованих систем кіберзахисту та блокчейн-платформ для безпечного збереження державних реєстрів створює значні ризики – тож, предметної

необхідності набуває посилення акцент на впровадженні прогнозних та превентивних механізмів захисту.

Окремою проблемою залишається недостатній рівень цифрової грамотності населення. Попри розвиток освітніх ініціатив, таких як онлайн-курси з кібербезпеки «Дія. Цифрова освіта», їхній вплив наразі є обмеженим та партикулярно-поодиноким. Доцільним кроком є інтеграція обов'язкових навчальних модулів із кібергігієни у шкільні програми та навчальні програми у закладах вищої освіт (ЗВО), підготовка держслужбовців та регулярні тренінги для працівників критичної інфраструктури.

Ще один стратегічний аспект – розширення міжнародної співпраці. Незважаючи на прогрес у співпраці з НАТО, ЄС та технологічними корпораціями, Україна має посилити свою присутність у глобальних кібербезпекових ініціативах. Зокрема, варто розширювати участь у міжнародних кібернавчаннях, інтегруватися у платформи обміну інформацією про загрози та налагоджувати глибшу взаємодію з міжнародними кіберцентрами.

Отже, для підвищення рівня захисту інформаційної безпеки необхідно удосконалювати законодавчу базу, впроваджувати передові технологічні рішення, покращувати рівень цифрової освіти та розширювати міжнародне співробітництво, що сукупно стане джерелом формування надійного фундаменту для формування стійкої системи кіберзахисту Української держави та, як наслідок, Української нації.

Сукупно та узагальнено, аналіз та доктринальне опрацювання проблематики та феномену використання методичні підходи протидії загрозам інформаційній безпеці України з метою забезпечення інформаційної сталості та прогностичної стійкості держави дозволили дійти наступних проміжних висновків.

В першу чергу, серед методичних підходів протидії загрозам інформаційній безпеці України виділяємо використання нормативно-правових

та організаційних механізмів забезпечення інформаційної безпеки, застосування технічних засобів та методології кіберзахисту, дбання про інформаційно-психологічну безпеку та протидію дезінформаційним загрозам, використання освітніх ініціатив та підвищення цифрової грамотності населення України та, водночас, інтеграцію міжнародної співпраці у сфері інформаційної безпеки у якості екстрактивного складника національної інформаційної та інформаційно-безпекової політики. Кожен із зазначених кластерів являє собою інструмент, спосіб, засіб та механізм реалізації концепції відкритого інформаційного суспільства в Україні із захищеним інформаційним простором – усе це в умовах глобальних викликів.

По-друге, забезпечення інформаційної безпеки України має декілька інноваційних сегментів впровадження. Першим з них варто називати галузь освіти у якості отримання відповідних знань (питання цифрової освіти «Дія. Цифрова освіта» для населення та цифрової освіти для здобувачів освіти), другим, що доповнює перший – запровадження інформаційної гігієни та цифрової грамотності безпосередньо на рівні закладів вищої освіти (ЗВО) шляхом встановлення певних правил користування інформаційними джерелами та інформаційними ресурсами (ідеологічний складник та безпековий складник одночасно – прикладом є заборона використання месенджеру Telegram у публічно-професійних потребах).

По-третє, найбільшого рівня проблемності у контексті дослідження аспектів реалізації принципів інформаційної безпеки України на методологічному рівні набуває налагодження процесу інституційної взаємодії між Радою національної безпеки і оборони України (РНБО), Службою безпеки України (СБУ), Держспецзв’язку та Міністерством внутрішніх справ України (МВС) відповідно нормативно визначеного кола їхньої компетенції.

3.2. Функціональний аналіз суб'єктів забезпечення інформаційної безпеки України в сучасних умовах

Інформаційна безпека є фундаментальним чинником національної безпеки України, оскільки сучасні загрози в цифровому середовищі здатні суттєво впливати на стабільність державних інституцій, економічний розвиток, обороноздатність та соціальну згуртованість. Стрімке розширення цифрових технологій і глобальна цифровізація створюють не лише нові можливості, а й низку серйозних викликів, пов'язаних із кіберзагрозами та захистом критичних інформаційних ресурсів.

Формування ефективної системи забезпечення інформаційної безпеки України передбачає впровадження системного підходу, що базується на чіткій взаємодії та розподілі функцій між державними структурами, приватними компаніями, громадським сектором і міжнародними організаціями. Кожен із цих суб'єктів відіграє визначальну роль у розбудові дієвої стратегії інформаційного захисту, запобіганні кібератакам і протидії маніпулятивним інформаційним кампаніям.

Актуальність та затребуваність функціонального аналізу суб'єктів забезпечення інформаційної безпеки України в сучасних умовах, окрім іншого, детермінована наявністю широкого кола інформаційних загроз, поширення дезінформації та зростаючої кількості кібератак, що своєю чергою потребує удосконалення законодавчої бази й технічний захисту, як і встановлення ефективні механізмів координації між усіма учасниками процесу. Сукупно, подібний процес вимагає застосування комплексного підходу до забезпечення інформаційної безпеки та має спрямовуватися на охоплення не лише використання технологічних інструментів для захисту даних, а й формування культури кібергігієни, поєднаного із підготовкою кваліфікованих фахівців у сфері кібербезпеки, та проактивною інтеграційною діяльністю відносно залучення України у глобальні ініціативи з протидії кіберзлочинності.

Нижче розглядатимемо концепт функціонального аналізу суб'єктів забезпечення інформаційної безпеки України в сучасних умовах крізь призму дослідження таких окремих, проте взаємопов'язаних між собою кластерів – державні органи як головні суб'єкти інформаційної безпеки, приватний сектор як учасник інформаційної безпеки, громадський сектор та медіа, а також – міжнародна співпраця у сфері інформаційної безпеки.

Першим та, водночас, основоположним у стратегічному вимірі та вимірі інституційного забезпечення сталого функціонування інформаційного простору України доцільно називати якраз-таки роль державних органів як головних суб'єктів інформаційної безпеки України, кожен із яких має свою, чітко визначену та чітко встановлену компетенцію. До таких органів (державних суб'єктів) належать Служба безпеки України (СБУ), Рада національної безпеки і оборони України (РНБО), Міністерство цифрової трансформації України (Мінцифра), Національна поліція України (Нацполіція) та Міністерство культури України (Мінкульт).

Так, законодавча кореляція між діяльністю Служби безпеки України (СБУ) та її компетенцією щодо забезпечення інформаційної безпеки України наявна у ст. 10 Розділу ІІ Закону України «Про службу безпеки України» № 2229-XII. Тут законодавцем зазначено, що центральним управлінням Служби безпеки України у якості одного із елементів системи організації діяльності даного органу може бути здійснено заходи щодо контррозвідувального захисту інтересів держави у сфері інформаційної безпеки.

Також потрібно відмітити, що свою діяльність Служба безпеки України (СБУ) як найвищий у ієрархії забезпечення інформаційної безпеки орган державної (публічної) влади провадить не персонально, а у тісному взаємозв'язку та на засадах взаємодії із іншими органами державної влади, а саме – Радою національної безпеки та оборони України (РНБО), Міністерством цифрової трансформації України (Мінцифрою) та Національною поліцією України (Нацполіцією).

Повноваження та компетенція Ради національної безпеки та оборони України (РНБО) у контексті забезпечення інформаційної безпеки України концептуалізуються відповідно до галузевого Закону України «Про Раду національної безпеки та оборони України» № 183/98-ВР [53], що визначає коло компетенції органу в усіх сферах державного спрямування та координації, включно із інформаційною.

Так, згідно із абз. 2 п. 1 ч. 1 ст. 4 Закону України «Про Раду національної безпеки та оборони України» № 183/98-ВР [53], компетенція Ради національної безпеки та оборони України поширюється, зокрема але не виключно, на сферу протидії порушень стратегічних національних інтересів держави в інформаційній сфері, що є одним зі складників національного благоденства та розвиткової стабільності.

В свою чергу, відповідно до абз. 7 п. 1 ч. 1 ст. 4 Закону України «Про Раду національної безпеки та оборони України» № 183/98-ВР [53], національним законодавцем презюмується опція діяльності Ради національної безпеки і оборони України на засадах проведення (здійснення) заходів інформаційного характеру з метою масштабування потенційних та реальних загроз у даній сфері у їхньому глобальному вимірі.

Сукупність зазначених наукових конотацій щодо розуміння повноважень Ради національної безпеки та оборони України (РНБО) у індивідуальному вимірі та поєднанні із компетенцією Служби безпеки України (СБУ) дозволяє говорити про спрямованість на координацію національного інформаційного простору, проте, якщо Рада національної безпеки та оборони України проводить радше поточні заходи зі стабілізації національної безпекової карти та парадигми держави, то Служба безпеки України здійснює контроль за діяльністю органів, що знаходяться відносно неї нижче за юрисдикцією.

Особливість Ради національної безпеки та оборони України (РНБО) у даному сегментарному співвідношенні полягає в тому, що інформаційна безпека як предмет регулювання, як і у випадку зі Службою безпеки України

(СБУ), розглядається крізь призму глобального національного інтересу держави, що полягає у ототожненні національної безпеки із безпекою інформації та, як наслідок, захищеністю державних ресурсів від потенційних атак та нападів (посягань) гібридної генерації.

Сутнісного значення у контексті раніше згаданої взаємодії зі Службою безпеки України (СБУ) набувають положення та компетенція щодо формування підвалин інформаційної безпеки в Україні Міністерства цифрової трансформації України (Мінцифри). Діяльності останньої як суб'єкта забезпечення інформаційної безпеки регламентується безпосередньо Постановою КМУ № 856 від 18.09.2019 р. Питання Міністерства цифрової трансформації [146].

Першочергово має зауважити, що роль та місце Міністерства цифрової трансформації (Мінцифри) у формуванні національної архітектури інформаційної безпеки формується на основі та підставі необхідності балансування та впорядкування даних та інформаційних систем в умовах глобалізації, інформатизації та діджиталізації. Це стосується як джерел інформації, що мають на меті власне обробку та систематизацію даних приватної ґенези, так і даних, що містять конструктивно важливі для функціонування державного апарату дані (як-от державна таємниця та ін.).

Уже в п. 1 Постанови КМУ № 856 від 18.09.2019 р. Питання Міністерства цифрової трансформації [146] можна знайти концептуальний підхід до формування стратегії залучення Мінцифри до створення засад інформаційної безпеки держави, адже тут національний законодавець згадує про дві інтенційні напрями діяльності органу, пристосовних до даного сегменту – розвиток інформаційного суспільства та національних електронних інформаційних ресурсів.

Також звертаємо увагу на положення пп. 9-7 п. 4 Постанови КМУ № 856 від 18.09.2019 р. Питання Міністерства цифрової трансформації [146]. Тут сформовано парадигму участі Мінцифри в процесах та процедурах взаємодії

органів державної влади (органів публічної влади). Така діяльність, зокрема, стосується ведення інформаційної взаємодії між зазначеними суб'єктами, а також – функціонування електронних реєстрів публічної формації.

Відтак, взаємозв'язок між повноваженнями та діяльністю Мінцифри, а також Службою безпеки України (СБУ) та Радою національної безпеки та оборони України (РНБО) доцільно виводити за тривимірною архітектурною моделлю.

Першим кластером зазначеного співвідношення, на наш погляд, доцільно визнати кореляційний зв'язок між власне повноваженнями Служби безпеки України (СБУ) в контексті масштабного моніторингу інформаційно-безпекового поля в Україні та, зокрема, повноваження Мінцифри щодо сприяння у проведенні такого моніторингу. Наприклад, видається затребуваною та застосовною опція документування та детекції правопорушень у сфері інформаційної безпеки органами державної влади та органами місцевого самоврядування Мінцифру (враховуючи абсолютне право останньої на організаційне впорядкування державних реєстрів відповідно до пп. 9-7 п. 4 Постанови КМУ № 856 від 18.09.2019 р. Питання Міністерства цифрової трансформації [146], котра підсумково підлягає комплексному доповненню згідно із повноваженнями Служби безпеки України (СБУ) щодо беззастережного контролю за виконанням приписів відносно уніфікованого формування безпечного та обороноздатного інформаційного простору.

Другим кластером співвідношення, на котрому ми акцентували увагу вище, є уніфікований статус Ради національної безпеки та оборони України (РНБО) щодо формування безпекового національного простору в усіх сферах, зокрема, і у галузі національної інформаційної безпеки. За таких умов, взаємодія зі Службою безпеки України (СБУ) виступає додатковим доповняльним елементом архітектурування простору національної інформаційної безпеки, а діяльність Мінцифри фактично уніфікує можливість впровадження концепцій інформаційної безпеки за допомогою інформаційно-

комунікаційних технологій (ІКТ) та ін.

Третім, і заключним, елементом кореляційної взаємодії формату «Служба безпеки України (СБУ), Рада національної безпеки та оборони України (РНБО) та Міністерство цифрової трансформації України (Мінцифра)» функціонування усіх трьох вищезазначених інституцій безпосередньо в інтересах інформаційної безпеки України та, як наслідок, національної безпеки України в генеральному розумінні даного терміну. Вищезазначений аналіз підводить до висновку, що діяльність зазначених органів є механізмом забезпечення інформаційної безпеки України, внаслідок чого зазначені органи публічної влади можуть бути визнані системою суб'єктів, відповідальних за національну інформаційно-безпекову політику.

Радше факультативного значення у контексті огляду суб'єктного складу забезпечення інформаційної безпеки України, водночас, набуває аналіз компетенції Національної поліції України (Нацполіції). Зазначимо водночас, що даний орган та його діяльність у контексті формування архітектури інформаційно-безпекового середовища сутнісно доповнюють взаємозв'язок формату «Служба безпеки України (СБУ), Рада національної безпеки та оборони України (РНБО) та Міністерство цифрової трансформації України (Мінцифра).

Керівним нормативно-правовим актом, котрим визначаються особливості реалізації практичних категорій інформаційної безпеки Національною поліцією України (Нацполіцією) на практиці, є Закон України «Про Національну поліцію України» № 580-VIII [50]. Опосередкований вплив діяльності Національної поліції України (Нацполіції) на реалізаційне забезпечення заходів публічного управління та адміністрування інформаційно-безпекового характеру наявний у ст. 28 Розділу IV зазначеного вище нормативно-правового акту, де національний законодавець відмічає участь Нацполіції у притягненні до відповідальності винних за порушення використання інформаційних ресурсів у випадках, коли це, зокрема, мало наслідком порушення прав, свобод, інтересів

людини та ін. Доцільно зауважити, що для цілей даної статті порушення використання інформаційних ресурсів, згідно із диспозицією, полягає у несанкціонованому використанні інформаційних систем, інформаційних ресурсів та інформаційно-комунікаційних систем (ІКТ) водночас.

На підставі досліджених особливостей ролі та місця Служби безпеки України (СБУ), Ради національної безпеки та оборони України (РНБО), Міністерства цифрової трансформації України (Мінцифри) та Національної поліції України (Нацполіції) у системі забезпечення інформаційної безпеки, можемо сформувати декілька проміжних концептуальних висновків.

Служба безпеки України (СБУ), Рада національної безпеки і оборони України (РНБО), Міністерство цифрової трансформації України (Мінцифри) та Національна поліція України (Нацполіція) є ключовими елементами державної системи забезпечення інформаційної безпеки, кожен із яких виконує важливу і специфічну роль у цьому процесі. СБУ виступає основним суб'єктом, відповідальним за протидію кіберзагрозам, захист державних інформаційних ресурсів і виявлення деструктивної діяльності у сфері інформації, а також координує заходи з боротьби з дезінформацією та пропагандою. РНБО забезпечує стратегічне планування, формує політику національної безпеки, включно з інформаційною сферою, та координує роботу всіх суб'єктів, задіяних у забезпеченні інформаційної безпеки.

Мінцифра, у свою чергу, є провідним органом, який розвиває інфраструктуру цифрової безпеки, впроваджує сучасні технології захисту даних, забезпечує розвиток кіберграмотності та реалізує державну політику у сфері цифровізації. Національна поліція зосереджена на розслідуванні правопорушень у сфері інформаційної безпеки, зокрема злочинів, пов'язаних із кібератаками, шахрайством та несанкціонованим доступом до інформаційних систем.

Таким чином, діяльність цих органів є взаємодоповнюючою та спрямованою на створення цілісної системи протидії сучасним загрозам в

інформаційному просторі України. Координація їх зусиль забезпечує надійний захист національних інтересів у цифровій епосі та зміцнює безпеку держави в умовах гібридних загроз.

Окрім діяльності органів, компетенція котрих у аспекті забезпечення інформаційної безпеки України полягає у спрямуванні та координації власне державно-управлінського механізму зазначеного процесу, надалі доцільно сконцентруватися на окресленні «соціального» наративу реалізації інформаційно-безпекової моделі крізь призму діяльності Міністерства культури та стратегічних комунікацій України (Мінкульту).

Юридична (нормативно-правова) складова діяльності Міністерства культури та стратегічних комунікацій України (Мінкульту) розглянута та конкретизована національним законодавцем у Постанові КМУ № 885 від 16.10.2019 р. Деякі питання діяльності Міністерства культури та стратегічних комунікацій [147].

Так, у абз. 3 пп. 1 п. 3 Постанови КМУ № 885 від 16.10.2019 р. Деякі питання діяльності Міністерства культури та стратегічних комунікацій [147] до основних цілей, завдань та функцій Мінкульту віднесено культивацію інформаційної політики України та, зокрема, інформаційної безпеки України як її складника.

Також, відповідно до пп. 5 п. 4 Постанови КМУ № 885 від 16.10.2019 р. Деякі питання діяльності Міністерства культури та стратегічних комунікацій [147], до прямих повноважень Мінкульту належить нормативно-правове регулювання у сфері інформаційної політики України. При цьому, у пп. 8 п. 4 Постанови КМУ № 885 від 16.10.2019 р. Деякі питання діяльності Міністерства культури та стратегічних комунікацій [147], національний законодавець відносить до кола компетенції Мінкульту пріоритезацію та перспективне рамкування інформаційно-безпекової галузі України, а пп. 131 п. 4 даного нормативного акту встановлює презумпцію методико-практичної допомоги Мінкульту в галузі архітектування інформаційної безпеки.

Кореляційний зв’язок між інформаційною безпекою та національною безпекою як взаємопов’язаними складниками державного управління, водночас, систематизований у пп. 154 п. 4 Постанови КМУ № 885 від 16.10.2019 р. Деякі питання діяльності Міністерства культури та стратегічних комунікацій [147], де інформаційно-культурні інтереси України віднесені національним законодавцем до структури зміцнення національно-безпекового державного профілю.

Другою кластерною категорією забезпечення інформаційної безпеки України у функціонально-суб’єктному вимірі, як ми зазначали раніше, є приватний сектор. На відміну від державного сектору, діяльність котрого має пряме юридичне спрямування та координацію в контексті інформаційно-безпекового архітектування, приватний сектор як суб’єкт забезпечення інформаційної безпеки та захищеності України, що виконує функцію реалізації інтересів держави у даному сегменті на засадах наявності більшого рівня кон’юнктурності арсеналу засобів, згаданий національним законодавцем лише у ст. 10 Закону України «Про основні засади забезпечення кібербезпеки України» № 2163-VIII [51], де юридично визначається необхідність державно-приватного партнерства у сфері кібербезпеки, що має бути інтегрована у контекстах співпраці між державними органами та приватними підприємствами для обміну інформацією про кіберзагрози та спільного реагування на них у контексті забезпечення інформаційно-безпекових здатностей та респонсивної можливості протидії появі таких.

Більшою мірою теоретичні напрацювання українських науковців [202] розкривають положення щодо етимології даного процесу в контексті реалізації інформаційно-безпекових цілей. Суб’єктами реалізації інформаційно-безпекових завдань відповідно положень ст. 10 Закону України «Про основні засади забезпечення кібербезпеки України» № 2163-VIII, таким чином, запропоновано вважати ІТ-компанії та операторів зв’язку (захист національних інформаційних мереж здійснюється через комплекс заходів із забезпечення

кібербезпеки, зокрема завдяки діяльності інтернет-провайдерів, які відстежують потенційні загрози, обмежують доступ до шкідливого контенту та впроваджують системи кібермоніторингу для виявлення й нейтралізації кібератак), фінансові установи (реалізують комплексні заходи для запобігання фінансовому шахрайству, кібератакам на банківські системи та несанкціонованому розголошенню конфіденційної інформації), а також – експертні центри та аналітичні установи (наприклад, українські кіберакадемії), що реалізують власні повноваження із забезпечення інформаційної безпеки України шляхом здійснення оцінки рівня захищеності, підготовки детальних аналітичних висновків та формування пропозицій щодо зміцнення інформаційної безпеки країни.

Категорія громадського сектору та медіа у якості суб'єктів забезпечення інформаційної безпеки України в сучасних умовах, в свою чергу, являє собою потужний інструмент викриття інформаційних маніпуляцій, боротьби з фейковими новинами та інформаційною гігієною населення. Медіа в даному випадку відповідають за протидію пропаганді від держави-агресора, нівелювання та попередження проявів дезінформації та створення якісного контенту всередині держави, що відповідатиме критеріям інформаційної безпеки та інформаційної гігієни в реаліях воєнного часу та викликів повоєнної відбудови, з якими стикнеться Українська держава [202, с. 95].

У вищезазначеному розрізі також необхідно звертати увагу на видозміни національного законодавчого поля. Так, наприкінці 2022 р. де-факто на виконання плану євроінтеграційного поступу України та виконання положень ст. 396 Глави 15 Розділу V (Економічне та галузеве співробітництво) Угоди про асоціацію з ЄС від 21.03.2014 р. (із подальшими змінами) було прийнято Закон України «Про медіа» № 2849-IX, що фактично перепрофілював роль та місце засобів масової інформації (ЗМІ) у конструюванні інформаційної безпеки шляхом надання оперативної, достовірної інформації населенню та взаємодії з ним. Звертаємо, зокрема, увагу на ст. 36 документу, в котрій питання

інформаційної безпеки держави запропоновано реалізувати крізь призму встановлення обмежень щодо змістовно-інформаційного наповнення. Дані норми забороняють розповсюдження через медіа та платформи з відкритим доступом до відеоконтенту матеріалів, що містять пропаганду насильницького повалення конституційного ладу, заклики до ведення агресивної війни, посягання на територіальну цілісність України чи інші загрози національній безпеці.

Тобто, можемо говорити про універсальну роль громадянсько-медійної взаємодії в Україні у контексті реалізації національних соціально-суспільних, політичних, владних та, власне, інформаційних інтересів держави. Інтеграція зазначених положень у суспільне життя передбачає не лише формування інформаційної відкритості, але й реалізацію прав та свобод громадян (природних, похідних) за допомогою побудови дієвої моделі інформаційної безпеки інституційно-нормативного спрямування.

Заключним елементом у системі функціонального аналізу суб'єктів забезпечення інформаційної безпеки України в сучасних умовах, відповідно запропонованої нами класифікації, є контекст міжнародної співпраці України у сфері інформаційної безпеки. Метою останнього є, по-перше, запровадження дієвих засобів охорони інформаційного суверенітету на внутрішньодержавному рівні та, по-друге, запозичення певної методології інформаційно-безпекової архітектури від західних партнерів та держав, які є для України прикладом у сегменті публічно-управлінської діяльності у контексті євроінтеграції. Такі аспекти міжнародної співпраці як елемент української державної інформаційної політики були нами описані у п. 4.2 Розділу VI даного дисертаційного дослідження, проте пропонуємо додатково продублювати зазначену інформацію.

Необхідно навести приклади кооперації із такими структурами, як Центр передових технологій кібероборони НАТО (NATO CCDCOE) та команда реагування Microsoft DART (Detection and Response Team), що сутнісно та

організаційно сприяє впровадженню передових практик у сфері кібербезпеки, завдяки чому і українські фахівці отримують доступ до новітніх технологій, аналітики щодо актуальних загроз та підтримки у протидії кібератакам [394]. У сукупності, за допомогою вищезазначених стартапів реалізуються такі категорії та завдання інформаційно-безпекового середовища, як забезпечення кібернавчання та технічної підтримки, підтримка України у кіберзахисті та боротьбі з дезінформацією та допомога у створенні ефективних інструментів захисту інформації.

На підставі функціонального аналізу суб'єктів забезпечення інформаційної безпеки України в сучасних умовах, відтак, нам вдалося дійти наступних проміжних умовиводів.

По-перше, державні інституції відіграють ключову роль у формуванні та реалізації стратегії забезпечення інформаційної безпеки. Вони займаються розробкою законодавчих актів, визначають пріоритетні напрямки кіберзахисту, здійснюють нагляд за дотриманням стандартів безпеки та координують заходи з протидії інформаційним загрозам. Водночас існує потреба у вдосконаленні механізмів міжвідомчої взаємодії, посиленні швидкості реагування на кібератаки та розширенні компетенцій профільних структур, відповідальних за кібербезпеку.

По-друге, приватний сектор, представлений провайдерами телекомунікаційних послуг, фінансовими установами та технологічними компаніями, відіграє вагому роль у забезпеченні стійкості національних інформаційних ресурсів. Комерційні структури впроваджують передові технології кіберзахисту, здійснюють аудит інформаційної безпеки та розробляють інноваційні рішення для виявлення й нейтралізації загроз. Для ефективнішого захисту цифрового простору необхідно активізувати співпрацю між державними та приватними суб'єктами, створивши комплексну систему оперативного обміну інформацією щодо кіберризиків і методів їхнього попередження.

По-третє, громадянське суспільство та міжнародні партнери відіграють значну роль у зміцненні інформаційної безпеки країни. Вони сприяють підвищенню рівня цифрової грамотності, здійснюють моніторинг загроз у медіапросторі та беруть участь у міжнародних ініціативах, спрямованих на боротьбу з дезінформацією та кіберзлочинністю. Розширення міжнародної співпраці та інтеграція України в глобальні системи кібербезпеки дозволять значно посилити захист національного інформаційного середовища та підвищити його стійкість до зовнішніх загроз.

3.3. Особливості реалізації механізмів забезпечення інформаційної безпеки в Україні: інституційно-правова конструкція та управлінські обмеження

У контексті попередніх досліджень, присвячених методичним підходам до протидії загрозам інформаційній безпеці України (п. 3.1), а також функціональному аналізу суб'єктного складу системи забезпечення інформаційної безпеки в сучасних умовах (п. 3.2), постає об'єктивна потреба у комплексному розгляді механізмів реалізації державної інформаційної політики в межах національної моделі. Зокрема, акцент переноситься на інституційно-правову конструкцію цих механізмів, яка, з одного боку, повинна забезпечувати ефективну координацію між усіма залученими органами, а з іншого – виявляє істотні структурні обмеження як у правовому, так і в управлінському вимірах.

На цьому етапі дослідження важливо не лише фіксувати наявність певних суб'єктів чи методик, а й виявити логіку їхньої інтеграції у функціональний механізм, визначити характер їхньої взаємодії, ідентифікувати фактори, що впливають на ефективність реалізації державної політики у сфері інформаційної безпеки. Особливої актуальності такий підхід набуває умовах загострення внутрішніх і зовнішніх інформаційних викликів, що вимагають гнучкої та скоординованої відповіді з боку органів державної влади.

Отже, у цьому підпункті увага буде зосереджена на критичному огляді та системному аналізі конфігурації механізмів забезпечення інформаційної безпеки в Україні, їхніх ключових елементів, взаємозв'язків та структурних недоліків. Такий підхід дозволяє не лише виявити внутрішні дисфункції, а й запропонувати шляхи адаптації існуючої моделі до реалій сучасного кіберсоціального простору.

У процесі розгортання дискурсу, пов'язаного з методичними основами протидії загрозам інформаційній безпеці України (п. 3.1), а також з актуалізацією функціональної структури та компетенцій основних суб'єктів забезпечення інформаційної безпеки (п. 3.2), постає об'єктивна потреба в інтеграційному баченні того, як наявні інститути, методики та адміністративно-організаційні процедури утворюють єдиний механізм, спрямований на досягнення стратегічних цілей національної інформаційної безпеки. Даний механізм, за своєю природою, не є сукупністю окремих організаційних рішень чи адміністративних процесів — він репрезентує собою цілісну функціональну модель, яка відображає як нормативну, так і операційну логіку реалізації державної політики в зазначеній сфері.

Доцільність переходу до структурного аналізу цієї моделі зумовлена низкою чинників: 1) на практиці спостерігається фрагментарність та розбалансованість міжвідомчої взаємодії; 2) на рівні концептуального розуміння бракує уніфікованого бачення самого механізму забезпечення інформаційної безпеки; 3) наукова спільнота пропонує альтернативні підходи до інституційного конструювання таких механізмів, що потребують залучення до порівняльного аналізу.

У цьому контексті надзвичайно важливо дати тлумачення самому поняттю механізму інституційно-управлінської моделі забезпечення інформаційної безпеки. Під ним, на переконання Е. К. Щепанюк та ін. [279, с. 7], доцільно розуміти системно організовану сукупність норм, принципів, повноважень, процедур, функцій, інституційних акторів і форм координації, що

реалізуються в рамках державної інформаційної політики з метою забезпечення стабільного інформаційного простору, недопущення деструктивного впливу на свідомість громадян і функціонування критичної інфраструктури. На наш погляд, усе вищезазначене діє в контексті державної інформаційної політики, спрямованої не лише на захист інформаційної сфери, а й на формування сталого, керованого та безпечного інформаційного простору, що здатний протистояти зовнішнім і внутрішнім деструктивним впливам.

На нашу думку, розгляд цього механізму саме в українському контексті дозволяє виявити унікальні риси, пов'язані із постколоніальними трансформаціями державно-правової системи, зумовленістю зовнішньою збройною агресією, а також інституційною неврегульованістю багатьох сфер, дотичних до ІБ. Оскільки пункти 3.1 та 3.2 репрезентували, відповідно, концептуальні та суб'єктно-функціональні зрізи, саме пункт 3.3 надає змогу інтегрувати ці аспекти у єдиний об'єкт аналізу, вивчаючи логіку взаємодії, структурну конституцію та ефективність застосування.

З огляду на це, український механізм забезпечення інформаційної безпеки необхідно розглядати не лише як фактологічну адміністративну конструкцію, а й як категоріальну модель, що поєднує в собі нормативні, управлінські та концептуальні особливості. Такий підхід дозволяє виявити як архітектоніку формальних структур, так і ті приховані суперечності, що зумовлюють неефективність державного реагування на сучасні інформаційні загрози.

Наукова традиція подібного аналізу знаходить своє відображення як у зарубіжній, так і в українській доктрині. М. Вілковскі [295, с. 110] наголошує, що відсутність узгодженого національного механізму управління ІБ породжує дезінтеграцію ресурсів, дублювання повноважень і зниження рівня реагування на інформаційні атаки.

Ми пропонуємо розглядати інституційну модель забезпечення ІБ як функціональну мережу міжінституційної координації, підкреслюючи проблему неузгодженості регуляторних інструментів між ключовими органами.

Отже, сукупно, запропонований аналітичний огляд українського механізму забезпечення інформаційної безпеки дозволяє перейти до поетапного осмислення моделей контекстуації інформаційної безпеки на інституційному рівні, що будуть розглянуті сегментарно та контекстуально до питань окреслення методичихі підходи протидії загрозі інформаційній безпеці України та функціонального аналізу суб'єктів забезпечення інформаційної безпеки України в сучасних умовах.

Насамперед, маємо виходити з того, що у межах попередніх пунктів даного розділу дисертаційного дослідження вже було здійснено функціональний аналіз суб'єктного складу сфери інформаційної безпеки України, а також методичних підходів до протидії ключовим загрозам. Водночас, особливої уваги заслуговує системне осмислення існуючого механізму ІБ саме крізь призму його структурно-організаційної побудови, управлінської логіки та здатності до адаптації в умовах гібридних інформаційних викликів, зокрема — повномасштабної російської збройної агресії проти України від 24.02.2022 р. До того ж, нинішній стан інформаційної безпеки потребує не лише аналізу фактологічного наповнення, але й глибокого осмислення її концептуальної архітектоніки, моделювання реалістичних сценаріїв і виявлення слабких ланок у механізмах реалізації державної політики.

Для цілей нашого дослідження особливостей реалізації механізмів забезпечення інформаційної безпеки в Україні крізь призму інституційно-правової конструкції та управлінських обмежень маємо усвідомлювати, що більшість державних систем інформаційної безпеки в історичній та сучасній перспективі будувалися навколо однієї з трьох базових моделей, серед яких [202, с. 95] :

1) модель централізованої вертикалі (характерна для авторитарних політичних режимів);
2) мережево-координаційна модель (притаманна для країн ЄС, де вагома

роль відводиться регуляторним агентствам та незалежним експертним структурам);

3) гібридна модель, що поєднує елементи централізму з елементами децентралізованої інформаційної відповідальності між різними гілками влади та секторами.

Українська модель на сучасному етапі наближається до останнього типу — гібридної, з намаганням поєднати стратегічну координацію із тактичними повноваженнями на відомчому рівні. Водночас такі конструкції потребують високого рівня взаємодії, чітко структурованих протоколів, єдиних стандартів реагування на загрози. Так, відсутність останніх породжує фрагментарність у реалізації політики безпеки та нерівномірність контролю над інформаційним простором. У цьому аспекті доречно апелювати до роботи К. Кіфера «Інформаційна безпека. Легальний, бізнесовий та технічний посібник» від 2004 р. [257, с. 35], де автор підкреслює, що країни з перехідними демократіями особливо вразливі до зовнішніх інформаційних маніпуляцій саме через низький ступінь скоординованості інституційних відповідей.

Потрібно зауважити, що методологія моделювання державної інформаційної політики в Україні за останнє десятиліття зміщувалася від статичних стратегій до сценарних підходів, що частково відобразилось у положеннях Указу Президента України «Про рішення Ради національної безпеки і оборони України від 29 грудня 2016 р. «Про Доктрину інформаційної безпеки України», яка, хоч і містить формалізовані підходи до розпізнавання загроз та стратегічного планування, проте не вийшла за межі декларативності. Фактичний механізм реалізації інформаційної політики досі базується на реактивному управлінні, а не на проактивному прогнозуванні, що фіксують також вітчизняні дослідницькі напрацювання.

На фоні тривалих проявів як гібридних, так і повномасштабних посягань на інформаційну безпеку та загальнодержавну безпеку, Україна стикається з феноменом багатошарового інформаційного впливу, який реалізується через

деструктивні наративи, маніпуляцію новинними потоками, інформаційне навантаження та спотворення реальності в онлайн-просторі, що, власне, вимагає переосмислення державно-управлінських підходів, зокрема — переходу від відомчо-орієнтованої логіки до архітектури, що базується на сценарному прогнозуванні, симуляційному аналізі та стратегіях розподіленої відповідальності.

Особливо важливим у цьому контексті є використання елементів системної динаміки та інструментів ситуаційного моделювання у державному плануванні заходів із забезпечення інформаційної безпеки. Прикладом може слугувати підхід моделювання ефективності міжвідомчої реакції залежно від типу загроз і швидкості інформаційної дифузії.

Також зауважимо, що, згідно з положеннями Указу Президента України № 392/2020 Про рішення Ради національної безпеки і оборони України від 14.09.2020 р. «Про Стратегію національної безпеки України» та Указу Президента України № 447/2021 Про рішення Ради національної безпеки і оборони України від 14 травня 2021 року «Про Стратегію кібербезпеки України» також декларується важливість інтеграції стратегічного планування у сфері інформаційної безпеки до загальної архітектури безпекового середовища. Проте, в практичному вимірі відсутні інструменти моніторингу ефективності управлінських рішень, що робить процес впровадження політик фрагментарним. Як зазначає М. Данн Кевелті у роботі «Cyber-Security and Threat Politics: US Efforts to Secure the Information Age» (2013 р.) [219, с. 130], головною передумовою ефективного державного управління у сфері ІБ є постійна адаптація політик до реальних змін у структурі загроз, а не до абстрактних шаблонів, на що варто було б зорієнтуватися і Україні.

Таким чином, державна система інформаційної безпеки України перебуває у фазі функціонального перегляду, що вимагає чіткішого структурування, підвищення інституційної взаємодії, а також включення інноваційних методів інформаційного скринінгу, попереджувального аналізу та

ризик-менеджменту. Системна вразливість не стільки в слабких інституціях, скільки у відсутності інструментів інституціоналізованого передбачення і відлагодженого механізму швидкої реакції на багаторівневі інформаційні атаки.

Після концептуального окреслення української інституційно-управлінської моделі у сфері інформаційної безпеки стає очевидним, що її ефективність визначається не лише суб'єктним складом чи нормативною основою, а насамперед – архітектурною логікою координації, рівнем функціональної злагодженості та наявністю передумов до адаптації. У контексті складної безпекової ситуації, що склалася в Україні внаслідок російської агресії, аналіз конструкції забезпечення інформаційної безпеки має зосереджуватись на виявленні внутрішньосистемних вад, які унеможливлюють ефективну протидію зовнішнім і внутрішнім загрозам.

Найбільш критичним аспектом чинної моделі є брак скоординованості між органами державної влади, які покликані реалізовувати заходи з інформаційної безпеки. Незважаючи на визначення повноважень у стратегічних документах, які ми означили вище, відсутність єдиного центру координації створює умови для дублювання функцій, нормативної колізійності та повільної інституційної реакції на інформаційні загрози.

Як зазначає той-таки М. Данн Кевелті [219, с. 127], ефективність інформаційного захисту в умовах кризової або воєнної ситуації прямо залежить від того, наскільки органи реагування працюють у синхронізованому режимі, а не в межах своїх вузьких мандатів. В українських умовах, як справедливо підкреслюється у тутешніх дослідженнях, спостерігається надлишкова автономія ключових акторів при одночасній відсутності горизонтальних механізмів обміну критичною інформацією [167, с. 140].

Класичний приклад такої невпорядкованості – інформаційна реакція в умовах масових кібератак, яка вимагає миттєвого залучення технічних, аналітичних, політичних і правоохоронних ресурсів. У наявній системі органи виконують свої завдання із затримкою, що уможливлює реалізацію

багатоступеневих деструктивних сценаріїв супротивника.

Другим рівнем проблеми, тісно пов’язаним із попереднім, є внутрішньоорганізаційні обмеження, які блокують ефективне управління ІБ навіть за наявності формально визначеної стратегії. Однією з найважливіших характеристик таких обмежень є політична фрагментація – постійна зміна урядів, несумісність ідеологічних векторів, ревізія програм інформаційного розвитку та ротація ключових кадрів, що призводить до втрати інституційної пам’яті.

Як справедливо відзначає М. Данн Кевелті, політична мінливість безпосередньо впливає на стабільність інституцій безпеки, які потребують тривалих циклів оновлення стратегій та комплексної експертизи [219, с. 130]. В умовах України, на наш погляд, відсутня спадкоємність безпекової політики – кожна нова управлінська команда ініціює «перезапуск» заходів у сфері ІБ, не опираючись на результати попередників.

Окремо слід виокремити ресурсне та кадрове виснаження сектору ІБ. Брак фахівців у галузі кіберзахисту, інформаційного права, цифрової криміналістики не дозволяє органам оперативно формувати аналітичні групи реагування, відстежувати джерела дезінформації чи здійснювати технічний аудит інформаційних платформ. Навіть за наявності сучасного технічного забезпечення, яке надходить до України від партнерів, проблема людського капіталу залишається критичною.

На тлі окреслених проблем виникає об’єктивна потреба в перегляді засадничих принципів інституційно-управлінської моделі забезпечення інформаційної безпеки. Йдеться не лише про реформу структури або розширення повноважень існуючих органів, а насамперед — про формалізацію нової архітектури інформаційної безпеки на засадах прозорості та гласності, де стратегія й тактика функціонуватимуть як частини єдиного безперервного процесу.

У цьому сенсі слід апелювати до концепції адаптивного управління

ризиками (adaptive security governance), запропонованої згаданим Л. Табанскі [280]. Згідно з нею, ефективна система ІБ повинна постійно змінювати власну архітектуру відповідно до характеру загроз, трансформації соціальних очікувань та технологічного прогресу. На рисунку 3.1 якраз-таки здійснено графічне представлення ключових, на наш погляд, рис такої моделі для контексту та цілей переходу до адаптивної архітектури забезпечення ІБ.

Рисунок 3.1. Структура моделі переходу до адаптивної архітектури інформаційної безпеки (ІБ)

Зі свого боку, українська наукова традиція також актуалізує цю необхідність. Зокрема, В. Аніщук стверджує, що в Україні відсутній інструментальний апарат для гнучкої перебудови моделей управління інформаційною безпекою відповідно до сценаріїв загроз [285].

Формалізація нової моделі має включати трирівневу структуру:

рівень стратегічного управління (створення аналітичного центру з прогнозування ІБ),

рівень оперативної координації (спільні центри реагування, що об’єднують ресурси різних міністерств),

рівень тактичного реагування (локальні сценарії дій на рівні відомств, органів місцевого самоврядування, окремих територіальних громад).

Саме така архітектоніка, на наше переконання, дозволить долати вузькість компетенцій, забезпечити наскрізне управління та створити умови для імплементації гнучкої моделі цифрової стійкості, до якої наразі прямують усі європейські країни, що зіштовхнулись із загрозами системного інформаційного впливу.

Розгляд ключових обмежень і деформацій інституційно-управлінської моделі забезпечення інформаційної безпеки України виявив глибоко вкорінені структурні вади, що не можуть бути усунуті виключно на нормативному рівні. Ці проблеми лежать у площині організаційної логіки, комунікативної динаміки та управлінської культури, тому їхнє вирішення потребує не лише зміни регламентів, а й переосмислення самої архітектури державного управління в сфері ІБ. Сформульовані нижче висновки є узагальненням авторського аналітичного підходу до виявленої проблематики.

По-перше, вітчизняна модель координації заходів із забезпечення інформаційної безпеки характеризується критично низьким рівнем функціональної інтеграції між інституціями, що беруть участь у процесі. Попри задекларовані повноваження окремих суб’єктів, практична реалізація заходів часто відбувається в режимі інституційної замкненості, без належного обміну даними, інформаційної синергії та горизонтальних координаційних механізмів. Це створює ситуацію фрагментарної реакції на загрози, унеможливлюючи формування єдиної інформаційної картини та стратегічного управлінського бачення. Відсутність єдиного координаційного центру – як інституційного, так і комунікативного – посилює вразливість України до багатофакторних

інформаційних атак, які вимагають швидкої багаторівневої реакції.

По-друге, реальна ефективність чинної моделі ускладнюється низкою внутрішніх управлінських обмежень, серед яких вирізняються політична фрагментація, нестабільність управлінських еліт, обмеженість ресурсної бази, дефіцит кадрового потенціалу та слабкість національної експертної спроможності у сфері інформаційної політики. Політична турбулентність в Україні призвела до відсутності довгострокового бачення у сфері ІБ, постійних змін пріоритетів і стратегічного дрейфу між інституційними підходами. Це унеможливлює як нормальне функціонування процедур управління ризиками, так і формування системної політики. Крім того, нерівномірний розподіл технічних і фінансових ресурсів між органами, застарілі підходи до підготовки фахівців та неповна реалізація принципу безперервності державного управління посилюють невідповідність між завданнями й інструментами їх реалізації.

По-третє, діагностовані системні обмеження зумовлюють необхідність докорінного перегляду самої конструкції інституційно-управлінського механізму забезпечення інформаційної безпеки. Автором запропоновано концептуальну модель переходу до адаптивної архітектури, побудованої на принципах міжвідомчої взаємодії, ризик-орієнтованого планування, технологічної гнучкості та етичної підзвітності. У такій моделі держава не лише реагує на загрози, а й функціонує як інформаційно стійка система, що здатна передбачати, симулювати й моделювати сценарії дестабілізації в цифровому середовищі. Це передбачає впровадження міждисциплінарних аналітичних платформ, динамічну координацію між секторами, створення постійно оновлюваних протоколів реагування та впровадження централізованого хабу аналітичного моніторингу.

Таким чином, підсумовуючи результати проведеного аналізу, можна стверджувати, що дієздатна модель інформаційної безпеки в Україні можлива лише за умови її переосмислення як адаптивної, відкритої, інтегрованої системи, де пріоритетом стане не тільки запобігання загрозам, а й формування

культури інформаційної стійкості на всіх рівнях державного управління. Системне оновлення управлінської конструкції має спиратися на баланс між стабільною нормативною базою, ефективною інституційною логікою та інноваційною аналітичною парадигмою, яка відповідатиме викликам нової інформаційної епохи.

Висновки до розділу 3

1. Систематизовано та науково обґрунтовано методичні підходи протидії загрозам інформаційній безпеці України в умовах військової агресії, що виражається у кластеризації методичних підходів протидії загрозам інформаційній безпеці у системі публічного управління, виділивши п'ять взаємодоповнюючих кластерів: нормативно-правові та організаційні механізми (через аналіз ЗУ «Про національну безпеку України» та ЗУ «Про основні засади забезпечення кібербезпеки України»); технічні засоби та методологія кіберзахисту (використання SIEM, IDS/IPS, міжнародна кооперація, наприклад, із NATO CCDCOE та Microsoft DART); інформаційно-психологічна безпека та протидія дезінформації (підвищення медіаграмотності, діяльність Центру протидії дезінформації, використання VoxCheck та StopFake); освітні ініціативи та підвищення цифрової грамотності (аналіз ініціативи «Дія. Цифрова освіта» та застосування ідеологічного контролю в ЗВО, наприклад, через обмеження використання месенджера Telegram); інтеграція міжнародної співпраці (положення Угоди про асоціацію з ЄС, долучення до Cyber Rapid Response Teams, співпраця з Google, Amazon, Microsoft;

2. Здійснено функціональний аналіз суб'єктного складу забезпечення інформаційної безпеки (ІБ) України.

Розроблено чотирикластерну класифікацію суб'єктів ІБ: Державні органи (СБУ, РНБО, Мінцифра, Нацполіція, Мінкульт), Приватний сектор (ІТ-компанії, оператори зв'язку, фінансові установи, експертні центри),

Громадський сектор та медіа та Міжнародна співпраця.

Сформульовано тривимірну архітектурну модель взаємодії ключових державних суб'єктів ІБ (СБУ, РНБО, Мінцифра) + Нацполіція, де: перший кластер – кореляційний зв'язок між масштабним моніторингом СБУ та сприянням у моніторингу і організаційним впорядкуванням держреєстрів Мінцифри; другий кластер – уніфікований стратегічний статус РНБО щодо формування безпекового простору, доповнений контролем СБУ та технологічною імплементацією Мінцифри (за допомогою ІКТ); третій кластер – функціонування усіх трьох інституцій в інтересах національної ІБ як механізму забезпечення національної інформаційно-безпекової політики.

Обґрунтовано розширення функціональної ролі Міністерства культури та стратегічних комунікацій України (Мінкульту) як ключового суб'єкта, що забезпечує соціально-суспільний (гуманітарний) наратив ІБ, зокрема, через культивування інформаційної політики, нормативно-правове регулювання у сфері ЗМІ (аналіз ЗУ «Про медіа») та зміцнення національно-безпекового профілю через інформаційно-культурні інтереси.

Конкретизовано функціональну участь приватного сектору у реалізації ІБ (згідно зі ст. 10 ЗУ «Про основні засади забезпечення кібербезпеки України») через виділення його основних суб'єктів (ІТ-компанії, фінансові установи, експертні центри) та їхніх практичних завдань (захист мереж, запобігання шахрайству, оцінка захищеності).

Акцентовано на ролі громадського сектору та медіа як потужного інструменту викриття інформаційних маніпуляцій та реалізації прав та свобод громадян шляхом побудови дієвої моделі інформаційної безпеки інституційно-нормативного спрямування.

3. Здійснено критичний системний аналіз інституційно-управлінської моделі забезпечення інформаційної безпеки України.

Обґрунтовано, що сучасна українська модель ІБ є гібридною, яка намагається поєднати стратегічну централізацію (РНБО) із відомчою

децентралізацією, але фактично функціонує як реактивна, фрагментарна система, що базується на відомчо-орієнтованій логіці замість необхідної проактивної, сценарно-прогнозної архітектури.

Виявлено та систематизовано ключові управлінські обмеження (внутрішньосистемні вади) реалізації механізмів ІБ в Україні, які лежать поза нормативно-правовою площиною:

Критично низький рівень функціональної інтеграції: Відсутність єдиного інституційного та комунікативного координаційного центру та горизонтальних механізмів обміну критичною інформацією між ключовими акторами (СБУ, РНБО, Мінцифра та ін.), що призводить до дублювання функцій, нормативної колізійності та повільної, фрагментарної реакції на багатофакторні загрози.

Політична фрагментація та втрата інституційної пам'яті: Нестабільність управлінських еліт, часта зміна пріоритетів і стратегічний дрейф, що унеможливлює довгострокове планування та спадкоємність безпекової політики.

Ресурсне та кадрове виснаження: Гострий дефіцит фахівців у сфері кіберзахисту та аналізу інформаційних загроз, який блокує здатність органів до оперативного формування аналітичних груп та ефективного використання технологічної допомоги від міжнародних партнерів.

Запропоновано концептуальну модель переходу до адаптивної архітектури забезпечення ІБ (на основі концепції adaptive security governance), яка передбачає формалізацію архітектури інформаційної безпеки на засадах прозорості та гласності та впровадження трирівневої структури управління: стратегічний рівень (створення аналітичного центру з прогнозування ІБ (орієнтація на передбачення та сценарне планування); оперативний рівень (створення спільних міжвідомчих центрів реагування (забезпечення синхронізованої відповіді); тактичний рівень (розробка локальних сценаріїв дій на рівні відомств та територіальних громад (гнучке реагування).

Стверджується, що дієздатна модель ІБ в Україні вимагає

переосмислення як адаптивної, інтегрованої системи, де пріоритетом є формування культури інформаційної стійкості та баланс між стабільною нормативною базою, ефективною інституційною логікою та інноваційною аналітичною парадигмою.

РОЗДІЛ 4
НАПРЯМИ УДОСКОНАЛЕННЯ МЕХАНІЗМІВ РЕАЛІЗАЦІЇ ІНФОРМАЦІЙНОЇ БЕЗПЕКИ У СИСТЕМІ ПУБЛІЧНОГО УПРАВЛІННЯ

4.1. Міжнародний досвід управління забезпеченням інформаційної безпеки

Міжнародна парадигма забезпечення інформаційної безпеки базується на впровадженні механізмів, способів та засобів нівелювання потенційних інформаційних, безпекових, кібербезпекових та іншого формату (дезінформація, гібридна агресія) ризиків, що мають ключовим об'єктом негативного впливу державно-управлінські процеси.

Відмітною особливістю процесу управління забезпеченням інформаційної безпеки на міжнародному рівні є, водночас, не лише реагування, але також виявлення і попередження загроз інформаційній сфері, що виникають як результат цифрового розвитку : використання кібертехнологій для вчинення атак на кібернетичну, цифрову та ІТ-інфраструктуру держави, навмисне створення передумов до інформаційного тероризму щодо іншої держави, її інформаційної ізоляції та вплив таким чином на бізнес та громадянське суспільство.

На наш погляд, у розрізі доктринального аналізу необхідно розпочати із сутності стратегічного управління забезпеченням інформаційної безпеки у якості процесу.

Розглядаючи питання регуляції та стандартизації управління інформаційною безпекою в США у якості процесу та феномену публічного управління та адміністрування, американський вчений Л. Табанскі [280]

відмітив, що сутність стратегічного управління забезпеченням інформаційної безпеки як процес, за котрий відповідають посадові особи та інституційний апарат держави, полягає у синхронізації юридичних, організаційних та технічних засобів, за допомогою яких здійснюється захист економічних та політичних інтересів держави та соціальних інтересів суспільства у контексті створення передумов державної стабільності. Можемо погодитися із зазначеним підходом до розуміння сутності стратегічного управління забезпеченням інформаційної безпеки, та відмітити, що у даному випадку вчений ототожнює даний процес із пошуком оптимального балансу між засобами нормативного закріплення та безпосереднього фактичного впровадження безпекової карти відносно даних та інформації, обіг котрих здійснюється в межах певної держави (її органів та установ) та може зазнавати негативного впливу як на зсередини, так і ззовні.

Одночасно із вищенаведеним повинні зауважити, що сутність стратегічного управління забезпеченням інформаційної безпеки в розвинених державах світу не має єдиноначального формату реалізації та відрізняється залежно від інтенцій державної політики, концептуальної спрямованості інтеграції інформаційно-безпекових інструментів та загального курсу держави у внутрішньодемократичному та зовнішньому розвитковому полі.

У процесі дослідження відмінностей стратегічного управління забезпеченням інформаційної безпеки в США та ЄС, іноземний дослідник Е. Фейгі [235, с. 1080] слушно зауважив, що пріоритети у формуванні та реалізації відповідних заходів інформаційно-безпекового характеру детерміновані насамперед різницею між підходами кожного із публічно-управлінських апаратів, котрі, в свою чергу, мають прецедентом власної появи різні завдання у вимірах геополітичних інтересів, рівня технологічного розвитку, соціальних потреб та історичного досвіду.

Вищезапропоноване визначення та науково-доктринальне розуміння походження сутності стратегічного управління забезпеченням інформаційної

безпеки у якості процесу, водночас, зумовлює необхідність більш конкретно зупинитися на прямих прикладах створення передумов управління інформаційним простором в США, ЄС, Великій Британії, Ізраїлі та Китаї як країнах із підвищеною чутливістю інформаційно-безпекового середовища, що потребує відповідного рівня поетапності захисту.

До прикладу, у США сутність політики щодо питань забезпечення інформаційної безпеки та стратегічної моделі управління останньою заснована на концептуальній реалізації стандартів, акцентованих на збереженні та примноженні фактів домінування в кіберпросторі, захисті критичної інфраструктури та забезпеченні глобального впливу через контроль над технологічними стандартами. Механізмами реалізації даного процесу в США є відповідна нормативно-правова надбудова, що складається із Закону про обмін інформацією про кібербезпеку 2015 р. (Cybersecurity Information Sharing Act, CISA 2015), Виконавчого наказу Президента США 14028 «Підвищення кібербезпеки країни» 2021 (Executive Order 14028 «Improving the Nation's Cybersecurity» 2021) та Закону про Агентство з кібербезпеки та безпеки інфраструктури 2018 р. (Cybersecurity and Infrastructure Security Agency Act 2018).

Виходячи із положень Закону про обмін інформацією про кібербезпеку 2015 р. (Cybersecurity Information Sharing Act, CISA 2015) [144], американський законодавець визначає одним із ключових пріоритетів діяльності у інформаційній галузі взаємодію між приватним та публічним сектором, тобто між громадянським суспільством та урядовими структурами (інституціями, відповідальними за реалізацію політики інформаційної та кібербезпеки водночас). У контексті приватно-публічної взаємодії у інформаційно-безпековій сфері з точки зору сутності даного процесу виділяємо положення Секції 4 даного нормативного акту (Sec. 4), де презюмується обов’язок держави надати юридико-правовий захист компаніям, установам та організаціям, що здійснюють власну діяльність у галузі передачі інформації та котрі повідомили

про наявні факти або потенційні факти порушення інформаційного суверенітету держави.

Концептуальні положення, регламентовані та конкретизовані у Виконавчому наказі Президента США 14028 «Підвищення кібербезпеки країни» 2021 (Executive Order 14028 «Improving the Nation's Cybersecurity» 2021), в свою чергу, першочергово базуються на інтенційній спрямованості вдосконалення інформаційної безпеки у контексті превалювання спроб дестабілізації кібербезпекового середовища та, водночас, стимулювання використання сучасних технологій та покращення обміну інформацією про загрози між урядом і приватним сектором в сегменті вдосконалення кібернетичної та цифрової безпеки і захищеності федеральних урядових мереж, що можуть містити стратегічну публічно-управлінську інформацію та дані, котрі підлягають захисту як такі, що становлять державну таємницю і, відповідно, підлягають багаторівневому захисту від потенційних незаконних посягань.

У Законі про Агентство з кібербезпеки та безпеки інфраструктури 2018 р. (Cybersecurity and Infrastructure Security Agency Act 2018) визначено та нормативно рамковано принципи, особливості та інтенційні виміри діяльності Агентство з кібербезпеки та захисту інфраструктури (Cybersecurity and Infrastructure Security Agency). Метою створення зазначеної інституції, відповідно Секції 2203 документу (Sec. 2203 Cybersecurity Division), є координації роботи у сфері кіберзахисту, забезпечення стійкості критичної інфраструктури та реагування на інциденти за допомогою наявної системи інформаційної інфраструктури із відповідним ступенем захищеності.

Проаналізовані тенденції сутності стратегічного управління забезпеченням інформаційної безпеки в США крізь призму нормативно-правової моделі дозволяють говорити про концентрованість даного процесу не лише на тенденції «горизонтального» державного управління, де нормативно-правові акти у сфері інформаційної безпеки є джерелом забезпечення останньої

де-юре, а не де-факто, а й на безпосередності досягнення результату. Такий забезпечується за допомогою залучення приватного сектору до взаємодії із інституціями інформаційної безпеки, внаслідок чого створюється прецедент т.зв. «державно-приватного партнерства» у даній галузі. На наш погляд, використання зазначеного підходу є інноваційним з точки зору досягнення відповідних інформаційно-безпекових цілей та, одночасно з цим, є підґрунтям у питаннях відповіді на виклики інформаційного простору сьогодення, пов'язані із діджиталізацією загроз.

Процедурна складова реалізації сутності стратегічного управління забезпеченням інформаційної безпеки в ЄС, з іншого боку, архітектована за дещо відмінною типологією, котру в державно-управлінському вимірі можна дефініціювати як «ціле та частини».

Першочергово маємо зауважити, що засадничим чинником стратегічного управління забезпечення інформаційної безпеки в ЄС є захист приватності громадян, уніфікована консолідація законодавства між державами-членами та забезпечення кіберстійкості держави за допомогою використання додаткових заходів взаємодії між громадянським суспільством та державою.

Законодавчими документами, котрі регулюють у ЄС питання стратегічного управління забезпечення інформаційної безпеки, є Загальний регламент про захист даних 2016 р. (GDPR 2016) [49], Регламент про кібербезпеку 2019 р. (Cybersecurity Act 2019) та Стратегія ЄС з кібербезпеки 2020 р. (EU Cybersecurity Strategy 2020). Сукупно, у зазначених нормативно-правових актах визначається порядок персонального захисту даних громадян та забезпечення кібербезпеки задля запобігання імовірним фактам витоку даних та інформаціїї державного значення; конкретизовано положення та стандарти для сертифікації ІТ-продуктів у рамках формування безпекового поля на території Союзу; конкретизуються пріоритети та напрями розвитку кібербезпеки, які реалізуються через відповідні законодавчі ініціативи та можуть бути запроваджені за допомогою впливу державних органів та установ ЄС, як-от

Європейське агентство з кібербезпеки (ENISA), Європол (European Union Agency for Law Enforcement Cooperation) та Європейська служба зовнішньої діяльності (EEAS).

Потрібно зауважити, що, на відміну від специфіки та стилістики стратегічного управління забезпечення інформаційної безпеки в США, європейська модель реалізації зазначеного підходу передбачає управління «згори донизу», де загальносоюзні підходи та інтереси у реалізації інформаційно-безпекової політики набувають загальнообов'язкового характеру для держав-членів ЄС. Зазначений формат політики генерації сутності стратегічного управління забезпеченням інформаційної безпеки в ЄС, на наше переконання, відзначається вищим рівнем впорядкованості та, імовірно, більшою застосовністю для зазначених цілей через декларативність, нормативний характер та неможливість відступу від респонденції державами. Даним фактом забезпечується уніфікованість моделі інформаційної безпеки як сутнісного стратегічного інституту в ЄС.

Надалі пропонуємо сконцентрувати увагу на Великій Британії як державі із опціонально-індивідуальним підходом до реалізації стандартів сутності стратегічного управління забезпеченням інформаційної безпеки. Не дивлячись на належність до англо-американської правової сім'ї, концепти реалізації інформаційно-безпекової політики країни є індивідуалізованими та частково походять і від європейських традицій охорони та зберігання інформації (даних), тому зазначений приклад підлягає розгляду в усамітненому (відокремленому) форматі.

Як зазначається у дослідженні особливостей архітектури інформаційної безпеки Великої Британії у її сутнісному вимірі від Ф. Дейвіса [225, с. 139], сегментами конкретизації державної політики у зазначеній галузі можна визнавати забезпечення стійкості національної інфраструктури, боротьбу з дезінформацією та протидію кіберзагрозам. Крім того, аспект виходу країни з ЄС демонструє акцент на розвитку національних технологій та локального

інфраструктурно-технологічного сектору реалізації інформаційно-безпекової політики, незалежного від підходів та стандартів інших держав.

Розглядаючи цю позицію ширше, варто зауважити, що британська модель інформаційної безпеки, як її інтерпретує Ф. Дейвіс, відображає синтез стратегічного прагматизму, правового реалізму та технологічного суверенітету. Вихід Сполученого Королівства з Європейського Союзу став своєрідним каталізатором для переосмислення ролі держави у цифровому просторі — від елемента інтегрованої європейської системи до самостійного суб'єкта, здатного вибудовувати власну парадигму кіберзахисту та інформаційного управління. Ця парадигма, за суттю, спирається на триєдину концепцію: інфраструктурна стійкість, інформаційна незалежність та операційна адаптивність.

Під інфраструктурною стійкістю розуміється здатність критичних систем — енергетичних, фінансових, телекомунікаційних, транспортних — зберігати функціональність у випадку кіберінцидентів або інформаційних атак. Власне, Британія є однією з небагатьох держав, де безпековий підхід охоплює не лише цифрову сферу, а й фізичну інфраструктуру, усвідомлюючи тісну взаємозалежність між ними. Саме тому урядова стратегія «National Cyber Strategy» передбачає не лише кіберзахист у вузькому сенсі, а і створення національних резервних систем, здатних забезпечити безперервність функціонування державних і приватних сервісів у кризових умовах.

Боротьба з дезінформацією у британській доктрині має виразно інституційний характер. Вона здійснюється через механізми координації між державними структурами (зокрема, Government Communications Service), технологічними компаніями та незалежними медіарегуляторами. Такий підхід демонструє перехід від репресивних методів протидії до системи «інформаційної гігієни», у центрі якої перебуває не цензура, а підвищення рівня довіри до офіційних джерел інформації, розвиток навичок критичного мислення та медіаграмотності серед громадян. Фактично, британська модель ставить за мету не стільки обмеження інформаційних потоків, скільки їх

оздоровлення.

Окремої уваги заслуговує аспект формування локального технологічного сектору, який після Brexit набув статусу пріоритетного напряму державної політики. Йдеться не лише про економічний протекціонізм, а передусім про стратегічну безпеку — мінімізацію залежності від зовнішніх постачальників у сфері цифрової інфраструктури, програмного забезпечення та засобів шифрування. Цей процес є логічним продовженням концепції «digital sovereignty», що втілює прагнення Великої Британії забезпечити самодостатність у галузі обробки, зберігання та передачі інформації.

Підхід, описаний Ф. Дейвісом, демонструє також характерну рису британського публічно-управлінського мислення — орієнтацію на інституційну еволюцію, а не революцію. У протидії інформаційним загрозам держава не руйнує існуючих механізмів, а поступово перебудовує їх, вводячи гібридні форми співпраці між державою, приватним сектором та науковими центрами. Таким чином, модель британської інформаційної безпеки набуває рис відкритої системи, де регулювання ґрунтується не лише на законі, але й на управлінській раціональності, публічній підзвітності та технологічному інноваціонізмі.

Маємо зазначити, що у контексті українського досвіду вивчення цієї моделі має особливу цінність. Так, Велика Британія фактично продемонструвала, що стратегія інформаційної безпеки не може бути лише реакцією на загрози — вона має бути інтегрованою політикою розвитку, у якій інформаційний суверенітет розглядається як форма національної конкурентоспроможності. Для України, яка перебуває у стані постійного інформаційного тиску з боку зовнішнього агресора, подібний підхід міг би стати орієнтиром у побудові власної системи, що поєднує гнучкість ринкових механізмів із чітким державним стратегічним баченням.

Таким чином, аналіз Ф. Дейвіса дозволяє констатувати, що британська архітектура інформаційної безпеки — це не лише набір політичних рішень чи технічних протоколів, а цілісна філософія державної стійкості, у центрі якої

перебуває людина — як носій інформації, як її споживач і водночас як найуразливіша ланка інформаційного ланцюга.

Як і у попередніх випадках, особливості сутності стратегічного управління забезпеченням інформаційної безпеки у Великій Британії найдоцільніше конкретизувати крізь призму положень національного законодавства. Ключовими нормативними документами, що передвизначають сутність інформаційно-безпекової стратегізації, є Акт про захист даних 2018 р. (Data Protection Act 2018), Закон про розслідувальні положення 2016 р. (Investigatory Powers Act 2016) та Національна стратегія кібербезпеки Великої Британії 2022-2030 р. (UK National Cyber Security Strategy 2022-2030). Пропонуємо більш детально зупинитися на положеннях зазначених актів законодавства у контексті стратегій забезпечення інформаційної безпеки у Великій Британії.

У Акті про захист даних 2018 р. (Data Protection Act 2018) [91], британський законодавець встановив стандарти обробки персональної інформації, захисту даних та чутливої інформації та механізми, за допомогою яких може бути реалізовано права громадянина на конфіденційність інформації. Застосовними у даному контексті вважаємо п. 12-15 (права суб'єкта інформації – rights of the data subject) Розділу II (Регламент про захист даних Великобританії – UK GDPR), котрі визначають право на інформацію та право на відстоювання власного інформаційного інтересу громадянином у якості засадничих положень державної політики у даному секторі. Загальна модель Акту про захисту даних 2018 р. (Data Protection Act 2018) та, зокрема, деяких його складових частин, як-от згаданий вище Розділ II документу дозволяє говорити про зв'зок британського законодавства в сфері захисту інформації із європейським – зокрема, із згаданим нами раніше у контексті регулювання сутнісних рис інформаційної безпеки в ЄС Загальним регламентом про захист даних 2016 р. (GDPR 2016).

Доповненням до Акту про захист даних 2018 р. (Data Protection Act 2018)

у контексті стилістичного формату регулювання сутності стратегічного управління забезпеченням інформаційної безпеки у Великій Британії, в свою чергу, є Закон про розслідувальні положення 2016 р. (Investigatory Powers Act 2016). У зазначеному документі, зокрема, регулюється діяльність правоохоронних органів та розвідувальних служб щодо перехоплення комунікацій, спостереження та збирання даних, котрі можуть мати значення для адміністрування інформаційного простору на рівні правового та публічно-управлінського забезпечення. Зокрема, сутність інтервенцій державних органів, як-от Національний центр кібербезпеки (National Cyber Security Centre - NCSC), Урядовий центр комунікацій (Government Communications Headquarters – GCHQ) та Інформаційний комісаріат (Information Commissioner's Office – ICO) регламентовано та декларовано у Частині 2 даного нормативного акту «Законне перехоплення комунікацій» (Lawful Interception of Communications), де у п. 15-17 Розділу I агреговано право на екзаменування національного інформаційно-безпекового простору задля недопущення системних порушень.

Національна стратегія кібербезпеки Великої Британії 2022-2030 р. (UK National Cyber Security Strategy 2022-2030), в свою чергу, виступає системним нормативним актом, що детермінує підходи до забезпечення національної безпеки, інформаційної безпеки та, водночас, кібербезпеки як елемента захищеності держави на рівні внутрішнього публічного управління та міжнародного статусу держави в умовах недопущення посягання на різні інваріації її суверенних прав. Документ включає заходи для захисту критичної інфраструктури, боротьби з кіберзагрозами, розвитку національного потенціалу в галузі кібербезпеки (згідно із п. 14-18 Стратегії). Вищезазначеним, на наш погляд, знову-таки підтверджується концептуальна акцентуація уваги на кібербезпеці як елементі національної та інформаційної безпеки та формується карта подальшої протидії загрозам даних та інформації як чинника незалежного функціонування держави та її реєстрів.

Потрібно розуміти, що сутність особливостей стратегічного управління

забезпеченням інформаційної безпеки за своїм призначенням та походженням є гнучким та варіативним процесом. Цілі та кінцева реалізація останніх залежить, зокрема але не виключно, від статусу держави та наявності/відсутності додаткових чинників респонденції на загрози останньої. Формат діяльності та сутнісного забезпечення інформаційно-безпекового формату правовідносин всередині держави на прикладі вищезазначеного ми пропонуємо дослідити нижче на прикладі політики Ізраїлю в даному сегменті.

На підставі деяких фахових досліджень у галузі інформаційної безпеки Ізраїлю крізь призму визначення сутності процесу стратегічного управління даним сектором [68, с. 177-178; 130, с. 23-24] можемо дійти висновку, що політика країни у галузі інформаційної безпеки насамперед сконцентрована на посиленні обороноздатності та стимулюванні становлення сектору високих технологій, де ключовими орієнтирами державної політики фактично визначено моніторинг кібернетичних загроз, насамперед заснований на адаптивності до змін внутрішнього та глобального безпекового середовища.

Відмінність Ізраїлю від інших держав у принципології побудови сутнісного управління сектором інформаційної безпеки полягає у превалюванні інституційного управління галуззю над нормативним, що передбачає сегментацію практики над теоретико-статичними напрацюваннями.

Ключовою інституцією, що визначає порядок та спрямованість діяльності сектору інформаційно-безпекового забезпечення в Ізраїлі, є Національний кібердиректорат (Israel National Cyber Directorate, INCD), котрий здійснює координацію та контроль за додержанням інформаційної безпеки на національному рівні, а до його завдань належить захист критично важливої інфраструктури засобами, зокрема, встановлення кореляції та взаємодії між державними та приватними організаціями із залученням останніх до процесу оборони від потенційних впливів агресії на кібернетичний а, отже, інформаційний простір держави. Діяльність останнього визначається положеннями Постанови уряду Ізраїлю № 2444 «Підвищення національної

готовності до кібербезпеки» від 15.02.2015 р. та Постанови уряду Ізраїлю № 3611 «Розвиток національних можливостей кіберпростору» від 07.08.2011 р., а також галузевим Законом про кіберзахист 1995 р. (Computer Law 1995).

Крім того, враховуючи необхідність постійного реагування Ізраїлю на можливі та потенційні виклики у галузі не лише інформаційної безпеки, але й військово-мілітарної здатності належним чином реагувати на прямі та гібридні форми впливу та агресії проти держави, урядом країни ініційовано інтеграцію військових та цивільних ресурсів для боротьби із кіберзлочинністю. Відповідно даної ініціативи, нормативною рамкою для якої є п. 3-5 Розділу II Закону про службу в армії Ізраїлю 1986 р. (Israel Defense Service Law 1986), підрозділи 8200 та 81, сегментом діяльності котрих є елітна розвідувальна служба, що спеціалізується на електронній розвідці та кібероперацїях, а також –технічна розвідка та розробка кіберзасобів, працюють над досягненням інформаційної безпеки держави у сучасному цифровому вимірі.

На основі проаналізованих особливостей державно-управлінського забезпечення інформаційної безпеки в Ізраїлі можемо стверджувати, що сутність даного процесу тут визначається крізь призму можливостей та особливостей реагувати на інформаційні подразники та безпекові подразники, які прямо або опосередковано походять та генеруються саме здатністю управляти даними всередині держави. Акцентуація уряду Ізраїлю на встановленні відповідності між політикою держави у сфері інформаційної безпеки та кібербезпекою як складовою частиною інформаційного простору, знову-таки, чітко вказує на тенденційні зміни та, водночас, гнучкість інформаційної безпеки як явища та складової політики держави.

Задля означення багатогранності сутності стратегічного управління забезпеченням інформаційної безпеки пропонуємо наостанок зосередити увагу на Китаї як країні із підвищеним рівнем контролю в даному секторі.

Описуючи сутнісні особливості стратегічного управління процесом забезпечення інформаційної безпеки в Китаї, тамтешня дослідниця М. Джіанг

[249] звернула увагу на характерні риси зазначеного процесу : цензура, контроль та нагляд над мережею Інтернет та акцент на підтримці державних, а не приватних компаній у сфері ІТ.

Центральна роль державних органів в управлінні інформаційною безпекою передбачає діяльність Центральна комісія з кібербезпеки та інформатизації (Central Cyberspace Affairs Commission), Міністерство громадської безпеки (Ministry of Public Security) та Національного управління криптографії (China's State Cryptography Administration), що спрямовані на реалізацію державної політики у сфері інформаційної та кібербезпеки пропорційно власним повноваженням та компетентностям.

Таким чином, до сфери відання Центральної комісії з кібербезпеки та інформатизації (Central Cyberspace Affairs Commission) належить формування політики та стратегій кібербезпеки держави. Примітно, що очолюється зазначений орган безпосередньо президентом Китаю, і, відповідно, спрямування та координація його діяльності відбувається за горизонтальною моделлю підпорядкування.

Особливості діяльності Міністерство громадської безпеки (Ministry of Public Security) детерміновані прямим зобов’язаннями даного органу у сфері державної інформаційного безпеки з точки зору сутнісного розуміння даного процесу, що передбачає, зокрема, відповідальність за забезпечення безпеки в національному кіберпросторі та боротьбу з кіберзлочинністю.

Роль та місце Національного управління криптографії (China's State Cryptography Administration) полягає у контролі використання криптографічних технологій у країні. Метою даного процесу є, перш за все, формування навичок математичні методи забезпечення конфіденційності, цілісності і автентичності інформації, що підлягає охороні в державних реєстрах.

Нормативно-правове регулювання сутності забезпечення інформаційної безпеки в Китаї побудовано за тривимірною нормативною структурою та передбачає регуляцію такими нормативними документами, як Закон про

кібербезпеку 2017 р. (Cybersecurity Law of the People's Republic of China 2017), Закон про захист персональних даних 2021 р. (Personal Information Protection Law of the People's Republic of China 2021) та Закон про національну безпеку 2015 р. (National Security Law of the People's Republic of China 2015). Положеннями зазначених нормативно-правових актів, зокрема, визначаються особливості регулювання захисту критичної інформаційної інфраструктури, обробки даних і діяльності іноземних компаній у китайському кіберпросторі; встановлюються аспекти контролю над збором, зберіганням і передачею персональних даних; інформаційна безпека визначається важливим аспектом національної безпеки.

Таким чином, аналіз сутності стратегічного управління процесом забезпечення інформаційної безпеки в Китаї дозволяє дійти висновку щодо гнучкості та варіативності даного процесу загалом, проте, водночас, і умовиводу щодо можливості формування негативної парадигми інформаційно-безпекового середовища. Можна говорити про два формати функціонування теорії інформаційної безпеки : позитивний та негативний. Позитивний являє собою забезпечення інформаційної безпеки зі збереженням права громадян на відкритість та гласність отримання інформації та обміну нею, тоді як негативний, як правило, прямо чи опосередковано обмежує інформаційні права, свободи та інтереси людини і громадянина, маючи на меті не лише забезпечення інформаційної обороноздатності держави, але й встановлення цензури на певні питання обміну даними та їхньої агрегації населенням та суспільством.

Окрім власне сутності стратегічного управління забезпеченням інформаційної безпеки в розвинених державах світу, розгляду та аналізу в рамках дослідження міжнародних норм та практик забезпечення інформаційної безпеки підлягає також мета та особливості даного процесу в сукупності.

Мета стратегічного управління забезпеченням інформаційної безпеки розглядається іноземними науковцями [253] як процес створення системи,

кінцевою метою діяльності котрої є забезпечення захисту державних джерел інформації, нейтралізація зовнішніх і внутрішніх загроз та забезпечення довіри до інформаційного середовища від громадянського суспільства, котре становить основний демократичний кластер соціального значення.

Окрім вищезазначеного, метою стратегічного управління забезпеченням інформаційної безпеки також можна визначати сприяння інноваціям та технологічному розвитку в зазначеній сфері. Зазначена ініціатива сутнісно передбачає підтримку інновацій у галузі інформаційних технологій та кібербезпеки, стимулювання розвитку національних компаній і забезпечення конкурентоспроможності на глобальному ринку.

Субсидіарною метою стратегічного управління забезпеченням інформаційної безпеки в розвинених державах світу, на наш погляд, також можна вважати підвищення обізнаності населення про наявність відповідного роду загроз. У рамках даного сегменту, зокрема, набуває необхідності побудова належної архітектури кібербезпеки, доступної до розуміння населенням, а також розвиток культури інформаційної безпеки серед громадян і підприємств на засадах формування у останніх категорій ототожнення власних дій із реалізацією принципів безпеки інформації на загальнодержавному рівні.

Основоположного та, водночас, сегментованого значення у системі розуміння стратегічного управління забезпеченням інформаційної безпеки в розрізі дослідження міжнародних норм та практик забезпечення інформаційної безпеки набуває висвітлення особливостей контекстуації останньої у розвинених державах світу. Саме на цьому буде побічно сконцентровано наш науковий інтерес нижче.

Опираючись на матеріали наукових досліджень вітчизняної та іноземної афіліації, можна виокремити особливості стратегічного управління інформаційною безпекою залежно від цілей та призначення та поділити останні на такі, як правове регулювання, інституційна структура, міжнародна співпраця та використання інновацій.

Правове регулювання як особливість стратегічного управління інформаційною безпекою передбачає наявність відповідного нормативного інструментарію, за допомогою якого здійснюється управління інформаційною та кібербезпекою водночас. Так, наприклад, як ми зазначали раніше, у США регулювання стратегічним управлінням інформаційною безпекою здійснюється за допомогою Закону про обмін інформацією про кібербезпеку 2015 р. (Cybersecurity Information Sharing Act, CISA 2015), Виконавчий наказ Президента США 14028 «Підвищення кібербезпеки країни» 2021 (Executive Order 14028 «Improving the Nation's Cybersecurity» 2021) та Закон про Агентство з кібербезпеки та безпеки інфраструктури 2018 р. (Cybersecurity and Infrastructure Security Agency Act 2018), а у ЄС – із використанням Загального регламенту про захист даних 2016 р. (GDPR 2016), Регламенту про кібербезпеку 2019 р. (Cybersecurity Act 2019) та Стратегії ЄС з кібербезпеки 2020 р. (EU Cybersecurity Strategy 2020). Цим, до слова, відзначається різниця та ідеологічна розгалуженість у регулюванні інформаційного простору та процедурної складової забезпечення безпеки даних та інформації всередині держави як елемента стійкості у питаннях протидії внутрішнім та зовнішнім загрозам.

Інституційна структура у якості особливості стратегічного управління інформаційною безпекою означає та передбачає реалізацію стратегічних цілей у галузі інформаційної безпеки за допомогою агенцій, органів та установ особливої юрисдикції. Такими органами у США є Агентство з кібербезпеки та безпеки інфраструктури (CISA), у ЄС – Європейська агенція з кібербезпеки (ENISA), у Великобританії – Національний центр кібербезпеки (NCSC).

Міжнародна співпраця та її роль у формуванні стратегічного управління інформаційною безпекою розвинених держав світу як характерна особливість даного процесу насамперед передбачає ототожнення безпеки даних із глобальною безпекою. Такий підхід першочергово вимагає взаємодії між державами, міжнародними організаціями та приватним сектором, засадничим

кластером ініціювання котрої є боротьба з інформаційними та кіберзлочинами. Юридичним та нормативно-правовим фактом, що де-факто детермінує наявність подібного взаємозв'язку, є Будапештська конвенція про кіберзлочинність від 23.11.2001 р., що встановлює стандарти та визначає архітектуру взаємодії між державами у рамках інтернаціонального співробітництва.

Заключною складовою особливостей стратегічного управління інформаційною безпекою можемо визначати використання інновацій. Це, зокрема, засоби інформаційно-комунікаційних технологій (ІКТ) та штучного інтелекту (ШІ), що підлягають використанню та застосуванню в аспекті адміністрування засобів контролю та нагляду за національним інформаційним простором. Використання зазначеного виду механізмів управління інформаційним простором, як правило, гарантує вищий рівень оперативності реагування на виклики та загрози інформаційній безпеці в умовах сьогодення та базується на необхідності неухильного усунення наявних колізій регулювання даної галузі на внутрішньодержавному рівні.

На основі проаналізованих у п. 4.1 Розділу IV даного дисертаційного дослідження характеристик узагальнення сутності, мети та особливостей стратегічного управління забезпеченням інформаційної безпеки крізь призму міжнародних норм та практик забезпечення інформаційної безпеки можемо зробити висновок про те, що зазначена діяльність є одним із ключових напрямів державного управління, спрямованим на захист національних інтересів в умовах стрімкого розвитку цифрових технологій та зростання інформаційних загроз.

Сутність стратегічного управління інформаційною безпекою полягає в побудові комплексної системи захисту інформаційного простору, яка включає політичні, правові, технічні, економічні та соціальні аспекти. Такі системи орієнтовані на протидію кіберзагрозам, забезпечення конфіденційності даних, підтримку цифрової інфраструктури та формування довіри суспільства до

інформаційних технологій.

Мета полягає у забезпеченні національної безпеки, стимулюванні інноваційного розвитку, захисті прав громадян, критичної інфраструктури та сприянні міжнародній співпраці у сфері інформаційної безпеки. Розвинені держави, як-от США, Велика Британія, ЄС, Ізраїль та Китай, адаптують свої стратегії до національних пріоритетів і викликів, зберігаючи спільні орієнтири на глобальну координацію.

Наостанок, особливості стратегічного управління інформаційною безпекою, залежно від цілей та призначення, передбачають використання таких механізмів управління, як правове регулювання, інституційна структура, міжнародна співпраця та використання інновацій.

4.2. Розвиток інституційних механізмів забезпечення інформаційної безпеки у системі публічного управління

У даному пункті дисертаційного дослідження ми пропонуємо сконцентрувати власну наукову та науково-доктринальну зацікавленість не лише на питаннях прикладів інституційного співробітництва іноземних держав у галузі інформаційної безпеки, але й на факторах, що першим чином детермінують ґенезу давного явища в практичному вимірі. Останні, відтак, потребують більшою мірою теоретико-аналітичного опрацювання, з чого, власне, ми і пропонуємо стисло розпочати.

Розглядаючи прямі та опосередковані підстави та чинники виникнення такого явища та феномену, як «глобальний характер інформаційної безпеки», американський дослідник-теоретик в галузі державного управління М. Дж. Робертс [272, с. 86] зазначив, що факт набуття інформаційною безпекою глобального характеру в позитивному сенсі спровокував розвиток цифрових технологій, залежність суспільства від інформаційних систем та міжнародну

інтеграцію в даній галузі. Останнє перелічене, в свою чергу, породило сутнісну та теоретико-практичну видозміну підходів до формування інституційної інфраструктури інформаційної безпеки. Інституційні можливості та ризики питання глобалізації інформаційної безпеки, на наш погляд, у даному випадку виступають екстрактивним доповненням до процесу архітектування інформаційної безпеки в рамках співробітництва та взаємодії (даний кластер буде проаналізовано нижче за текстом).

Тобто, у сучасній науковій та управлінській думці феномен глобального виміру інформаційної безпеки трактується як закономірний наслідок трансформаційного розвитку людства, де інформація перетворилася на ключовий ресурс політичного, економічного та культурного впливу. Сформувалася цілісна парадигма, в межах якої інформаційна безпека перестала бути внутрішньою функцією держави і почала сприйматися як частина ширшої системи глобальної взаємодії, у якій переплетені економічні, технологічні та гуманітарні складові.

Аналізуючи дану позицію можемо також зробити проміжний умовивід, що глобалізація інформаційного простору створює нову реальність, у якій межі між внутрішнім і зовнішнім середовищем фактично розмиваються. Це вимагає не лише перегляду класичних моделей управління безпекою, але й розроблення інтегрованих концепцій, здатних забезпечити баланс між відкритістю цифрового середовища та потребою у його контролі. У такому підході акцент зміщується від оборонної парадигми до управлінсько-профілактичної, що передбачає формування систем раннього реагування, підвищення стійкості критичної інфраструктури, розвиток аналітичних і комунікаційних механізмів.

На наш погляд, тут М. Дж. Робертс розглядає глобальний характер інформаційної безпеки як індикатор рівня зрілості міжнародних відносин у цифрову епоху. З одного боку, посилюється взаємозалежність держав, що сприяє створенню спільних стандартів, протоколів та етичних рамок у сфері кіберзахисту. З іншого — підвищується вразливість національних систем до

зовнішніх інформаційних впливів, що змушує держави шукати нові форми колективного реагування та обміну інформацією. Даний процес охоплює як урядові, так і позаурядові рівні — міжнародні організації, наукові консорціуми, приватні технологічні компанії, громадянські ініціативи.

Також, у розглянутому нами його науковому напрацюванні приділено увагу взаємозв'язку глобальної інформаційної безпеки з поняттям інформаційного суверенітету. Під впливом глобалізаційних процесів класичне уявлення про суверенітет зазнало змін: тепер воно все частіше тлумачиться не як ізоляційна здатність держави, а як уміння забезпечити власну автономію в умовах відкритого обміну даними та транскордонних інформаційних потоків. Це зумовлює потребу у виробленні збалансованих управлінських стратегій, де поєднуються інтереси національної безпеки з вимогами глобальної взаємодії.

Відмічаємо також і перехід на більш критичний підхід, згідно з яким глобалізація інформаційної безпеки несе в собі ризики надмірної стандартизації, централізації контролю над даними та втрати державами можливості самостійно визначати власну політику у сфері інформації. У цій площині актуальним стає питання про пошук нових моделей співіснування глобального і національного рівнів безпеки, про створення системи динамічної рівноваги, яка б дозволяла одночасно зберігати відкритість і гарантувати стійкість.

Отже, у ширшому значенні, глобальний характер інформаційної безпеки відображає тенденцію до формування спільного інформаційного простору людства, що функціонує за принципами взаємозалежності, комунікаційної мобільності та технологічної інтегрованості. Цей простір стає не лише середовищем обміну даними, але й сферою формування нових соціальних і політичних відносин, що у свою чергу впливають на саму природу державного управління. Інформаційна безпека, отже, перетворюється на комплексний соціально-управлінський феномен, який одночасно включає у себе політичні, правові, етичні та культурні аспекти.

Таким чином, узагальнюючи підхід М. Дж. Робертса щодо трактування поняття глобального характеру інформаційної безпеки, можна стверджувати, що глобалізація інформаційної безпеки є не просто техніко-технологічним процесом, а глибокою управлінською трансформацією, що формує нову архітектоніку світової системи. Вона засвідчує перехід від фрагментарних національних політик до інтегрованих форм міжнародного співіснування, де безпека постає не як засіб ізоляції, а як механізм взаємодії та розвитку.

Інституційні можливості глобального характеру інформаційної безпеки включають в себе розвиток багатосторонньої співпраці між державами, інтеграцію державно-приватного партнерства у галузі забезпечення інформаційної сталості та стабільності держав, інвестиційно-технологічне та людсько-ресурсне забезпечення належного рівня ефективності архітектування інформаційної безпеки та, наостанок, контексти удосконалення нормативно-правової бази з метою реалізації принципів оперативного реагування на обставини, що потребують державного та державно-інституційного втручання у кластери національної політики у зазначеній сфері [75, с. 15]. Надалі ми пропонуємо зупинитися на вивченні особливостей зазначених інституційних можливостей глобального характеру інформаційної безпеки з точки зору теорії та практики публічного управління та адміністрування.

Розвиток багатосторонньої співпраці у якості інституційної можливості, що визначає та детермінує глобальність інформаційної безпеки як явища та фактору об’єктивної дійсності, спрямований на урахування можливостей ділитися досвідом і створювати спільні стандарти інформаційно-безпекового середовища міждержавного значення [76, с. 14]. Більше того, у дослідженні В. Ф. Ургесси [290, с. 12-13] відмічається, що «багатостороння співпраця у сфері інформаційної безпеки є ключовим компонентом глобальної стратегії захисту від кіберзагроз, а розвинені держави світу активно підтримують цю ідею, оскільки сучасний інформаційний простір не має чітких кордонів, а загрози, з якими стикаються країни, часто носять транснаціональний характер». На наш

погляд, подібне трактування проблеми розвитку багатосторонньої співпраці у рамках моделі інституційної глобалізації процесу схоронності даних на міжнародному рівні являє собою універсальний формат концепції впливу на інформаційний простір із використанням позитивного впливу на галузь, що підкреслює комплексний та універсальний характер інформаційної безпеки та її транснаціональне значення (адже міжнародна інформаційна безпеки у даному випадку = безпеці кожної із держав міжнародної спільноти окремо, що підкреслює необхідність налагодження зв'язків одна з одною заради спільної цілі – внутрішньої безпеки, заснованої на взаємній ресурсній залежності).

Фактично, у ширшому аналітичному контексті багатостороння співпраця постає не лише як практичний інструмент обміну технологіями, методологіями та досвідом, а й як фундаментальна стратегічна парадигма, яка визначає характер глобального інформаційного середовища. Цей процес охоплює комплекс взаємопов'язаних напрямів — від створення спільних стандартів кіберзахисту, процедур раннього попередження та реагування на загрози до формування узгоджених політик щодо регулювання обігу даних, захисту персональної інформації та протидії дезінформації. Співпраця в такому ключі сприяє підвищенню рівня колективної стійкості та зміцненню довіри між державами, що є критично важливим для підтримки безпеки у відкритому цифровому просторі.

Особливе значення набуває взаємозв'язок між національними стратегіями та міжнародними рамками регулювання, який формує багаторівневу систему координації. Саме через цей взаємозв'язок держави отримують змогу поєднувати власні інтереси з глобальними цілями безпеки, забезпечуючи, з одного боку, автономію у прийнятті рішень на внутрішньому рівні, а з іншого — синхронізованість дій із партнерами по міжнародних платформах. Такий підхід дозволяє не лише оптимізувати захисні механізми, але й створює передумови для розвитку спільних науково-технічних і освітніх програм, обміну інформацією про кіберзагрози та адаптації нормативних моделей до

швидко змінних умов глобальної інформаційної екосистеми.

Багатостороння співпраця в інформаційній безпеці також виступає фактором формування нового виду міжнародної взаємозалежності, де безпека кожної держави безпосередньо впливає на стабільність інших учасників системи. Така взаємозалежність підкреслює необхідність постійного моніторингу ризиків, проведення спільних навчань і відпрацювання кризових сценаріїв, а також впровадження адаптивних управлінських структур, здатних гнучко реагувати на зовнішні й внутрішні загрози.

У концептуальному вимірі багатостороння співпраця формує базис для розвитку системної інтеграції інформаційної безпеки на глобальному рівні. Вона дозволяє розглядати міжнародні стандарти не лише як регуляторні рамки, але й як платформу для об’єднання зусиль різних держав та інституцій, створюючи узгоджені моделі обміну даними, захисту критичної інфраструктури та протидії транснаціональним інформаційним загрозам. Таким чином, багатостороння співпраця постає як центральний концептуальний елемент у побудові стійкого, інтегрованого та динамічного глобального середовища інформаційної безпеки, що одночасно враховує інтереси національної безпеки та колективної стабільності міжнародної спільноти.

Розглядаючи та аналізуючи феномен багатосторонньої співпраці у якості інституційної можливості, що визначає та детермінує глобальність інформаційної безпеки як явища та фактору об’єктивної дійсності в державно-управлінському вимірі, необхідно також зупинитися на перевагах останньої, адже такими передвизначається практичний аспект транснаціонального співробітництва у даній галузі, котрий ми розглядатимемо далі у п. 3.2 Розділу ІІІ зазначеного дисертаційного дослідження. До них, згідно матеріалів однієї із іноземних праць згаданого вище М. Дж. Робертса [272, с. 87-88], належить координаційна системність даного процесу, розподіл відповідальності між акторами (учасниками) процесу забезпечення інформаційної безпеки на транснаціональному рівні та, зокрема, аспект ефективної протидії

транснаціональним загрозам.

Питання системної координації як феномену багатосторонньої співпраці у якості інституційної можливості, що визначає та детермінує глобальність інформаційної безпеки як явища та фактору об'єктивної дійсності в сегменті публічного управління та адміністрування, розглядається з позиції наявності спільних стандартів та процедур, що дозволяють уникати розбіжностей у регулюванні та посилювати взаємну довіру між державними органами різних держав [272, с. 87].

Розподіл відповідальності як сегментарний елемент феномену багатосторонньої співпраці у якості інституційної можливості, що визначає та детермінує глобальність інформаційної безпеки як явища та фактору об'єктивної дійсності в публічно-управлінській площині, має на меті опцію об'єднання ресурсів країнами задля вирішення спільних проблем, знижуючи індивідуальне навантаження [272, с. 87].

Контекст ефективної протидії транснаціональним загрозам у якості частини багатосторонньої співпраці в рамках інституційної можливості, що визначає та детермінує глобальність інформаційної безпеки як явища та фактору об'єктивної дійсності в публічному управлінні та адмініструванні, в свою чергу, з позиції теорії державно-управлінського вчення заснований на презумпції багатосторонньої співпраці як джерела забезпечення швидкого обміну інформацією та координації заходів із формування інформаційної цілісності та сталості державного апарату [272, с. 87].

Надалі пропонуємо сконцентруватися на безпосередніх практичних елементах інституційних можливостей глобального характеру інформаційної безпеки. Для цього необхідно здійснити аналіз прикладів транснаціонального інституційного та законодавчого співробітництва, що має місце між США, ЄС та іншими державами.

У даному контексті, зокрема, необхідно звертати увагу на способи, засоби та механізми, за допомогою яких розвинені держави світу реалізують ті

чинники, що є теоретичною основою процесів позитивної інституціоналізації інформаційної безпеки, котрі ми зазначали та розглядали вище (координаційна системність процесу, розподіл відповідальності між акторами (учасниками) процесу забезпечення інформаційної безпеки на транснаціональному рівні та аспект ефективної протидії транснаціональним загрозам).

Так, сприяння міжнародній координації багатосторонньої співпраці як інституційна можливість реалізовується розвиненими державами світу на основі проєктної та юридико-правової координації. Наприклад, за допомогою Глобального форуму із кіберекономіки (Global Cybersecurity Forum) країни (формальне членство не передбачене, проте ключовими акторами в даному випадку виступають США, Велика Британія, Канада, Європейський Союз, Китай, Індія, Японія, Австралія та Південна Корея) об'єднують власні можливості з метою створення спільних стандартів у галузі протидії проявам посягань на інформаційну безпеку конкретної держави, а також на глобальну (транскордонну) безпеку даних та інформації, що може бути предметом протиправних дій від третіх сторін [272, с. 88].

Окрім підходів, що ми розглянули вище у рамках контексту сприяння міжнародній координації багатосторонньої співпраці як інституційної можливості глобального характеру інформаційної безпеки, остання також підлягає забезпеченню на більш локальному, внутрішньому рівні. Одним із таких прикладів є інтеграція державно-приватного партнерства у галузі забезпечення інформаційної сталості та стабільності держав як інституційна можливість глобального характеру інформаційної безпеки, на детальному огляді котрого ми зупинимося далі.

Контекст інтеграції державно-приватного партнерства у галузі забезпечення інформаційної сталості та стабільності держав як інституційна можливість глобального характеру інформаційної безпеки натомість полягає у технологічному стимулюванні, спрямованому саме на інформаційний державний сектор. Інституційна можливість у даному випадку означає

наявність забезпеченого ефективного розподілу ресурсів, знань і технологій між державними органами та приватними компаніями, зокрема операторами критичної інфраструктури, котрі реалізують цілі державної політики щодо схоронності даних та збереження інформаційного суверенітету держави як складової суверенітету національного. Цим, де-факто, гарантується також контекст економічного стимулювання, адже державно-приватне партнерство, що є рушієм даної кластерної категорії взаємодії, засноване на залученні приватних виконавців за державний кошт на взаємовигідних для обох сторін умовах. Практичні приклади такої взаємодії будуть розглянуті нами нижче.

Зокрема, впадає в око наявність ініціативи щодо співпраці у галузі забезпечення інформаційної безпеки від розвинених держав світу. Згаданий раніше орган – Агентство з кібербезпеки та безпеки інфраструктури США (Cybersecurity and Infrastructure Security Agency (CISA), наприклад, відповідно до положень, знову-таки, згаданого нами раніше Закону про кібербезпеку та безпеку інфраструктури 2018 р. (Cybersecurity and Infrastructure Security Act (CISA) of 2018) (зокрема, у Sec. 2202, 2209, 2215) ініціює співпрацю з приватними компаніями у сферах обміну інформацією, кібернавчання та реагування на інциденти.

Потрібно також зауважити, що власне процес інтеграції державно-приватного партнерства у галузі забезпечення інформаційної сталості та стабільності держав як інституційна можливість глобального характеру інформаційної безпеки на практичному рівні має власною ознакою обмін інформацією. Такий обмін, як правило, має або нормативне, або інституційне рамкування, і у випадку із кіберзагрозами та загрозами інформаційній безпеці у даному контексті можемо говорити про приклад ЄС, де на задоволення зазначений потреб функціонує Атлас кібербезпеки (EU Cybersecurity Atlas). Мета останнього, відповідно до ст. 5 (Article 5) Регламенту (ЄС) № 2019/881 Європейського Парламенту та Ради від 17 квітня 2019 року про Агентство Європейського Союзу з кібербезпеки (ENISA) та сертифікацію кібербезпеки

інформаційно-комунікаційних технологій (Акт про кібербезпеку) (Regulation (EU) 2019/881 of the European Parliament and of the Council of 17 April 2019 on ENISA (the European Union Agency for Cybersecurity) and on information and communications technology cybersecurity certification and repealing Regulation (EU) No 526/2013 (Cybersecurity Act), полягає у сприянні співпраці між державними та приватними організаціями, а також сприянні розвитку спільних підходів до управління ризиками та обміну інформацією про загрози.

З огляду на проаналізовані підходи до регулювання та стратегічної конкретизації сегменту процес інтеграції державно-приватного партнерства у галузі забезпечення інформаційної сталості та стабільності держав у глобальному вимірі відзначимо наявність двох, пропорційно відмінних та, водночас, ідеологічно поєднаних підходів до стандартизації зазначеного сегменту. Так, підхід США із «куруванням» діяльності Агентства з кібербезпеки та безпеки інфраструктури США (Cybersecurity and Infrastructure Security Agency (CISA) Законом про кібербезпеку та безпеку інфраструктури 2018 р. (Cybersecurity and Infrastructure Security Act (CISA) of 2018) відрізняється від концепції ЄС, де ініціатива Атлас кібербезпеки (EU Cybersecurity Atlas) регламентована Регламенту (ЄС) № 2019/881 Європейського Парламенту та Ради від 17 квітня 2019 року про Агентство Європейського Союзу з кібербезпеки (ENISA) та сертифікацію кібербезпеки інформаційно-комунікаційних технологій (Акт про кібербезпеку) (Regulation (EU) 2019/881 of the European Parliament and of the Council of 17 April 2019 on ENISA (the European Union Agency for Cybersecurity) and on information and communications technology cybersecurity certification and repealing Regulation (EU) No 526/2013 (Cybersecurity Act), проте сутнісні цілі обох цих процесів полягають у підвищенні рівня державно-приватної взаємодії у секторі забезпечення інформаційної та, відповідної, державної безпеки.

Потрібно зауважити, що інформаційна безпека як стала категорія публічного управління та адміністрування, а саме її глобальний контекст та

характер у розрізі потенційних інституційних можливостей даного процесу може бути розкрита за допомогою інших, екстрактивних категорій його розуміння. Одним із таких є інвестиційно-технологічне та людсько-ресурсне забезпечення належного рівня ефективності архітектування інформаційної безпеки, котре ми далі проаналізуємо з власне наукової та популярно-практичної позицій.

Узагальнено, інвестиційно-технологічне та людсько-ресурсне забезпечення належного рівня ефективності архітектування інформаційної безпеки як інституційна можливість може бути дефініційовано як залучення державами відповідного роду та категорії ресурсів, спрямованого на забезпечення інформаційної безпеки як процесу державного управління та, водночас, здатності держави реагувати на відповідного роду виклики та трансформації. Першочергового значення у даному випадку набуває підвищення здатності протидіяти кіберзагрозам, адже саме це є сегментарною детермінантою внутрішньої та зовнішньої захищеності держави (як правило, кібератаки є або інтегративним складником, або «трампліном» до розширення агресивних, загарбницьких дій, що активно продемонстровано прикладом збройної агресії рф проти України у гібридному (2014-2022 р.) та повномасштабному (2022-дотепер) форматах.

Країнами, на прикладах котрих доцільно в даному випадку сконцентрувати власну увагу, є Велика Британія та Ізраїль.

Зокрема, у Великій Британії розвиненим є концептуальний підхід державного інвестування у технологічний розвиток держави. Останній регламентується на нормативно-правовому рівні : у Національній стратегії кібербезпеки 2022-2030 р. (National Cyber Security Strategy 2022-2030) презюмовано необхідність створення технологічних інноваційних центрів та підтримки дослідницьких ініціатив для покращення безпеки критичної інфраструктури, а також безпеки даних та інформації як критичного вузла державної діяльності та захищеності секретних даних (Розділи 2 та 4, Місії 1 та

2 (Chapter 2, 4 Missions 1-2).

Спостереження архітектури та структурного забезпечення формування інформаційно-безпекового середовища з позиції людського ресурсу та інноваційності у Великій Британії також дозволяє говорити про акцент не лише на нормативному регулюванні даного процесу (що, як правило, відзначається статичністю та не завжди підпадає під реальні завдання, що формуються у інформаційно-безпековому та державно-безпековому просторах), а й належній кадровій підготовці, що існує окремо від законодавства та передбачає реалізацію принципу кібернетичної освіченості населення з метою належного рівня респонденції на подібного рівня генерації загрози незалежно від рівня останніх. Прикладом такої ініціативи у Великій Британії є стартап «CyberFirst», спрямований на навчання молоді основам кібербезпеки, в рамках якого державні та приватні організації спільно фінансують проєкти із підготовки кадрів у сфері інформаційної безпеки та, зокрема, інфраструктурної безпеки держави.

У Ізраїлі, натомість, акценти у розрізі інвестиційно-технологічного та людсько-ресурсного забезпечення належного рівня ефективності архітектування інформаційної безпеки як інституційної можливості мають поєднане, проте дещо відмінне поле трактування та забезпечення. Тут також присутня політика державних інвестицій у технології, що допомагає реалізовувати проєкти із забезпечення інформаційного безпекового середовища, проте вони не мають прямого нормативного окреслення та, за звичаєвою моделлю, здебільшого покладені на відповідальну інституцію – Національний кібердиректорат (Israel National Cyber Directorate, INCD).

Водночас, за допомогою стимулювання приватного сектору у Ізраїлі стає можливим не лише впровадження стандартів державно-приватної взаємодії, але й орієнтації на людські ресурси в процесі забезпечення безпеки даних та інформації, адже в сегменті даного співробітництва створюються «кіберкластери» – інноваційні хабів, де державні та приватні інституції спільно

розробляють рішення для інформаційної безпеки, а Інвестування у навчальні програми для підготовки фахівців відбувається через університети, спеціалізовані центри та програми під егідою безпосередньо Національного кібердиректорату (Israel National Cyber Directorate, INCD), чим гарантується не лише інноваційність, але й зацікавленість у досягненні кінцевої мети у вигляді захисту чутливих та важливих з точки зору державного функціонування даних, що знаходяться у рамках державного реєстрування та обробки.

Заключним елементом інституційних можливостей глобального характеру інформаційної безпеки є контексти удосконалення нормативно-правової бази з метою реалізації принципів оперативного реагування на обставини, що потребують державного та державно-інституційного втручання у кластери національної політики у зазначеній галузі. Нижче проаналізуємо сегментовані моделі даного процесу.

Фактично, зазначений процес включає в себе опрацювання усіх проаналізованих можливостей та елементів удосконалення державного управління інформаційною безпекою на внутрішньому та міжнародному (зовнішньому) рівнях. Юридично та нормативно, даний процес можна ототожнити та охарактеризувати як здатність держав і міжнародних інституцій ефективно адаптуватися до швидкоплинних змін у інформаційному просторі, також – кіберпросторі як складовій першого, прецедентів кібернетичного терору, зловживання даними або незаконного втручання у державні та закриті реєстри шляхом вчинення актів кібертероризму, кінцевим об’єктом якої так або інакше є саме інформаційна безпека як елемент державної захищеності.

Окрім проаналізованої вище інформації, що стосується аспектів інтенсифікації міждержавної взаємодії та співробітництва між державами у галузі інформаційної безпеки та прикладів впровадження інновацій в управління інформаційним простором шляхом залучення відповідних ресурсів (Велика Британія, Ізраїль), ключового, на наш погляд, значення у контексті потенційних мірил та меж удосконалення нормативно-правової бази з метою

реалізації принципів оперативного реагування на обставини, що потребують державного та державно-інституційного втручання у кластери національної політики у зазначеній галузі, набуває технологічна адаптація нормативно-правової бази.

На переконання Д. Макропулу та В. Папаконстантіну [263, с. 215], стратегічного значення в питаннях оперативного та, водночас, ефективного реагування на виклики, генеровані втручанням у інформаційний простір держав на сучасному етапі, зокрема, загострення міжполітичних (геополітичних) елементів напруги набуває процес оновлення законодавства відповідно до нових технологій. Такими технологіями можна називати штучний інтелект (ШІ), інтернет речей (IP або IoT – Internet of Things) та інформаційно-комунікаційні технології (ІКТ).

У ширшому концептуальному контексті розглянутий підхід підкреслює необхідність системного та комплексного осмислення того, як технологічні інновації трансформують не лише оперативні процедури захисту інформаційного простору, а й принципи та парадигми правового регулювання. В умовах стрімкого розвитку цифрових технологій та їх глобального проникнення у всі сфери суспільного життя, традиційні механізми законодавчого забезпечення інформаційної безпеки перестають бути достатньо ефективними. Сучасна технологічна динаміка вимагає від законодавця, аналітичних центрів та державних інституцій постійного оновлення норм і правил, формування адаптивних підходів до регулювання процесів збору, обробки, зберігання та поширення інформації.

Штучний інтелект у цьому контексті виступає не лише як технологія, що здатна автоматизувати обробку даних і прогнозування загроз, а й як фактор, який змінює саму природу інформаційного поля. Використання алгоритмічних систем, машинного навчання та автоматизованих рішень у сфері безпеки створює нові можливості для контролю інформаційних потоків, водночас відкриваючи потенційні ризики для приватності та захисту персональних

даних. Законодавство в таких умовах повинно передбачати механізми прозорості алгоритмів, аудит технологій та відповідальність за порушення інформаційно-безпекових стандартів у цифровому середовищі, забезпечуючи баланс між інноваційним розвитком і захистом прав громадян.

Інтернет речей, як ще один важливий технологічний сегмент, посилює потребу у формуванні інтегрованих моделей законодавчого реагування, оскільки значна частина критично важливих інфраструктурних систем — від енергетики та транспорту до охорони здоров'я та державного управління — зараз включає пристрої, які обмінюються даними у реальному часі. Ці технологічні елементи, з одного боку, відкривають нові можливості для оперативного моніторингу та управління ресурсами, а з іншого — створюють додаткові канали для потенційних кібератак, спроб втручання та маніпуляцій інформацією. Тому законодавче оновлення у сфері ІР має враховувати специфіку масового підключення пристроїв до мережі, стандарти безпеки комунікаційних протоколів, а також принципи відповідальності виробників та операторів систем.

Інформаційно-комунікаційні технології в даному підході розглядаються як базисна платформа, що дозволяє забезпечувати міждержавну інтеграцію та співпрацю у сфері інформаційної безпеки. Водночас, ІКТ відкривають нові горизонти для організації та функціонування національних інформаційних просторів, що потребує законодавчого визначення меж доступу, контролю, захисту даних та протидії дезінформації. Такий підхід дозволяє формувати інтегровану систему захисту, де державні органи, комунікаційні компанії та суспільство у цілому взаємодіють для забезпечення ефективного реагування на загрози, що мають транснаціональний характер.

Власне, стратегічна значимість оновлення законодавства полягає в його здатності не лише реагувати на існуючі загрози, а й передбачати потенційні ризики. Це забезпечує формування превентивних заходів, що зменшують ймовірність серйозних інформаційних криз та критичних втрат для держави та

суспільства. Водночас адаптація нормативної бази до технологічних змін підвищує здатність держави здійснювати координацію між державними структурами, приватними суб'єктами та міжнародними партнерами у сфері інформаційної безпеки, що особливо важливо в умовах геополітичної напруженості.

На наш погляд, цей підхід демонструє комплексне бачення взаємозв'язку між технологічними інноваціями, правовим регулюванням та стратегіями державного реагування. Він підкреслює, що ефективна інформаційна безпека на сучасному етапі неможлива без інтеграції технічних, організаційних та правових механізмів, а також без постійного переосмислення нормативної бази у відповідності до швидко змінних умов цифрового середовища. При цьому підкреслюється, що законодавче оновлення має бути не лише реактивним, а й проактивним, забезпечуючи довгострокову стійкість національних інформаційних систем і формуючи основу для координації з міжнародними стандартами та практиками.

Таким чином, підхід Д. Макропулу та В. Папаконстантіну можна розглядати як концептуально цілісний, оскільки він поєднує технологічний, правовий і стратегічний виміри, що забезпечує комплексну систему адаптації до викликів сучасного інформаційного середовища. У нашій оцінці, саме така багаторівнева інтеграція стає ключовою умовою побудови ефективного механізму забезпечення інформаційної безпеки, що здатен реагувати на сучасні геополітичні виклики та технічні трансформації інформаційного поля, формуючи таким чином надійну основу для національної стабільності та суверенітету.

Зауважимо, що у перспективі застосування зазначеного підходу до формування законодавчої та нормативної політики дозволяє створювати більш гнучкі моделі регулювання, що враховують специфіку різних секторів економіки, суспільного життя та критично важливих інфраструктур. Це, у свою чергу, сприяє розбудові комплексної системи інформаційної безпеки, де

державні органи, приватний сектор і громадянське суспільство взаємодіють у тісній координації, забезпечуючи захист інформаційного простору та національної безпеки в умовах швидких технологічних та геополітичних змін.

Від себе також додамо, що використання останніх у галузі інформаційної безпеки може мати два різко відмінних прояви позитивного та негативного застосування : допомоги виявлення кіберпорушників та детекції порушень системи інформаційної безпеки та, відповідно, використання зазначеного устаткування задля архітектування та генерації кібератак та атак, спрямованих на порушення інфраструктурної цілісності безпеки держави та безпеки і схоронності інформації та ресурсів, що адмініструють відповідні державні бази та ін. Тому сутнісної необхідності у даному випадку набуває саме використання позитивних можливостей, що пропонує штучний інтелект (ШІ), інтернет речей (IP або IoT – Internet of Things) та інформаційно-комунікаційні технології (ІКТ) задля забезпечення безпеки даних та інформації. Прикладом такого, на наш погляд, є положення, відображені у Розділах 2 та 4, Місіях 1 та 2 (Chapter 2, 4 Missions 1-2 Національної стратегії кібербезпеки Великобританії 2022-2030 р. (UK National Cyber Security Strategy 2022-2030).

Окрім інституційних можливостей, глобальний характер інформаційної безпеки як стала державно-управлінська, правова та філософсько-правова конструкції наділений певними ризиками, що походять від його правової природи та теоретичної парадигми застосування.

Розглянемо останні побічно далі, коротко надавши їм класифікаційну характеристику. Так, до ризиків глобального характеру інформаційної безпеки, відповідно деяких іноземних та вітчизняних наукових досліджень у даній галузі [263], належить кіберзлочинність та асиметричні загрози, проблеми розуміння суверенітету, аспект ескалації кіберконфліктів та недостатня глобальна регуляція.

Кіберзлочинність та асиметричні загрози як складова ризиків глобального характеру інформаційної безпеки насамперед являє собою фактор наявності

імовірності атак на інформаційні реєстри, критичну інформаційну інфраструктуру держави, персональні дані користувачів або чутливу інформацію, що може складати державну таємницю [263, с. 245]. Зазначена категорія більшою мірою має філософський характер та спрямована на усвідомлення факту того, що досконалі законодавчі підходи та інституційно-законодавча взаємодія, як це є в США та ЄС, не позбавляє потенційної опціональності необхідності реагувати на кібератаки та кіберзлочинну поведінку по відношенню до держави. Сутнісне розуміння даного підходу, в першу чергу, має передбачати акцент на постійному вдосконаленні інформаційного законодавства та законодавства, що прямо або опосередковано регулює питання збирання, обігу, використання інформації тощо.

Особливості та проблеми розуміння суверенітету, в свою чергу, є категорією, що переважно виходить та походить від стилістики та специфіки державного управління у конкретній державі. Прикладом, що у даному випадку доцільно застосувати, є Китай, де інформаційні можливості та можливості діджиталізації, глобального прогресу як правило використовуються апаратом публічного управління не з метою розширення можливостей міжнародної взаємодії та співробітництва у галузі інформаційної безпеки, а з метою обмеження можливостей міжнародної координації, фокусування на внутрішньому контролі та цензурі. Відтак, це породжує прецедент використання можливостей «цифрового суверенітету» в інтересах державного апарату, тоді як мета демократичного управлінського регулювання полягає в представленні інтересів громадянського суспільства через владні органи у якості представницьких. Така модель дозволяє нам говорити про те, що інформаційна безпека у сутності та сукупності своїх складових може розглядатися як негативний прояв (елемент) залежно від контексту застосування її характерних рис.

Ескалація кіберконфліктів як сутнісна складова потенційних ризиків глобального характеру інформаційної безпеки передбачає можливість (опцію)

фактору потенційної мілітаризації інформаційного простору. Факторами, що на теоретичному та практичному рівні можуть впливати на зазначену конструкцію, є умови, в яких певній державі доводиться провадити власну інформаційну політику та, водночас, провадити захист власного інформаційного простору. Так, Ізраїль формує власну інформаційно-безпекову політику на концепції, що передбачає використання військового контексту людського ресурсу (наявність підрозділів 8200 та 81, сегментом діяльності котрих є елітна розвідувальна служба, що спеціалізується на електронній розвідці та кібероперацїях, а також –технічна розвідка та розробка кіберзасобів, працюють над досягненням інформаційної безпеки держави у сучасному цифровому вимірі). Окрім безпосереднього факту позитивного впливу на інформаційну безпеку всередині держави внаслідок наявних кіберзагроз, зазначена модельна структура передбачає можливі ризики для превалювання мілітарних заходів впливу на інформаційну безпеку над державно-процедурними, що може загрожувати загальним демократичним засадам функціонування громадянського суспільства на засадах свободи слова, думки та дії індивіда.

Недостатність аспекту глобальної регуляції у якості ризику глобального характеру інформаційної безпеки, наостанок, може та повинна розглядатися як виклик для міжнародної спільноти у контексті реалізації стратегічних завдань даної сфери. Зокрема, відсутність єдиної глобальної нормативної бази у сфері кібербезпеки ускладнює запобігання міжнародним кіберзагрозам, а діяльність міжнародних організацій, як-от ООН чи НАТО (політико-глобальний та безпеково-мілітарний контексти) не можуть вплинути на належне конструювання позитивної парадигми даного сегменту.

Отже, проаналізовані особливості інституційних можливостей та ризиків глобального характеру інформаційної безпеки дозволили нам дійти наступних проміжних умовиводів.

Глобальний характер інформаційної безпеки є багатовимірним явищем,

що відображає інтеграцію сучасного світу, де інформаційні системи, цифрові технології та комунікаційна інфраструктура стають критично важливими елементами державного управління, економіки та суспільного життя. Інституційні можливості глобальної інформаційної безпеки полягають у розвитку міжнародної співпраці, інтеграції державного та приватного секторів, інвестиціях у технології та людські ресурси, а також у створенні ефективної нормативно-правової бази для оперативного реагування на кіберзагрози. Розвинені держави світу, такі як США, Велика Британія, ЄС та Ізраїль, демонструють приклади комплексного підходу до забезпечення інформаційної безпеки, поєднуючи стратегічне управління, науково-дослідницькі ініціативи, державно-приватне партнерство та міжнародну взаємодію.

Серед ключових інституційних можливостей варто виділити розвиток багатосторонньої співпраці, що базується на спільних стандартах і нормативних актах, таких як Директива NIS2 в ЄС чи міжнародні угоди в рамках ООН. Інтеграція державного та приватного секторів забезпечує адаптивність і стійкість інформаційних систем, дозволяючи об’єднати ресурси та експертизу для ефективного подолання кіберзагроз. Інвестиції в технології, створення інноваційних центрів і підтримка дослідницьких програм стають фундаментом для забезпечення технологічного лідерства у сфері інформаційної безпеки, особливо в таких країнах, як Велика Британія та Ізраїль. Водночас нормативно-правова база є важливим інструментом для врегулювання діяльності, пов’язаної з кібербезпекою, зокрема в аспектах оперативного реагування, державного регулювання та міжнародного співробітництва. Водночас, до ризиків глобального характеру інформаційної безпеки варто відносити кіберзлочинність та асиметричні загрози, проблеми розуміння суверенітету, аспект ескалації кіберконфліктів та недостатність глобальної регуляції.

4.3. Розробка комунікаційної стратегії як складової системи публічного управління інформаційною безпекою

Національне управління інформаційною безпекою держав, що є предметом нашого огляду у контексті визначення та аналізу критеріїв та складових міжнародних норм та практики забезпечення інформаційної безпеки має певні закономірності, способи та механізми реалізації – фактичного впровадження.

Поняття «комунікаційна стратегія» у контексті її аналізу як складової національного управління інформаційною безпекою можна розглядати крізь призму різних наукових позицій. На підставі аналізу наукових напрацювань вітчизняних та іноземних авторів [116, 238] можна дійти висновку, що останню найкраще визначати як інструмент забезпечення ефективного інформаційного захисту держави за допомогою легітимних інструментів. Такими легітимними інструментами у даних аналітичних працях названо організоване управління потоками інформації, стратегічні комунікації, інформаційну протидію загрозам та підтримку інформаційної стійкості суспільства.

Теоретичне розуміння комунікаційної стратегії як складової національного управління інформаційною безпекою також виходить з того, що у її рамках відбувається системне планування, забезпечене необхідністю врахування міжнародних стандартів кіберзахисту. Кіберзахист як категорія практичного застосування в рамках комунікаційного управління інформаційною безпекою, в свою чергу, є відповідником критерію універсального захисту даних, котрий має місце у діджиталізованому інформаційному просторі. Пріоритетом, в свою чергу, в даному випадку виступає формування довготривалих механізмів взаємодії між урядовими структурами, медіа, приватним сектором та громадянським суспільством для запобігання кіберзагрозам, дезінформації та інформаційним маніпуляціям.

Можна вважати, що комунікаційна стратегія як складова національного

управління інформаційною безпекою виконує роль реалізатора аспекту протидії інформаційним, політичним та безпековим кризовим явищам. Кінцевим завданням зазначеної активності є формування статусу довіри до влади, владних інституцій та відкритих джерел інформації в умовах загроз гібридного та реального форматів.

Перш ніж переходити до дослідження прикладів комунікаційних стратегій як складової національного управління інформаційною безпекою з позиції окремих законодавчих кейсів, доцільно зупинитися на аналізі основних концепцій інформаційної безпеки, що фактично детермінують побудову останніх.

Так, серед концепцій інформаційної безпеки, виходячи із наукових позицій К. Жадька [36, с. 24] та польської дослідниці Е. Степаненко [164, с. 523], доцільно виділяти концепцію цифрового суверенітету, концепцію інформаційного нейтралітету та концепцію стратегічних комунікацій.

Концепція цифрового суверенітету держави як складова національного управління інформаційною безпекою із теоретико-концептуального виміру базується на незалежності держави у галузі цифрових та інформаційних технологій. Реалізація такого принципу передбачає контроль над цифровою державною інфраструктурою, побудову ускладненої архітектури побудови комунікаційних мереж з метою контролю обігу даних, кінцевим завданням чого є недопущення посягань на інформацію відповідного рівня та виду.

Ключовим елементом концепції цифрового суверенітету держави як складової національного управління інформаційною безпекою є її технологічний компонент. Останній виражається у розвиткові та стимулюванні цифрових платформ, технологій хмарного (віддаленого, серверного) зберігання даних, а також – проведення аналітично-інноваційних досліджень у сфері зберігання інформації та забезпечення її схоронності від зовнішніх атак.

Економічний аспект концепції цифрового суверенітету держави як складової національного управління інформаційною безпекою, в свою чергу,

доповнює концептуальну модуль технологізації, описану вище. У її рамках засадничими питаннями державного управління стають ІТ-секторальні інновації, спрямовані на зменшення залежності від іноземного програмного забезпечення та апаратного забезпечення та інтеграцію цифрового суверенітету із навчанням його азам у державних економічно-розвиткових програмах [125, с. 523].

Концепція інформаційного нейтралітету, в свою чергу, в теоретичному вимірі та розумінні походить від і базується на забезпеченні балансування між національною безпекою та інформаційною відкритістю, що реалізується державою за допомогою впровадження політики невтручання у локальні та глобальні міжнародні конфлікти як керівною в публічно-управлінських процесах [36, с. 25].

Реалізація (фактичне запровадження) концепції інформаційного нейтралітету держави як складової національного управління інформаційною безпекою, в свою чергу, базується на розмежуванні та поєднанні підходу до міжнародної безпекової та кібербезпекової співпраці і невтручання у інформаційно-конфліктні ситуації, що мають місце на території інших держав [36, с. 23].

Як і у випадку із реалізацією принципів концепції цифрового суверенітету держави як складової національного управління інформаційною безпекою, концепція інформаційного нейтралітету має сегментованим мірилом власної реалізації технологічний складник. На відміну від концепції цифрового суверенітету, в межах реалізації концепції інформаційного нейтралітету на рівні техніко-технологічних інновацій держава працює над наданням вільного доступу до мережі Інтернет громадянам безвідносно до політичної або дискримінаційної політики. Цензура або блокування контенту без встановлених та визначених юридичних підстав, своєю чергою, забороняється та не застосовується [36, с. 23].

З точки зору теорії державного управління, безпосередня процедура

формування інформаційного нейтралітету як державної політики та державного курсу має одним із критеріїв наявність культурного аспекту. Реалізація такого потребує інформаційної освіти громадян. Інформаційна освіта громадян, на думку американської науковиці С. М. Штіцлейн [276, с. 97] є комплексною феноменологічною парадигмою, що включає в себе навчання здатностям критичного мислення, медіаграмотності та механізмів протидії фейковим новинам у населення та підтримку незалежних засобів масової інформації та громадських (медійних) ініціатив, що включає в себе реалізацію принципу свободи слова на інституційно-управлінському рівні.

У більш широкому концептуальному розумінні, інформаційна освіта громадян виступає не лише як освітній процес, але й як ключовий елемент формування національної інформаційної культури та колективного критичного усвідомлення. Вона спрямована на формування у громадян стійких навичок оцінювання достовірності інформації, аналізу її джерел, розпізнавання потенційних маніпуляцій та розуміння соціально-політичних контекстів, у яких поширюється інформація. Такий підхід забезпечує базис для розвитку активного громадянського суспільства, здатного ефективно реагувати на інформаційні виклики та загрози, а також здійснювати власний внесок у побудову безпечного інформаційного середовища.

Критичне мислення, як складова інформаційної освіти, виступає як інструмент оцінки не лише контенту повідомлень, але й мотивів, цілей та можливих наслідків їх поширення. Це створює передумови для формування відповідальної поведінки в інформаційному просторі, де громадяни не лише споживають інформацію, а й активно беруть участь у її створенні, поширенні та контролі за її достовірністю. У цьому сенсі інформаційна освіта стає невід’ємною складовою національної стратегії інформаційного нейтралітету, адже вона дозволяє створювати суспільство, здатне до самоорганізації та самоконтролю у сфері інформації.

Медіаграмотність, як ще один важливий компонент, передбачає освоєння

технологій аналізу інформаційних потоків, розпізнавання пропагандистських та дезінформаційних кампаній, а також розуміння принципів роботи сучасних медіаекосистем. Це дозволяє громадянам більш усвідомлено сприймати новини, соціальні повідомлення та цифровий контент, що в свою чергу зменшує ризик маніпуляцій та сприяє підвищенню рівня колективної інформаційної безпеки.

Не менш важливим є розвиток інституційної підтримки незалежних медіа та громадських ініціатив, які забезпечують плюралізм думок та доступ до альтернативної інформації. Держава, у цьому контексті, виконує роль координатора та гаранта принципів свободи слова, створюючи нормативні та організаційні передумови для забезпечення незалежності медіа, підтримки ініціатив громадянського суспільства, а також захисту від цензурного тиску та інформаційного домінування окремих суб'єктів.

Важливим аспектом є й інтеграція інформаційної освіти у формальні освітні програми та неперервне навчання дорослого населення. Така системність забезпечує формування у громадян безперервного навичкового та концептуального розвитку, здатності до швидкої адаптації у умовах динамічних інформаційних змін, включно з поширенням нових технологій комунікації, цифрових платформ та соціальних мереж. В результаті формується компетентне суспільство, яке не лише володіє навичками критичного аналізу інформації, але й усвідомлює власну роль у підтриманні національного інформаційного суверенітету та інформаційної стабільності.

З огляду на вищезазначене, інформаційна освіта громадян можна розглядати як багаторівневу, системну та інтегровану парадигму, що охоплює освітній, соціально-психологічний, технологічний та правовий аспекти. Вона поєднує індивідуальні компетенції та суспільні механізми саморегуляції інформаційного середовища, забезпечуючи баланс між свободою слова, правами громадян на інформацію та захистом від загроз дезінформації, маніпуляцій і пропаганди.

Таким чином, формування інформаційної освіти громадян виступає не лише необхідним компонентом державної політики щодо забезпечення інформаційного нейтралітету, але й фундаментальним інструментом побудови стійкого, інтегрованого та безпечного інформаційного простору, здатного забезпечити національну стратегію стійкості та протидії сучасним інформаційним викликам і трансформаціям цифрового середовища.

Концепція стратегічних комунікацій у системі реалізації основ національного управління інформаційною безпекою у теоретичному розумінні має власною основою кооперацію формату «держава та суспільство», що за певних умов підлягає експансіюванню на внутрішні правовідносини та міжнародні відносини із державами-партнерами з метою досягнення власних стратегічних цілей у сегменті державного регулювання та управління. Стратегічні комунікації в даному випадку виступають універсальною державно-управлінською та інформаційною ідеальною моделлю, що спрямована на досягнення принципів протидії дезінформації, гібридним інформаційно-безпековим маніпуляціям та атакам на інформаційну галузь та інформаційну інфраструктуру, котра є опорним джерелом захисту від теоретичного негативного впливу на національні інформаційні мережі та інформаційні канали, за допомогою яких громадяни (населення) споживають відповідний контент на засадах вільного доступу до інформаційних ресурсів.

Розглядаючи концепцію стратегічних комунікацій більш широко в контексті даного визначення, що ми надали вище, слід підкреслити, що вона виступає не лише як інструмент управлінської взаємодії держави та суспільства, але й як складна система соціальних, технологічних та культурних взаємозв’язків, спрямованих на забезпечення стійкості національного інформаційного простору. У своїй суті, стратегічні комунікації охоплюють широке коло процесів: планування, організацію, координацію та контроль інформаційних потоків, синхронізацію діяльності органів влади та незалежних медіа, моніторинг суспільної реакції на різні інформаційні впливи, а також

прогнозування потенційних загроз і вироблення відповідних контрзаходів.

Важливо зазначити, що стратегічні комунікації мають багатошарову структуру, яка включає правові, технологічні, соціально-психологічні та культурні компоненти. З правового боку вони спираються на систему законів і нормативних актів, що регламентують інформаційний простір та визначають межі державного втручання у сферу медіа та інформації. Технологічний аспект охоплює використання сучасних інформаційно-комунікаційних технологій, інструментів кіберзахисту, алгоритмів обробки даних та моніторингу інформаційних потоків, що дозволяє своєчасно виявляти загрози та реагувати на них. Соціально-психологічний компонент стосується формування у населення критичного сприйняття інформації, розвитку навичок медіаграмотності, а також створення умов для підвищення довіри до державних і громадських інституцій, що займаються інформаційною безпекою. Культурний рівень включає врахування історичних, мовних, регіональних та інших специфічних факторів, що визначають особливості сприйняття та поширення інформації в суспільстві.

Стратегічні комунікації у такому контексті виступають як комплексний механізм інтеграції державних стратегій та суспільних практик, де ключовим завданням є забезпечення балансу між правом громадян на вільний доступ до інформації та необхідністю захисту державного інформаційного суверенітету. Вони покликані створювати прозорі та зрозумілі канали комунікації, сприяти формуванню довіри між владою та населенням, а також забезпечувати швидке реагування на кризові інформаційні ситуації.

Ще одним важливим аспектом є роль стратегічних комунікацій у міжнародному контексті. В умовах глобалізації та цифровізації інформаційних потоків будь-яка держава стикається з транскордонними загрозами, включно з кібератаками, дезінформаційними кампаніями та спробами впливу на громадську думку. Стратегічні комунікації дозволяють виробляти узгоджені позиції з міжнародними партнерами, створювати спільні стандарти реагування

на загрози, а також інтегрувати міжнародний досвід у національні програми інформаційної безпеки.

Таким чином, концепція стратегічних комунікацій у системі національного управління інформаційною безпекою є багатовимірною та багатофункціональною, об'єднуючи правові, технологічні, соціальні та культурні компоненти. Вона виступає фундаментальною платформою для забезпечення інформаційної стабільності, протидії загрозам дезінформації та кібернетичної небезпеки, а також для побудови довірчих відносин між державою та суспільством, що в цілому сприяє ефективній реалізації національної стратегії інформаційної безпеки у сучасних умовах.

Цей підхід також підкреслює необхідність інтегрованого мислення та системного бачення, де стратегічні комунікації стають не лише інструментом оперативного реагування, але й засобом довгострокового прогнозування, планування та підтримки стійкості національної інформаційної інфраструктури. Вони забезпечують комплексне управління ризиками, дозволяють ідентифікувати потенційні вразливості, координувати дії різних державних та суспільних суб'єктів і формувати механізми, що зменшують вплив негативних факторів на інформаційний простір.

У цілому, стратегічні комунікації можна розглядати як динамічний, постійно еволюційний процес, що поєднує інтереси держави та суспільства, надає можливість інтегрувати міжнародний досвід та адаптувати його до національного контексту, а також створює платформу для активної участі громадян у формуванні безпечного, прозорого та збалансованого інформаційного середовища.

Якраз-таки у випадку із проблематикою впровадження та комплексного дослідження стратегічних комунікацій у системі реалізації основ національного управління інформаційною безпекою потрібно говорити про сутнісну поєднаність із формуванням комунікаційної стратегії як складова національного управління інформаційною безпекою, що і є предметом нашого

дослідження у п. 4.3 Розділу IV зазначеного дисертаційного дослідження. На підставі окреслених складників екзистенційного розуміння концепції цифрового суверенітету, концепції інформаційного нейтралітету та концепції стратегічних комунікацій як концепцій інформаційної безпеки, на підставі яких де-факто формується сучасне розуміння витоків комунікаційної стратегії у якості інформаційно-безпекової парадигми державного регулювання, пропонуємо нижче перейти до аналізу зазначеного феномену з позиції особливостей її впровадження залежно від конкретних державних моделей, котрі ми описали вище.

Комунікаційну стратегію як складову національного управління інформаційною безпекою в розрізі концепції цифрового суверенітету, на наш погляд, потрібно аналізувати на прикладі США, Франції та Китаю. Кожна із країн, при цьому, впроваджує дану комунікаційну стратегію, виходячи із цілей та специфіки власної внутрішньої та зовнішньої політики.

У США формування комунікаційної стратегії як складової національного управління інформаційною безпекою в контексті реалізації концептуальних приписів та стандартів цифрового суверенітету впроваджується за трьома напрямами – захистом критичної інформаційної інфраструктури від небажаного впливу, розвитком хмарних технологій та інновацій та, водночас, санкціонуванням іноземних (зокрема, китайських) технологій, що можуть зашкодити національній безпеці та національним інтересам держави.

Прикладом реалізації комунікаційної стратегії як складової національного управління інформаційною безпекою за напрямом захисту критичної інформаційної інфраструктури від небажаного впливу в США є реалізація концепції «America First» як політичної позиції у кібернетичному просторі. Напрямами реалізації зазначеної концепції є захист американської критичної інформаційної інфраструктури від іноземного негативного впливу. Подібний підхід, зокрема, передбачає концептуалізацію за напрямами не лише запобігання кібератакам та кіберзагрозам, але й запровадження превалювання

інформаційної інфраструктури (баз даних, систем збору/обробки/систематизації інформації) національного виробництва з метою економічного стимулювання виробників за допомогою наявних інструментів.

Розвиток хмарних технологій у контексті запровадження комунікаційної стратегії як складової національного управління інформаційною безпекою в США, в свою чергу, базується на наданні державної (стратегічної, фінансово-економічної) підтримки важливих та «опорних» з точки зору реалізації концепцій інформаційної безпеки компаній. До таких компаній, зокрема, належать Microsoft Azure та Amazon Web Services (AWS). Перша є відповідальною за хмарні обчислення, а також – розробку, виконання програм та зберігання даних на серверах, розташованих у розподілених дата-центрах, тоді як друга – також за хмарні обчислення, але у розрізі зберігання даних у віддаленому форматі за допомогою використання платформ-серверів віртуальної ґенези.

Сегмент санкціонування іноземних (зокрема, китайських) технологій, що можуть зашкодити національній безпеці та національним інтересам держави у контексті реалізації комунікаційної стратегії як складової національного управління інформаційною безпекою у США передбачає насамперед блокування деяких виробників та інформаційних ресурсів всередині країни. Так, наприклад, Федеральна комісія з питань зв'язку США (The Federal Communications Commission (FCC) визначала компанію Huawei загрозою національній безпеці рішенням від червня 2020 р., також заборонивши компаніям США використовувати державні кошти для купівлі її обладнання [119]. В свою чергу, соціальна мережа TikTok підпала під санкції та можливість повного блокування також через загрозу національній безпеці США, опцію її розгляду у контексті інструменту Китаю в пошукові вразливих місць американської інформаційної інфраструктури через взаємодію із користувачами із США.

В свою чергу, у Франції проблема реалізації комунікаційної стратегії як

складової національного управління інформаційною безпекою в сегменті цифрового суверенітету являє собою більш мірою «західноєвропейський» стандарт до забезпечення інформаційно-безпекової незалежності. Також можемо виділити три критерії зазначеного процесу – серед них розвиток національного «софту», законодавчий контроль діяльності технологічних компаній та підтримка європейських ініціатив щодо забезпечення інформаційної безпеки на внутрішньому партикулярному рівні. Коротко проаналізуємо кожен із вищезазначених етапів (складників).

У рамках розвитку національного «софту» як складової реалізації комунікаційної стратегії як складової національного управління інформаційною безпекою у Франції насамперед акцентують увагу на створенні альтернативних алгоритмів забезпечення функціонування державних органів та інституцій без використання програмного забезпечення від Google та Microsoft. Натомість, в країні створюється внутрішня програмна альтернатива – так, державні органи у своїй діяльності, залежно від сутнісної специфіки виконуваних операцій, використовують сервіси Nextcloud, BlueMind та Secure Cloud by OVHcloud.

Так, Nextcloud є прямою альтернативою Google Drive, а уряд Франції використовує його у якості хмарного сховища та системи для співпраці із забезпеченням повного контролю над конфіденційною інформацією з метою реалізації кінцевої мети, котра полягає у схоронності даних державних інформаційних реєстрів. BlueMind, в свою чергу, є французькою платформою для електронної пошти, календарів та контактів, що використовується у державному секторі, і за сутнісним та програмним наповненням фактично кореспондує системі Gmail від Google. Наостанок, застосунок Secure Cloud by OVHcloud використовується урядом Франції з метою забезпечення локального зберігання даних та відповідності нормам General Data Protection Regulation (GDPR) у контексті хмарного зберігання даних із грифом секретності та державної таємниці.

Наостанок у контексті реалізації комунікаційної стратегії як складової

національного управління інформаційною безпекою в сегменті цифрового суверенітету розглянемо приклад Китаю. Останній, на відміну від США та Франції (як країни-члена ЄС із демократичним пріоритетами та традиціями), в даному випадку запроваджується «на умовах» держави, тобто цілком та повністю кореспондує напрямам, за якими держава здійснює контроль національної державної політики на рівні директивного регулювання. Тут, знову-таки, можна виділяти три рівнозначних, проте різних за специфічним наповненням напрями реалізації – функціонування великого китайського фаєрволу (firewall), запровадження альтернативних національних ресурсів відносно світових технологій та Закон про кібербезпеку 2017 р. (Cybersecurity Law of the People's Republic of China 2017) як керівний у архітектуванні технологічної складової реалізації принципів інформаційної безпеки та кібербезпеки як її системно-структурної модельної складової.

В контексті функціонування великого китайського фаєрволу (firewall) у контексті реалізації комунікаційної стратегії як складової національного управління інформаційною безпекою в сегменті цифрового суверенітету говоримо про контроль, нагляд та фільтрування трафіку в мережі Інтернет. Ключової інтенцією у даному випадку є державні обмеження доступу громадян до зовнішніх ресурсів. Метою цього, на переконання китайського вченого К. Чуйхонга [222, с. 480] є не лише політичне, але й ідеологічне забезпечення створення належного рівня інформаційної освіченості громадян. Реалізація такої державної ініціативи передбачає, зокрема, обмеження доступу до альтернативних джерел інформації, що містять ознаки іншої, відмінної від китайської соціалістичної (авторитарно-диктаторської) ідеології та, відтак, можуть набути ознак дестабілізуючих та згубних для інформаційно-безпекової стабільності держави в стратегічному вимірі.

Розглядаючи дану практику з точки зору наукового аналізу та порівняльного підходу, можна зазначити, що китайський великий фаєрвол виступає яскравим прикладом суверенного підходу до управління

інформаційним простором, де держава не лише встановлює правила доступу до інформації, але й формує системну модель поведінки користувачів в мережі. З одного боку, подібна система дозволяє гарантувати захист національного інформаційного суверенітету, підтримувати стабільність державних комунікацій та протидіяти дезінформаційним і кіберагресивним проявам із зовнішніх джерел. З іншого – вона демонструє теоретичну концепцію цифрового державного протекціонізму, де ключову роль відіграють механізми контролю, фільтрування, моніторингу та регулювання потоків інформації, а також інтеграції технологічних і правових інструментів у єдину систему управління.

У науковому контексті це явище можна розглядати як приклад того, як держава може формувати інформаційний ландшафт із врахуванням національних стратегічних цілей та ідеологічного контексту, використовуючи високотехнологічні рішення для запобігання ризикам дестабілізації. Феномен великого фаєрволу можна трактувати як поєднання технічного, правового та соціокультурного вимірів національної інформаційної політики, де технології виконують роль інструменту реалізації державних норм і правил, а населення адаптується до нових інформаційних умов через зміну поведінкових і комунікаційних моделей.

З точки зору теорії інформаційної безпеки та державного управління, діяльність такого масштабу підкреслює необхідність комплексного підходу до регулювання інформаційного середовища, що охоплює не лише технічні заходи захисту мереж та даних, але й формування нормативної бази, інформаційної культури та освіченості користувачів. Важливим є те, що науковий аналіз демонструє взаємозв’язок між контролем над інформаційними потоками і формуванням державної політики у сфері цифрового суверенітету: контроль над джерелами інформації, моделювання поведінки користувачів та забезпечення дотримання правил доступу стає не лише технічним, але й соціально-політичним інструментом управління.

Більш того, у широкому теоретико-порівняльному вимірі великофаєрвольна модель Китаю дозволяє проаналізувати співвідношення між національними підходами до інформаційної безпеки та міжнародними практиками, що характерні для демократичних країн, де акцент робиться на балансі між свободою доступу до інформації та безпекою. У випадку Китаю очевидно, що держава віддає пріоритет стабільності та контролю над інформаційним простором, що дає можливість реалізувати довгострокові стратегічні цілі, водночас формуючи специфічну інформаційну культуру серед населення.

Таким чином, науковий аналіз феномену великого китайського фаєрволу дозволяє зробити висновок про його багатовимірний характер: він одночасно є технологічним, соціокультурним, правовим та ідеологічним механізмом управління інформаційною безпекою. Це явище демонструє, що в умовах глобалізації та інтенсивного розвитку цифрових технологій суверенний контроль над інформаційним простором стає стратегічним ресурсом держави, а ефективна реалізація цього контролю потребує поєднання технологій, нормативної регламентації та системи інформаційної освіти населення, що разом створює цілісну модель національної інформаційної безпеки у стратегічному вимірі.

У підсумку, огляд наукових думок свідчить, що реалізація державного контролю над інформаційним простором через великофаєрвольні механізми є комплексним явищем, яке одночасно враховує технологічний розвиток, правові норми, соціально-психологічні аспекти та ідеологічні завдання, створюючи ефективну модель цифрового суверенітету та управління інформаційною безпекою на національному рівні.

Аспект запровадження альтернативних національних ресурсів відносно світових технологій щодо реалізації комунікаційної стратегії як складової національного управління інформаційною безпекою в сегменті цифрового суверенітету на теренах Китаю набуває, знову-таки, стратегічного значення у

розрізі використання автентично створеного та програмованого «софту». Замість Google, Facebook та Amazon було розроблено національні альтернативи у вигляді власних платформ (WeChat, Baidu, Alibaba). Мета такого процесу – перш за все створення програмного забезпечення, «толерантного» до можливих перевірок, контролю та нагляду від органів державної влади, внаслідок чого відбувається узурпація та жорсткий контроль інформаційного простору, заборона використання інформаційних ресурсів у спосіб та з метою, що не кореспондує цілям та пріоритетам національної державної стратегічної політики.

Врешті-решт, положення Закону про кібербезпеку 2017 р. (Cybersecurity Law of the People's Republic of China 2017) до питання реалізації комунікаційної стратегії як складової національного управління інформаційною безпекою в сегменті цифрового суверенітету ставить перед собою стратегічне завдання формування багатоярусної системи безпеки даних. Зокрема, визначаються особливості регулювання захисту критичної інформаційної інфраструктури, обробки даних і діяльності іноземних компаній у китайському кіберпросторі; встановлюються аспекти контролю над збором, зберіганням і передачею персональних даних; інформаційна безпека визначається важливим аспектом національної безпеки.

Як ми зазначали раніше, основоположним контекстом, що детермінує різницю в публічному адмініструванні галуззю інформаційної безпеки та, відповідно, формуванні комунікаційної стратегії як складової національного управління інформаційною безпекою, є обраний державною розвитково-політичний курс (напрям). Промовистим в даному випадку є концепція інформаційного нейтралітету, котру використовують держави, які, як правило, сповідують принцип неконфліктної міжполітичної діяльності на міжнародній арені. Сконцентруємо увагу на прикладі Швейцарії, Швеції та Канади.

Наприклад, у Швейцарії принцип дотримання нейтралітету як концепція трансформувався і на сферу політично нейтрального реагування на конфлікти у

інформаційній сфері за умови, що останні не зачіпають інтереси країни. Іншими кластерними категоріями, в рамках яких у державі реалізуються принципи інформаційного нейтралітету, є незастосування цензури в мережі Інтернет та підтримка свободи слова на локальному рівні, що дозволяє говорити про двовимірний – зовнішній та внутрішній – формат реалізації зазначеної ініціативи. Нормативно-правовою рамкою вищезазначеного у Швейцарії є Акт № 998_115 від 08.11.1815 р. щодо визнання та гарантії постійного нейтралітету Швейцарії та недоторканності її території та частково – «Ініціатива про нейтралітет», ініційована партією SVP від 16.11.2022 р.

У Швеції, в свою чергу, принцип інформаційного нейтралітету реалізується за схожою зі Швейцарією структурою. Процес передбачає звужене регулювання та вплив держави на сферу інформаційного простору, в умовах чого навіть кризові політичні та безпекові ситуації не можуть виступати чинником обмеження права громадян на інформацію як базового права та свободи. В інформаційних конфліктах, що мають місце на території інших держав, Швеція також дотримується нейтральної політики. Примітно, що законодавче регулювання політики інформаційного нейтралітету, що розповсюджується на зовнішньому та внутрішньому рівні, у Швейцарії має аналогово-правове нормування : у Розділі 2 Акту про форму правління (Regeringsformen) від 1974 р. встановлюється концепція вираження поглядів та переконань у інформаційній сфері, а Акт про свободу друку (Tryckfrihetsförordningen), один із найстаріших нормативних документів у галузі інформаційної свободи та суверенітету (1766 р.) у Розділі 2 та Розділі 3 конкретизував положення щодо державно-управлінської гласності та свободи обігу інформаційних даних. Положення обох документів у контексті архітектури інформаційної безпеки та формування комунікаційної стратегії інформаційної безпеки у галузі інформації є актуальними у Швеції станом на сьогодні.

Приклад Канади відносно реалізації принципу інформаційного

нейтралітету у системі комунікаційної стратегії забезпечення національного управління інформаційною безпекою є корисним в контексті поєднання незалежності засобів масової інформації (ЗМІ) та невтручання в національний медіапростір із програми боротьби з фейковими новинами, спрямованими на дезінформацію, засобами фактчекінгу. Дуальний характер забезпечення інформаційно нейтральної державної політики регламентується ст. 2(b) Конституційного акту 1982 р. (The Constitution Act, 1982) та загальними положеннями Закону про доступ до інформації 1985 р. (Access to Information Act, 1985), якими гарантується інформаційна свобода та доступ до владних документів як гарантія та індикатор процесу відкритості державного управління.

В заключенні пропонуємо сконцентрувати увагу на прикладах реалізації комунікаційної стратегії національного регулювання інформаційної безпеки крізь призму впровадження концепції стратегічних комунікацій. Країнами, що в даному випадку є корисними та застосовними для наукового аналізу, плануємо уважати Велику Британію та, власне, Україну.

У Великій Британії, наприклад, концепція стратегічних комунікацій у якості складової частини комунікаційної стратегії національного регулювання інформаційної безпеки реалізується завдяки діяльності Національного центру кібербезпеки (National Cyber Security Centre – NCSC) та 77-ї бригади Збройних сил Великої Британії, до компетенції котрої входить протидія інформаційним загрозам та забезпечення проведення інформаційних операцій. Завдяки формуванню такої парадигми двоетапного управління інформаційним простором відбувається забезпечення його здатності реагувати на подразники, викликані як внутрішньою, так і зовнішньою політикою держави.

В свою чергу, тенденційний приклад України у контексті побудови комунікаційної стратегії регулювання національного інформаційного простору важливий та застосовний для розуміння загальних тенденцій даного процесу через аспект кризовості даного процесу. Гібридна війна рф проти України

упродовж 2014-початку 2022 рр. створила необхідність посилення стратегіко-комунікаційної інформаційної політики держави. За таких умов статус, значення та місце Ради національної безпеки та оборони України (РНБО) підкріпилося додатковим органом контролю та нагляду за безпековістю інформаційного простору – Центром протидії дезінформації (ЦПД). Діяльність Центру протидії дезінформації на нормативно-правовому рівні регламентується Указом Президента України № 187/2021 від 07.05.2021 р. Питання Центру протидії дезінформації. Основні елементи діяльності зазначених державних органів в Україні у контексті підтримання респондентності на відповідні кризові явища та джерела дестабілізації інформаційного простору – забезпечення не лише власне схоронності даних, але й територіальної цілісності та незалежності України в умовах спочатку гібридного, а наразі – повномасштабного вторгнення рф до України від 24.02.2022 р.

Таким чином, на підставі проаналізованих даних та інформації відносно особливостей використання комунікаційної стратегії як складової національного управління інформаційною безпекою можна зробити висновок про те, що остання є важливим інструментом формування стійкості держави перед сучасними загрозами в інформаційному просторі. Вона забезпечує ефективне управління інформаційними потоками, дозволяючи знижувати вплив дезінформації, пропаганди та кіберзагроз. Враховуючи зростання технологічних викликів, формування ефективної комунікаційної стратегії стає ключовим фактором захисту інформаційної суверенності держави.

Окрім того, комунікаційна стратегія як складова національного управління інформаційною безпекою визнається основою національної інформаційної політики, спрямованої на забезпечення відкритості державного управління, підвищення довіри громадян до урядових інституцій та протидію інформаційним атакам, що включає в себе розробку національних стандартів комунікації, впровадження сучасних цифрових технологій та координацію між державними органами, що відповідають за інформаційну безпеку. У даному

контексті доцільно застосувати класифікаційний поділ комунікаційної стратегії в умовах забезпечення інформаційної безпеки на концепцію цифрового суверенітету (США, Франція, Китай), концепцію інформаційного нейтралітету (Швейцарія, Швеція, Канада) та концепцію стратегічних комунікацій (Велика Британія, Україна), що використовується державами залежно від цілей публічно-управлінської діяльності.

Висновки до розділу 4

1. Досліджено теоретичні засади стратегічного управління інформаційною безпекою (ІБ) шляхом систематизації та компаративного аналізу міжнародних моделей, що дозволило: уточнити сутність стратегічного управління забезпеченням ІБ як процесу синхронізації юридичних, організаційних та технічних засобів для захисту державних, економічних і соціальних інтересів, із ключовим акцентом на пошуку оптимального балансу між нормативним закріпленням та фактичним впровадженням безпекової карти; розробити типологію міжнародних моделей стратегічного управління ІБ на основі аналізу досвіду США, ЄС, Великої Британії, Ізраїлю та Китаю; систематизувати мету стратегічного управління ІБ на три взаємопов'язані рівні (захист (базовий): нейтралізація загроз та забезпечення довіри до інформаційного середовища; розвиток (інноваційний): сприяння інноваціям та технологічному розвитку (ІКТ та ШІ) в ІБ; стійкість (соціальний): підвищення обізнаності населення та розвиток культури інформаційної безпеки (кібергігієни); виокремити чотири ключові особливості стратегічного управління ІБ у розвинених державах світу: правове регулювання, інституційна структура, міжнародна співпраця (Будапештська конвенція) та використання інновацій (ШІ та ІКТ);

2. Узагальнено розуміння сутності та інституційних можливостей глобального характеру інформаційної безпеки.

Уточнено трактування глобального характеру інформаційної безпеки як глибокої управлінської трансформації та індикатора зрілості міжнародних відносин у цифрову епоху, що формує нову архітектоніку світової системи, де інформаційний суверенітет тлумачиться не як ізоляційна здатність, а як уміння забезпечити автономію в умовах транскордонного обміну даними.

Обґрунтовано ключові інституційні можливості глобального характеру ІБ в контексті публічного управління: розвиток багатосторонньої співпраці (розглянуто як фундаментальна стратегічна парадигма, що формує новий вид міжнародної взаємозалежності. Виокремлено її переваги: координаційна системність, розподіл відповідальності та ефективна протидія транснаціональним загрозам); інтеграція державно-приватного партнерства (ДПП) (проаналізовано як механізм технологічного стимулювання та ефективного розподілу ресурсів, знань і технологій (на прикладі CISA у США та EU Cybersecurity Atlas в ЄС); інвестиційно-технологічне та людсько-ресурсне забезпечення (доведено, що акцент зміщується з виключно нормативного регулювання на кадрову підготовку та інноваційні хаби (кіберкластери) для підвищення кібернетичної освіченості населення (на прикладах CyberFirst у Великій Британії та діяльності INCD в Ізраїлі).

Визначено необхідність технологічної адаптації НПБ до викликів штучного інтелекту (ШІ), Інтернету речей (IP/IoT) та інформаційно-комунікаційних технологій (ІКТ), підкреслюючи, що законодавство має бути не лише реактивним, а й проактивним для забезпечення довгострокової стійкості.

Концептуалізовано багаторівневу інтеграцію технічних, організаційних та правових механізмів як ключову умову побудови ефективного механізму забезпечення ІБ, здатного реагувати на сучасні геополітичні виклики та технічні трансформації інформаційного поля.

3. Удосконалено концептуальні засади формування комунікаційної стратегії як складової системи публічного управління інформаційною безпекою.

Систематизовано та поглиблено аналіз основних концепцій інформаційної безпеки, які детермінують побудову комунікаційної стратегії, виокремивши та розкривши їхні ключові складові в управлінському вимірі: концепція цифрового суверенітету (підкреслено її технологічний (розвиток національних цифрових платформ) та економічний (зменшення залежності від іноземного ПЗ/апаратного забезпечення) компоненти); концепція інформаційного нейтралітету (уточнено, що її реалізація включає не лише політику невтручання у зовнішні конфлікти, а й культурний аспект – інформаційну освіту громадян (критичне мислення, медіаграмотність) та інституційну підтримку незалежних медіа); концепція стратегічних комунікацій (розглянуто як багатовимірну та багатофункціональну систему (правовий, технологічний, соціально-психологічний, культурний компоненти) управління, що забезпечує стійкість національного інформаційного простору та баланс між свободою доступу до інформації та захистом суверенітету.

Проведено порівняльний аналіз моделей реалізації комунікаційної стратегії на прикладі провідних держав, демонструючи її залежність від обраного політико-розвиткового курсу: авторитарна/Протекціоністська модель (Китай): Визначено, що вона ґрунтується на жорсткому контролі та фільтруванні трафіку (Великий китайський фаєрвол), запровадженні національних альтернатив світовим ресурсам (WeChat, Baidu), що є прикладом цифрового державного протекціонізму; суверенно-прагматична модель (США, Франція): Сфокусована на захисті критичної інфраструктури (США – America First), розвитку національного ПЗ та технологічних альтернатив (Франція – Nextcloud, BlueMind), а також санкціонуванні іноземних технологій (США – Huawei, TikTok); нейтрально-демократична модель (Швейцарія, Швеція, Канада): Базується на політично нейтральному реагуванні на зовнішні конфлікти, незастосуванні цензури та підтримці свободи слова/незалежності ЗМІ у поєднанні з програмами боротьби з дезінформацією (фактчекінг у Канаді).

РОЗДІЛ 5
СТРАТЕГІЧНІ НАПРЯМИ РОЗВИТКУ МЕХАНІЗМІВ РЕАЛІЗАЦІЇ ІНФОРМАЦІЙНОЇ БЕЗПЕКИ У СИСТЕМІ ПУБЛІЧНОГО УПРАВЛІННЯ

5.1. Формування механізмів розвитку інформаційної безпеки в умовах сучасних викликів та загроз

Сучасна система інформаційної безпеки держави перебуває у стані безперервної трансформації, що зумовлено динамікою глобальних процесів, розвитком цифрових технологій та активізацією гібридних загроз. Так, у попередніх розділах дисертаційного дослідження було визначено теоретико-методологічні та нормативно-правові засади функціонування механізмів інформаційної безпеки, а також здійснено аналіз наявних практик і міжнародного досвіду. Натомість, у Розділі V даного дисертаційного дослідження ключовим завданням стає розроблення концептуально-стратегічного бачення їхнього розвитку, що корелює із логікою формулювання авторської моделі, здатної інтегрувати різнорівневі інституційні, правові та технологічні механізми у цілісну систему захисту інформаційного простору, котрі ми викладемо у Розділі V дисертації.

Таким чином, у Розділі V даного дисертаційного дослідження нами буде розглянуто сучасні виклики й тенденції розвитку механізмів інформаційної безпеки, які формують основу для подальших стратегічних підходів і, зрештою, для вироблення авторської концепції розвитку інформаційної безпеки держави.

Виходячи з означеної логіки, першочерговим завданням є окреслення тих викликів, що мають визначальний вплив на сучасну архітектуру інформаційної безпеки держави, як-от ризики, що проявляються у глобальному масштабі та

внутрішньому середовищі та, як наслідок, ґенерують необхідність перегляду традиційних підходів до захисту національного інформаційного простору.

У цьому контексті вбачаємо за доцільне розпочати безпосередньо із огляду глобальних та національних факторів ризику інформаційної безпеки як елементу сучасних викликів та тенденцій розвитку механізмів інформаційної безпеки.

Глобальні та національні фактори ризику інформаційної безпеки постають у XXI с. як системний виклик для держав, оскільки інформаційне середовище стає самостійним театром протиборства. Зокрема, гібридні війни дедалі частіше реалізуються не лише у воєнній чи політичній площині, а й у цифровому вимірі. Специфіка останніх полягає у комплексному поєднанні військових, дипломатичних, економічних, інформаційних та кібернетичних засобів впливу, що ускладнює виявлення джерел загрози та знижує ефективність традиційних механізмів оборони. До слова, досвід України з 2014 р. є показовим прикладом того, як інформаційні операції стають ключовим інструментом агресії, спрямованої на підрив політичної стабільності та соціальної єдності.

Дезінформація як різновид інформаційного впливу становить окремий пласт ризиків, оскільки вона не лише трансформує суспільні настрої, а й підриває легітимність державних інституцій. Так, Європейський Союз (ЄС) у 2015 р. створив спеціальну робочу групу East StratCom Task Force, яка займається протидією дезінформації, зокрема з боку рф. У національному вимірі, наприклад, ця загроза виявляється через поширення фейкових новин, маніпулятивних наративів у медіа та соціальних мережах, а також у спробах дискредитувати стратегічні державні курси.

Не менш вагомим викликом є кібератаки, які з інструмента економічного шпигунства перетворилися на метод впливу на критичну інфраструктуру держав. Згідно з доповідями Європейського агентства з кібербезпеки (ENISA), у 2022–2023 рр. найбільше зросла кількість атак на енергетичний сектор,

фінансові установи та державні органи. Для України у даному контексті характерними стали кібератаки на державні ресурси та об’єкти критичної інфраструктури, що координувалися у тісному зв’язку з воєнними діями та військовою агресією рф, що мала не лише директивну, але й інформаційно-мілітарну форму прояву та контекстуації.

Особливу складність у розрізі викликів та тенденцій розвитку механізмів інформаційної безпеки в умовах турбулентного та динамічного сьогодення становить феномен інформаційної асиметрії, коли держава і суспільство перебувають у нерівних умовах щодо доступу, аналізу та інтерпретації інформації. Асиметрія, своєю чергою, може мати як технологічний вимір (нерівний доступ до сучасних цифрових інструментів), так і когнітивний (різний рівень медіаграмотності громадян). Як результат, виникає дисбаланс між швидкістю поширення інформації та здатністю суспільства її критично осмислювати, що створює сприятливий ґрунт для маніпуляцій.

Таким чином, глобальні та національні ризики — гібридні війни, дезінформація, кібератаки та інформаційна асиметрія — утворюють систему взаємопов’язаних загроз, які визначають стратегічний порядок денний у сфері інформаційної безпеки держави та потребують комплексного переосмислення існуючих механізмів протидії.

Узагальнені вище глобальні та національні фактори ризику окреслюють традиційну площину загроз, з якою держави стикаються протягом останніх десятиліть. Проте, паралельно із класичними проявами інформаційної війни формується новий вимір викликів, обумовлений стрімким розвитком цифрових технологій. Сучасні інформаційні ризики дедалі частіше виникають не стільки як наслідок прямої агресії, скільки як результат використання новітніх інструментів штучного інтелекту, аналітики великих даних, технологій синтетичного контенту (deepfake) та алгоритмічних систем управління інформаційними потоками. Саме вони змінюють архітектуру інформаційного простору, породжуючи як нові можливості для розвитку, так і безпрецедентні

загрози для національної безпеки.

У цьому контексті доцільно окреслити ключові інструменти та механізми протидії високотехнологічним загрозам, що формують нову цифрову архітектуру ризиків. Передусім, маємо говорити про запровадження комплексних систем виявлення та маркування синтетичного контенту (зокрема, автоматизованих модулів розпізнавання deepfake-матеріалів, що застосовуються провідними інформаційними платформами). Також, важливим напрямом є розвиток алгоритмів автоматизованої верифікації джерел інформації, здатних оцінювати походження, достовірність та аномальні патерни поширення контенту (наприклад, за моделями поведінкової аналітики, що використовуються ENISA та CERT-EU). На додаток, згадуємо про формування на рівні держави центрів компетенцій зі штучного інтелекту та цифрової криміналістики, які здійснюватимуть аудит алгоритмічних систем, аналіз шкідливих моделей генеративного ШІ та розробку національних стандартів їх безпечного використання [182, с. 55].

Паралельно, необхідним є розвиток практик алгоритмічної прозорості та підзвітності цифрових платформ (зокрема, обов'язкове розкриття принципів роботи рекомендаційних систем та критеріїв модерації контенту, як це передбачено європейським Digital Services Act). Також, необхідно працювати над удосконаленням механізмів моніторингу великих масивів даних для раннього виявлення інформаційних аномалій — наприклад, хвиль координованої поведінки бот-мереж, нетипового навантаження на інформаційні ресурси чи синхронізованого поширення деструктивних наративів. Окремим елементом має стати системна політика розвитку цифрової й медіаграмотності громадян, спрямована на мінімізацію когнітивних ризиків та посилення здатності суспільства ідентифікувати маніпулятивний чи штучно згенерований контент [182, с. 55].

На наше переконання, реалізація зазначених інструментів формує підґрунтя для створення стійкої, адаптивної та прогностично орієнтованої

системи інформаційної безпеки, яка здатна не лише реагувати на загрози, а й передбачати їхню появу у цифровому середовищі, що динамічно трансформується.

У контексті огляду феномену нових тенденцій розвитку механізмів інформаційної безпеки маємо насамперед виходити з того, що наразі штучний інтелект (ШІ) перетворився на стратегічний ресурс XXI ст., а його застосування охоплює сфери оборони, державного управління, бізнесу, освіти та інформаційних комунікацій. З одного боку, штучний інтелект (ШІ) відкриває нові можливості для забезпечення інформаційної безпеки, що генералізуються від автоматизованого моніторингу кіберзагроз до ідентифікації фейкових повідомлень у соціальних мережах. На противагу, штучний інтелект (ШІ), як зазначає С. Гудмен, стає інструментом атак, адже алгоритми машинного навчання можуть бути використані для створення складних фішингових схем, персоналізованих дезінформаційних кампаній та автоматизованого виробництва контенту [243, с. 140].

Тут-таки видається аргументованим сформувати відповідні авторські (індивідуальні) пропозиції, спрямовані на зменшення негативного впливу ШІ на інформаційну безпеку. Серед них можемо виділити : 1) впровадження багаторівневої системи контролю застосування алгоритмів машинного навчання, яка поєднує автоматизоване виявлення аномалій з обов’язковою експертною оцінкою у випадках високоризикових інформаційних інцидентів; 2) встановлення прозорих процедур аудиту алгоритмів, що використовуються у критично важливих сферах (державні комунікації, виборчі процеси, медіаплатформи), включно з незалежною експертизою їх здатності генерувати маніпулятивний або деструктивний контент; 3) розроблення на національному рівні стандартів детекції синтетичного контенту, які б дозволили оперативно ідентифікувати deepfake-матеріали й мінімізувати ризики їхнього використання у дестабілізаційних кампаніях.

Сукупно, означені вище інструменти можуть бути використані як базові

механізми профілактики та нейтралізації новітніх інформаційних загроз, зумовлених функціонуванням штучного інтелекту (ШІ).

На підтвердження викладеної нами вище тезової практичної інформації щодо згубності та контраверсійності штучного інтелекту (ШІ) у певному його вимірі маємо зазначити, що останній здатен радикально змінити баланс сил у сфері безпеки, оскільки дозволяє меншим акторам здійснювати вплив, співмірний із можливостями держав, що є безпосереднім транснаціональним викликом.

Окрім того, аналітика великих даних (Big Data) стала одним із ключових чинників формування «суспільства ризику», котру продукував та концептуалізував ще П. Боуен [216]. Величезні масиви даних, які щодня генеруються громадянами, бізнесом та органами влади, використовуються для прогнозування поведінки, створення політичних профілів та персоналізації інформаційного впливу. За даними IBM, щоденно у світі створюється понад 2,5 квнтлн. байтів інформації, і ці ресурси стають підґрунтям для як легітимної комерційної діяльності, так і для маніпуляцій суспільною думкою, що набуває особливої актуальності під час виборчих кампаній. Розглядаючи даний феномен, науковці схиляються до думки, що монополізація доступу до big data транснаціональними корпораціями створює нову форму інформаційної асиметрії, у якій держава втрачає контроль над критично важливими інформаційними потоками [216].

У міжнародній практиці помітними є різні підходи до нейтралізації ризиків, пов’язаних із концентрацією великих даних. У США ключову роль відіграє Федеральна торгова комісія (FTC), повноваження якої ґрунтуються насамперед на Section 5 of the Federal Trade Commission Act (15 U.S.C. § 45), що забороняє недобросовісні та оманливі практики у сфері обробки даних, що дозволяє FTC сформувати широку прецедентну практику протидії алгоритмічним маніпуляціям і прихованому профілюванню, а також встановити стандарти прозорості для технологічних платформ [235, с. 1075]. На

доповнення, у Південній Кореї превентивна модель контролю побудована навколо Personal Information Protection Act (PIPA) та обов'язкового Data Protection Impact Assessment, нагляд за яким здійснює Personal Information Protection Commission (PIPC) [235, с. 1078]. Поєднання оцінок впливу, державного аудиту та санкційного механізму створює більш жорсткий, ніж американський, режим запобігання зловживанням big data, тоді як зазначені вище практики загально демонструють, що ефективна протидія інформаційним ризикам у сфері великих даних потребує інституційного нагляду, прозорості алгоритмів та відповідальності платформ інформаційного домінування та монополізації.

Додатковим трендом є технології діпфейк (deepfake), що суттєво змінила характер інформаційних загроз, внаслідок чого використання генеративних нейромереж для створення синтетичних зображень, відео чи аудіо вийшло за межі експериментів і стало інструментом політичних маніпуляцій та, як наслідок, інформаційного впливу. У поєднанні з платформами соціальних медіа, означена технологія створює середовище тотальної недовіри, коли суспільство втрачає можливість відрізняти правдивий контент від фальсифікованого, що актуалізує проблему «кризи достовірності», яку, наприклад, Н. Ріпсмен та Т. Пол вважають однією з ключових загроз демократичним інституціям, з чим ми, власне, також маємо честь погодитися [271, с. 3-19].

Завершальним, але не менш значущим компонент сучасних інформаційних ризиків є алгоритмічна маніпуляція. В даному випадку, алгоритми пошукових систем, соціальних мереж і рекламних платформ фактично визначають, яку інформацію отримає користувач, формуючи так звані «інформаційні бульбашки», що призводить до сегментації суспільного дискурсу, поляризації громадської думки й посилення вразливості до маніпуляцій. У європейському контексті наявну проблему намагаються врегулювати через прийняття Digital Services Act від 2022 р., який зобов'язує

платформи забезпечувати прозорість алгоритмів та мінімізувати ризики маніпуляцій.

Щодо подальшого розкриття та конкретизації даного питання у вітчизняних умовах повинні відмітити, що в Україні нормативне регулювання діяльності медіа та інформаційних комунікацій здійснюється, зокрема, через Закон України «Про медіа» № 2849-IX, який надає Національній раді з питань телебачення і радіомовлення повноваження контролювати дотримання законодавчих вимог провайдерами медіа та окремих цифрових платформ (ст.8, ст. 9 нормативно-правового акту). Поряд із цим, оновлена редакція Закону України «Про електронні комунікації» № 1089-IX встановлює правові рамки для діяльності інтернет- та ІКТ-провайдерів, регулює порядок їхньої реєстрації, права й обов'язки щодо забезпечення інформаційної безпеки (п. 7 ч. 1 ст. 2 нормативного документу), що створює базу для контролю за поширенням контенту та обмеженням шкідливого впливу на користувачів [285].

Водночас, потрібно зауважити, що спеціалізованих норм, які б прямо регулювали алгоритмічну маніпуляцію, прозорість алгоритмів або аудити алгоритмічних систем платформ, наразі не існує, що формує нормативну прогалину, чим підкреслено актуальність та синхронну необхідність подальшого вдосконалення законодавства з урахуванням сучасних технологічних тенденцій та інформаційних ризиків, зокрема щодо алгоритмічної прозорості та мінімізації ризиків маніпуляцій у цифровому середовищі.

Отже, новітні технологічні тенденції, такі як штучний інтелект, великі дані (big data), діпфейки (deepfake) та алгоритмічна маніпуляція створюють нову конфігурацію інформаційних загроз, яка значною мірою перевищує масштаби та складність класичних ризиків. І, відповідно, для держави це означає необхідність інтеграції інноваційних інструментів до системи захисту, водночас формуючи власні етичні та правові стандарти використання цих технологій.

Водночас, ключовим каналом поширення та реалізації зазначених ризиків стають саме соціальні мережі та цифрові платформи, які трансформувалися у домінуюче середовище суспільної комунікації, мобілізації та політичного впливу. Їхня роль є подвійною: з одного боку, вони створюють нові можливості для демократизації інформаційного простору та комунікації держави з громадянами; з іншого — стають аренами маніпуляцій, інформаційних атак і підриву національної безпеки.

Соціальні мережі у XXI столітті перетворилися на глобальну інфраструктуру суспільної комунікації, що охоплює більшість населення планети. Для України ця тенденція також характерна – як зазначає І. Брацук у власному аналізі війни як медійної події, близько 70 % громадян у 2022 р. мали облікові записи щонайменше в одній соціальній мережі [11, с. 23-25]. Таке охоплення робить цифрові платформи не лише засобом повсякденного спілкування, а й ареною для мобілізації суспільних рухів, формування політичних настроїв та реалізації цілеспрямованих інформаційних операцій. Водночас, з метою мінімізації загроз інформаційної безпеки у соціальних мережах, українські органи державної влади застосовують комплексний підхід, включно із моніторингом дезінформації (Національна рада з питань телебачення і радіомовлення, положення ст. 8 Закону України «Про медіа» № 2849-IX), розробкою рекомендацій щодо безпечного користування платформами (Мінцифра, Держспецзв’язку) та міжнародною співпрацею щодо верифікації контенту [169, с. 185]. Подібні механізми дозволяють обмежувати поширення шкідливого або маніпулятивного контенту без обмеження свободи вираження думок, поглядів та переконань, чим досягається бажаний ефект демократизації інформаційного простору, що ідеологічно корелює із приписами ст. 34 Основного закону – Конституції України [200, с. 75].

З одного боку, представники закордонного та українського наукового дискурсу з приводу даного питання [11, с. 23-25] наголошують на демократизуючому потенціалі соціальних мереж. Останні відкривають нові

можливості для горизонтальної комунікації, самоорганізації та розбудови громадянського суспільства. Саме завдяки цим платформам відбулися масштабні соціальні рухи початку XXI ст. — від Арабської весни до Революції Гідності на Майдані у 2013-2014 рр. У цьому контексті соціальні мережі розглядаються як каталізатор політичної участі та інструмент залучення громадян до процесів ухвалення рішень. Для держави це створює додаткові можливості розвитку цифрової демократії, підвищення прозорості урядування та формування нових каналів взаємодії з громадянами.

Водночас, та сама інфраструктура, що забезпечує відкритість і швидкість комунікацій, стає сприятливим середовищем для поширення загроз інформаційній безпеці. Подібні тенденції спостерігаються і в Європі, де Європейська служба зовнішніх дій (EEAS) у 2022 р. виявила систематичні кампанії рф та Китаю, спрямовані на підрив довіри до демократичних інститутів і розпалювання суспільних конфліктів. Оглянута фактологія дозволяє зробити висновок, що цифрові платформи стають водночас каналом демократизації та полем для маніпулятивних впливів.

Додатковим чинником ускладнення ситуації є алгоритмічна архітектура соціальних мереж, яка впливає на структуру інформаційних потоків та даних, що отримують користувачі. Відповідно, алгоритми ранжування контенту сприяють поширенню емоційно забарвлених, сенсаційних повідомлень, незалежно від їхньої достовірності. Наприклад, як зазначено у дослідженні М. Воркмена [296, с. 320], неправдиві новини у соціальних мережах (наприклад, Twitter (X)) поширюються дійсно набагато швидше, ніж перевірені факти, що пояснюється простотою отримання такої інформації, удаваним достовірним форматом її оприлюднення та подання і небажанням індивіда критично аналізувати останню внаслідок інформаційної перевантаженості життя. Можна стверджувати, що логіка функціонування Інтернет-платформ та соціальних мереж орієнтована на максимізацію «залучення» користувачів, тоді як питання достовірності інформації залишається другорядним, а технологічні особливості

роботи цифрових платформ, на додаток, лише де-факто підсилюють ризики поширення дезінформації.

У науковому контексті дане явище розглядається як складний багатовимірний процес, що поєднує технічні, соціальні та когнітивні аспекти інформаційного середовища. Алгоритмічні моделі ранжування контенту не є нейтральними; вони створюють специфічні комунікаційні канали та схеми споживання інформації, які безпосередньо формують сприйняття реальності користувачами. Переважно такі алгоритми підсилюють схильність до підтвердження власних переконань (ефект підтвердження), що, у свою чергу, генерує «інформаційні бульбашки» та ізоляцію від альтернативних точок зору. Це формує середовище, де дезінформація може існувати і поширюватися швидше, ніж коректна, верифікована інформація, створюючи потенційно небезпечний контекст для формування громадської думки та прийняття рішень.

Більш того, алгоритмічний контроль інформаційних потоків можна розглядати як складову частину більш широкого феномену цифрової економіки уваги, де основною метою платформ стає не інформаційна прозорість або освітня функція контенту, а максимізація користувацької активності та часу перебування в мережі. Такий підхід, як підкреслюють численні дослідження у сфері медіаекології та інформаційної безпеки, створює додаткові виклики для державного регулювання інформаційного простору, оскільки поширення недостовірних матеріалів відбувається швидше, ніж його коригування або нейтралізація.

З точки зору теоретичної парадигми інформаційної безпеки, алгоритмічна архітектура соціальних мереж виступає як каталізатор трансформації традиційних підходів до захисту інформаційного середовища. Вона демонструє, що сучасні інформаційні загрози мають комплексний, динамічний та непередбачуваний характер, що вимагає від державних органів та інституцій уваги до питань регулювання не лише контенту, але й алгоритмічних процесів, які визначають поширення інформації у цифровому просторі. Водночас,

алгоритмічна залежність користувачів від платформ створює додатковий рівень складності при спробах формування критичного інформаційного мислення та медіаграмотності у суспільстві.

Крім того, науковий аналіз свідчить про те, що алгоритмічна архітектура соціальних мереж є інтегральним фактором формування глобальної інформаційної екосистеми. Вона взаємодіє з іншими технологічними, соціальними та політичними чинниками, що впливають на динаміку інформаційних потоків, зокрема на рівні міжнародного обміну даними, протидії дезінформаційним кампаніям та управління кіберзагрозами. Цей аспект підкреслює необхідність комплексного підходу до побудови механізмів правового регулювання інформаційної безпеки, де враховується не лише контент і його легальність, а й алгоритмічні особливості, які визначають швидкість і масштаб його поширення.

Таким чином, алгоритмічна архітектура соціальних мереж виступає ключовим компонентом сучасного інформаційного середовища, що формує динаміку сприйняття та поширення інформації. Науковий аналіз цього явища підкреслює, що забезпечення інформаційної безпеки в цифровому середовищі вимагає не лише правового та технічного регулювання, але й глибокого розуміння соціально-психологічних та когнітивних механізмів, які визначають поведінку користувачів, їх взаємодію з контентом та ступінь вразливості до дезінформації. У підсумку, комплексний огляд підтверджує багатовимірність проблематики алгоритмічного впливу на інформаційні потоки та наголошує на необхідності інтеграції наукових знань у практику державного регулювання та стратегічного планування в сфері інформаційної безпеки.

Невід’ємною складовою проблеми викликів та тенденцій розвитку механізмів інформаційної безпеки є також економічний вимір функціонування соціальних мереж, унаслідок чого збирання та обробка великих масивів даних про користувачів створює умови для мікротаргетингу політичних повідомлень, що відкриває нові горизонти маніпуляцій. На додаток, Європейський

наглядовий орган із захисту даних (EDPS) у 2021 р. попередив, що монополізація інформації глобальними корпораціями загрожує базовим демократичним інститутам, оскільки перетворює політичну конкуренцію на сферу технологічної маніпуляції, впливу на соціальну думку та, як наслідок, соціальну свідомість.

Особливого значення роль соціальних мереж набуває і у контексті гібридних війн. Війна рф проти України продемонструвала, що цифрові платформи стали інструментом системних інформаційних атак. За даними Центру стратегічних комунікацій та інформаційної безпеки України від 2023 р., лише протягом перших шести місяців повномасштабного вторгнення було виявлено понад 3 500 фейкових повідомлень, поширюваних у соціальних медіа з метою підриву довіри до влади та деморалізації суспільства. Таким чином, соціальні мережі перетворилися на важливу арену сучасних гібридних конфліктів, де інформаційний вплив стає не менш небезпечним, ніж військова агресія.

Зазначені вище виклики спонукають держави та міжнародні інституції розробляти нові механізми регулювання цифрових платформ. Наприклад, у Європейському Союзі (ЄС, як ми зазначали раніше, ухвалено Digital Services Act 2022 р., який передбачає підвищення прозорості алгоритмів, обов’язкову боротьбу з дезінформацією та захист прав користувачів [39]. У свою чергу, в Україні у 2021 р. була презентована Стратегія інформаційної безпеки, що серед ключових пріоритетів визначила протидію загрозам у цифрових медіа (п. «Недостатній рівень медіаграмотності (медіакультури) в умовах стрімкого розвитку цифрових технологій»). Однак, необхідно констатувати, що ефективність таких заходів залежить від співпраці держави з технологічними гігантами, які залишаються глобальними суб’єктами з власними економічними та політичними інтересами, та через яких, зокрема, найчастіше відбувається ретрансляція даних, що залишає питання відносно достовірності та інформаційно-гігієнічної екстраполяції на свідомість громадян (населення)

держави.

Відтак, доцільно констатувати, що соціальні мережі та цифрові платформи становлять феномен подвійної природи та, водночас, відкривають нові можливості для демократичного розвитку та формування цифрової культури, але також створюють широкий спектр інформаційних загроз, від дезінформаційних кампаній до гібридних атак. Їхній вплив визначається не лише кількісними показниками користування, а й поєднанням технологічних, соціальних та політичних чинників. Внаслідок цього, для держави першочерговим завданням є формування збалансованої політики, яка поєднуватиме регуляторні заходи, стратегічні комунікації та цифрову освіту громадян, що структурно та ідеологічно відрізняється від заборони розвитку цифрових платформ.

У сучасних умовах цифрової трансформації ключовим елементом забезпечення ефективної інформаційної безпеки стає також інформаційна гігієна та підвищення кіберстійкості суспільства. Так, інформаційна гігієна передбачає комплекс заходів, спрямованих на формування навичок критичного сприйняття інформації, виявлення джерел дезінформації, розпізнавання маніпуляційних технологій та належне поводження з персональними даними у цифровому середовищі. За даними Організації економічного співробітництва та розвитку (OECD) від 2021 р., понад 45% користувачів мережі Інтернет у світі не мають достатньої компетентності для перевірки достовірності отриманої інформації, що робить їх особливо вразливими до дезінформаційних кампаній та кібератак. Одночасно з цим, ЮНЕСКО (UNESCO) у згаданому дослідженні «Тематична конференція, присвячена Глобальному тижню медіа та інформаційної грамотності 2020 року» від 2020 р. підкреслює, що формування цифрової грамотності на ранніх етапах освіти значно підвищує стійкість громадян до маніпулятивного контенту та сприяє створенню свідомої та відповідальної онлайн-спільноти. Усе це разом формує певний компас проблематики споживання інформації, що ускладнює процес «відсікання»

неправдивих відомостей та може дестабілізувати діяльність державного, інституційного апаратів тощо.

На рівні державних інституцій, ефективна стратегія кіберстійкості включає тренінги, навчальні програми та симуляційні вправи, які моделюють реальні сценарії інформаційних атак. Прикладом є практики Швеції та Фінляндії, де державні органи проводять регулярні навчання для співробітників міністерств та комунальних установ з протидії фейковим новинам, кібератакам і спробам соціального інжинірингу. Такі програми охоплюють алгоритми перевірки джерел інформації, моделювання поведінки в умовах кібератак, а також психологічні аспекти сприйняття контенту, що дозволяє знизити ефект масових маніпуляцій.

Особливої уваги в контексті огляду сучасних викликів та тенденцій розвитку механізмів інформаційної безпеки потребує синергія між технологічними інструментами та поведінковими практиками. Сучасні рішення на основі штучного інтелекту та аналітики великих даних здатні виявляти фейковий контент, блокувати бот-мережі та відстежувати дезінформаційні кампанії в режимі реального часу. Проте, ефективність таких систем значною мірою залежить від компетентності користувачів, тому що без розуміння базових принципів інформаційної гігієни навіть сучасні алгоритмічні рішення можуть не стати на заваді дезінформаційній діяльності. Як результат, можемо говорити про двоплановий підхід, що може бути використаний для нівелювання зазначених негативних тенденцій інформаційного обігу – технічні засоби захисту мають доповнюватися навчанням і просвітницькою роботою серед населення.

Важливим аспектом є інституційне впровадження практик кіберстійкості. Як ми зазначали раніше, насамперед в Європейському Союзі (ЄС) створюються національні платформи з підвищення цифрової обізнаності, включаючи онлайн-курси, відкриті навчальні матеріали та інтерактивні симуляції кібератак, на які доцільно звертати увагу в контексті врегулювання потенційного

дезінформаційного простору і Україні. Так, у рамках ініціативи EU Cybersecurity Month (Місяць кібернетичної безпеки) громадяни мають змогу долучатися до тренінгів із безпечного користування соціальними мережами та електронними сервісами, що підвищує рівень загальної кіберстійкості населення Крім того, аналітика показує, що держави з високим рівнем цифрової освіти та критичного мислення громадян демонструють більшу стійкість до зовнішніх інформаційних впливів і здатні швидше реагувати на гібридні загрози.

Системне формування інформаційної гігієни передбачає також інтеграцію освітніх програм у навчальні заклади різних рівнів, від шкіл до закладів вищої освіти, а також в рамках корпоративної та державної освіти, що надає змогу не лише підвищити обізнаність, а й створює основу для розбудови національної культури інформаційної безпеки, де громадянин усвідомлює свою відповідальність за збереження безпеки інформаційного простору та має навички для протидії загрозам. Таким чином, інформаційна освіта і формування культури кіберстійкості виступають критично важливими складовими сучасних механізмів захисту інформаційного простору, створюючи багаторівневу систему, яка поєднує технологічні, організаційні та поведінкові елементи.

Таким чином, освітній і поведінковий вимір формування інформаційної безпеки створює фундамент, на якому будується суспільна стійкість до зовнішніх та внутрішніх загроз. Водночас, даного рівня недостатньо у сучасному глобалізованому цифровому середовищі, де інформаційні потоки перетинають національні кордони, а технології змінюють структуру суспільних відносин швидше, ніж традиційні інститути встигають адаптуватися. Саме тому держава, міжнародні організації та наднаціональні утворення потребують ефективних регуляторних та правових механізмів, які б створювали інституційну рамку для захисту цифрового простору. Якщо освіта формує свідомого користувача, то право забезпечує правила інтеграції набутих умінь, що визначають межі свободи, відповідальності та допустимих форм поведінки

у мережі Інтернет як спільному інформаційному просторі.

Сучасна інформаційна доба характеризується стрімким розвитком технологій, які радикально змінюють як можливості доступу до інформації, так і масштаби загроз для безпеки. Кіберпростір став простором, де традиційні форми правового регулювання постійно стикаються з викликами технологічної динаміки, породжуючи проблеми як на рівні національних юрисдикцій, так і на рівні міжнародного права. Ми, знову-таки, відмічали раніше за текстом, що саме Європейський Союз (ЄС) демонструє найбільш системну реакцію на цифрові виклики, створюючи рамкове законодавство для усього європейського простору. Так, Digital Services Act (DSA) від 2022 р. передбачає принципово новий підхід до регулювання онлайн-платформ, зобов'язуючи їх видаляти незаконний контент, протидіяти дезінформації та забезпечувати прозорість алгоритмів, а Data Governance Act (DGA), що діє паралельно та доповнює положення першого, спрямований на формування єдиного європейського ринку даних та підвищення довіри до обігу інформації. Обидва акти покликані не лише врегулювати діяльність приватних суб'єктів, але й створити умови для поєднання інноваційності з безпекою.

На національному рівні також відбувається інтенсивний розвиток правових рамок. Чимало держав розробили власні стратегії кібербезпеки (наприклад, США, Велика Британія, Україна), що включають положення щодо боротьби з дезінформацією, підвищення цифрової грамотності та створення інституцій для реагування на кібератаки. Український контекст особливо показовий, адже гібридна, а потім – повномасштабна війна рф проти України актуалізувала необхідність системної протидії як на полі бою, так і в інформаційному просторі, що призвело до ухвалення низки спеціальних законів і стратегій.

У цьому контексті важливою дилемою залишається баланс між забезпеченням безпеки та захистом прав людини. Заходи протидії дезінформації та мови ворожнечі нерідко межують із ризиком надмірного

контролю над свободою слова. Міжнародні індекси, зокрема Freedom on the Net (Freedom House), щороку фіксують тенденцію, коли посилення інформаційного контролю використовується авторитарними режимами для обмеження громадянських прав під прикриттям боротьби з неправдивою інформацією (фейками) [137, с. 125]. Водночас, демократичні держави намагаються вибудувати інші механізми: чіткі правові процедури, прозорість ухвалення рішень та залучення громадянського суспільства. Наприклад, положення Digital Services Act (DSA) від 2022 р. передбачають можливість оскарження дій платформ користувачами, а також обов'язок пояснювати логіку алгоритмічних рішень, що значно зменшує ризики зловживань.

Ще однією характерною ознакою сучасних загроз є їхній транснаціональний характер. Кібератаки, кампанії з дезінформації чи витоки даних не зупиняються на кордонах, що потребує міжнародного співробітництва. ООН, ОБСЄ, НАТО та інші міжнародні організації формують базові принципи поведінки держав у кіберпросторі, однак відсутність універсального міжнародно-правового договору у цій сфері створює серйозні прогалини. Фактично кожна держава встановлює власні правила, що може призводити до фрагментації глобального інформаційного простору.

Цифрова трансформація, водночас, посилює залежність суспільств від великих технологічних корпорацій, які контролюють обіг даних і визначають механізми доступу до інформації, формуючи рамки суспільного дискурсу. Це ставить питання про здатність держав ефективно регулювати акторів, чия економічна та технологічна потуга іноді перевищує можливості цілих країн. Нові технології, такі як штучний інтелект, блокчейн чи квантові обчислення, лише загострюють ці виклики, адже відсутність чітких правил їхнього використання створює ризики для приватності, трудових прав і демократичних процедур, зокрема в контексті deepfake-технологій чи автоматизованого ухвалення рішень.

Узагальнюючи, можна стверджувати, що регуляторні та правові

механізми є невід'ємною складовою інформаційної безпеки. Останні не здатні замінити освітніх та поведінкових заходів, проте формують інституційний каркас, який забезпечує баланс між свободою і безпекою. Перспективи розвитку правового регулювання у сфері цифрової трансформації полягають у пошуку оптимальної моделі, що враховуватиме національні особливості та водночас ґрунтуватиметься на міжнародній координації, а також поєднуватиме технологічний прогрес із захистом прав людини.

Аналіз особливостей особливостей виклик та тенденцій розвитку механізмів інформаційної безпеки дозволив нам дійти наступних умовиводів.

По-перше, сучасні механізми інформаційної безпеки формуються в умовах поєднання глобальних та національних факторів ризику, серед яких особливе місце займають гібридні війни, дезінформаційні кампанії, кібератаки та посилення інформаційної асиметрії. Це створює складне багаторівневе середовище, яке вимагає адаптивних стратегій реагування.

По-друге, розвиток новітніх технологій, таких як штучний інтелект, великі масиви даних, deepfake-технології та алгоритмічна маніпуляція, значно розширює спектр інформаційних загроз. Водночас ці ж технології можуть бути використані як інструменти зміцнення інформаційної безпеки, що вимагає вироблення збалансованої політики їх регулювання та застосування.

По-третє, соціальні мережі та цифрові платформи виступають подвійним чинником: вони є середовищем поширення ризиків та маніпуляцій, але водночас відкривають нові можливості для демократизації суспільства, розвитку цифрової культури та протидії загрозам. Це обумовлює необхідність формування комплексної політики, яка поєднуватиме регуляторні, комунікаційні та освітні заходи.

По-четверте, інформаційна гігієна та розвиток культури кіберстійкості виступають базовими елементами захисту інформаційного простору. Освітні програми в школах, університетах і державних інституціях забезпечують формування відповідального ставлення громадян до інформаційного

середовища, що зменшує вразливість суспільства до дезінформації та маніпуляцій. Таким чином, освіта стає ключовим інструментом зміцнення національної стійкості до інформаційних загроз.

По-п’яте, регуляторні та правові механізми є необхідним інституційним підґрунтям для ефективної протидії ризикам цифрової трансформації. Новітні ініціативи, зокрема Digital Services Act, Data Governance Act та національні стратегії кібербезпеки, демонструють спроби поєднати захист суспільства від дезінформації й кібератак із гарантуванням прав людини та свободи слова. Збалансоване правове регулювання дозволяє уникнути надмірного обмеження цифрових платформ і водночас забезпечити стійкість держави та суспільства до інформаційних загроз.

5.2. Державно-управлінські та міжсекторальні механізми забезпечення інформаційної безпеки в умовах гібридних загроз

Сучасні гібридні загрози, що поєднують кібернетичні атаки, інформаційні кампанії, дезінформацію та інші інструменти впливу, істотно ускладнюють традиційні підходи до гарантування національної безпеки. Їхня особливість полягає у розмитості меж між воєнними, політичними, економічними та інформаційними інструментами, що вимагає від держави комплексної системи управління, здатної швидко реагувати на багаторівневі виклики. У цьому контексті інформаційна безпека постає не лише технічною чи правовою категорією, а насамперед предметом ефективної організації управлінських процесів на національному та міжнародному рівнях.

Ключовим завданням в даному випадку є пошук оптимальної моделі координації зусиль державних і недержавних інституцій, адже централізоване ухвалення рішень забезпечує єдність і швидкість реагування, але може страждати від надмірної бюрократизації, тоді як децентралізований підхід дозволяє враховувати специфіку окремих секторів, проте породжує ризик

розбалансованості й дублювання функцій. Додатковим важливим виміром виступає розвиток публічно-приватного партнерства, яке дедалі більше визнається необхідним у сфері інформаційної безпеки, враховуючи роль приватних компаній (від банківського сектору й телекомунікацій до соціальних мереж) як критично важливих акторів кібер- та інформаційного простору.

Таким чином, аналіз моделей управління інформаційною безпекою в умовах гібридних загроз дозволяє не лише оцінити їх сильні та слабкі сторони, а й визначити можливості для формування збалансованої системи, де держава виступає координатором, але не єдиним виконавцем, забезпечуючи синергію зусиль усіх ключових суб'єктів.

Централізована модель управління інформаційною безпекою передбачає концентрацію основних функцій із координації, планування та реагування на інформаційні загрози в руках спеціально уповноважених державних органів. Вона ґрунтується на уніфікованій системі прийняття рішень, чіткій ієрархії повноважень і відповідальності та оперативному управлінні ресурсами. Такий підхід зазвичай вважається найбільш ефективним у ситуаціях, коли необхідна швидка мобілізація державних інституцій для протидії масштабним кібератакам чи інформаційним кампаніям. Водночас централізована модель може бути надмірно бюрократизованою та недостатньо чутливою до специфіки окремих секторів.

Одним із найяскравіших прикладів централізованого підходу є модель, запроваджена у США після терактів 11.09. 2001 р. Так, створення Міністерства внутрішньої безпеки (Department of Homeland Security, DHS) дозволило зосередити під одним дахом функції кіберзахисту, захисту критичної інфраструктури та протидії тероризму. У структурі DHS, як ми зауважували раніше, діє Агентство з кібербезпеки та безпеки інфраструктури (CISA), яке виконує роль координаційного центру для всіх федеральних відомств та приватного сектору. Важливою особливістю є те, що CISA виступає не лише як орган реагування, а й як центр стратегічного прогнозування, аналітики та

розробки стандартів кіберстійкості, що згодом впроваджуються на рівні всіх штатів, що забезпечує єдину систему стандартів, уникаючи хаотичності у сфері інформаційної безпеки.

Не менш показовим є досвід Ізраїлю, який розглядається як одна з найбільш кіберстійких держав світу. Тут у 2017 р. було створено Національний кібердиректорат (Israel National Cyber Directorate, INCD), підпорядкований безпосередньо прем'єр-міністру. Так, INCD концентрує в собі функції з моніторингу кіберзагроз, реагування на інциденти та розробки державної політики у сфері кіберзахисту, а центральне підпорядкування забезпечує швидкість ухвалення рішень та координацію між військовими, розвідувальними та цивільними структурами. Водночас, держава створює інституційні платформи співпраці з приватним сектором, але вони інтегровані саме в єдину вертикаль управління. Тобто, ізраїльська модель показує, як централізація не лише не суперечить розвитку інноваційного сектору, а й створює для нього чіткі безпекові рамки.

Цікавим є й досвід Великої Британії, де функціонує Національний центр кібербезпеки (National Cyber Security Centre, NCSC) у складі Штаб-квартири урядового зв'язку (GCHQ), що дозволяє поєднати аналітичний потенціал спецслужб і практичний вимір реагування на інциденти. Як результат, формується високий рівень довіри між державою та суспільством, адже NCSC працює не лише з урядовими структурами, а й активно взаємодіє з університетами, науковими центрами та бізнесом. Одночасно з цим, саме централізований контроль за діяльністю NCSC забезпечує єдність підходів до управління ризиками та інформаційної безпеки у всіх секторах [137, с. 125].

В Україні централізовану модель реалізують насамперед через діяльність Ради національної безпеки і оборони України та Служби безпеки України. Відповідно до законодавства, саме СБУ уповноважена здійснювати заходи у сфері захисту державних інформаційних ресурсів, протидії кіберзлочинам та інформаційним атакам. В свою чергу, як ми зазначали раніше, РНБО координує

діяльність усіх суб'єктів сектору безпеки та оборони, визначаючи стратегічні пріоритети і формуючи нормативну базу. Знову-таки, у 2021 р. ухвалено нову Стратегію кібербезпеки України, де передбачено створення єдиної системи реагування на кіберінциденти, що безпосередньо свідчить про посилення централізованих управлінських механізмів.

Однак, українська централізована модель стикається з низкою обмежень. По-перше, це дублювання повноважень між різними інституціями, що знижує ефективність управління. По-друге, нерідко бракує належної координації з приватним сектором, який фактично контролює критичну цифрову інфраструктуру. По-третє, в умовах війни рф проти України централізація управління інформаційною безпекою часто реалізується у форматі кризових рішень, а не системних інституційних механізмів.

Порівняння з іноземними моделями дає змогу виділити кілька напрямів, які Україна могла б імплементувати. Створення єдиного національного центру кібер- та інформаційної безпеки за аналогією з CISA у США чи NCSC у Великій Британії дозволило б уникнути дублювання повноважень та забезпечити координацію всіх суб'єктів. Пряме підпорядкування органу вищим державним посадовцям, як це реалізовано в Ізраїлі, дозволить прискорити ухвалення рішень і підвищити політичну вагу питань кібербезпеки. Формування єдиних національних стандартів кіберзахисту, обов'язкових для державних і приватних структур, могло б бути реалізовано через адаптацію європейських та американських стандартів. Важливою також є комунікаційна функція центрального органу, яка передбачає роботу з громадянами, проведення навчань та інформаційних кампаній. Акцент на інноваційні технології та науку, що реалізується через залучення університетів і дослідницьких інституцій, створює підґрунтя для розвитку власних алгоритмів захисту й підвищує стійкість інформаційного простору.

Серед переваг централізованої моделі слід назвати швидкість ухвалення рішень та реагування на кризові ситуації, уніфікацію стандартів і методів

захисту, чітку вертикаль відповідальності та політичну вагу рішень. Водночас, її слабкими сторонами залишаються ризик бюрократизації та повільності у міжсекторальній взаємодії, обмежена гнучкість у специфічних галузях, концентрація рішень у невеликій групі осіб, що створює політичні ризики, а також недостатнє залучення приватного сектору, який володіє більшістю технологічних ресурсів.

В той же час, децентралізована модель управління інформаційною безпекою передбачає розподіл повноважень між різними державними структурами та секторними органами, де кожен суб'єкт відповідає за безпеку у межах своєї компетенції. Такий підхід, як зазначає М. Данн Кевелті, зазвичай передбачає, що міністерства, відомства, регуляторні агентства та спеціалізовані центри формують і реалізують політику кібер- та інформаційної безпеки у своїй галузі, водночас координуючи дії через міжвідомчі комісії або спільні робочі групи. Основна перевага децентралізації полягає в гнучкості, адаптивності та швидкій реакції на специфічні загрози в різних секторах, однак така система потребує чіткої координації, щоб уникнути розрізненості дій та дублювання функцій.

З наукового погляду, децентралізована модель управління інформаційною безпекою є складним багаторівневим механізмом, що поєднує адміністративні, технічні та комунікаційні аспекти функціонування державної політики у цифровій сфері. Вона створює умови для формування спеціалізованих компетенцій у різних органах влади, дозволяє швидко реагувати на локальні кіберінциденти та інформаційні загрози, а також забезпечує більш гнучке впровадження нових технологічних рішень відповідно до специфіки конкретного сектора або регіону. Такий підхід демонструє практичну відповідність принципам ефективності, оперативності та адаптивності державного управління в умовах постійної зміни цифрового та інформаційного середовища.

Водночас науковий аналіз показує, що децентралізація вимагає високого

рівня міжорганізаційної координації та синхронізації дій. Необхідно створювати єдині стандарти обміну інформацією, уніфіковані протоколи реагування на загрози та механізми контролю за виконанням визначених функцій. Відсутність таких елементів може призводити до фрагментації інформаційного простору, створювати «сліпі зони» у виявленні загроз і знижувати загальний рівень національної кіберстійкості. З погляду теорії державного управління, децентралізована модель водночас виступає лабораторією для тестування нових інструментів управління та технологічних рішень, які потім можуть бути масштабовані на національному рівні.

Більш того, децентралізована модель створює унікальні можливості для інтеграції приватного сектору та громадянського суспільства у процеси забезпечення інформаційної безпеки. Наприклад, через публічно-приватні партнерства, консорціуми та міжвідомчі робочі групи держава може залучати технологічні компанії, наукові установи та незалежні організації до моніторингу, аналізу та протидії кіберзагрозам. Такий підхід сприяє більш ефективній адаптації державних стратегій до реалій швидкоплинного цифрового середовища та забезпечує синергію між різними рівнями компетентності та ресурсами учасників інформаційного простору.

Крім того, децентралізація в управлінні інформаційною безпекою дозволяє формувати спеціалізовані регіональні та секторні команди реагування, що здатні оперативно локалізувати інциденти та мінімізувати їхні наслідки. Наукові дослідження підкреслюють, що подібні підрозділи, інтегровані у загальнодержавну систему, створюють баланс між автономією органів влади та цілісністю національної інформаційної політики. Це, у свою чергу, підсилює надійність державних систем у боротьбі з кіберзагрозами та забезпечує стійкість ключових інформаційних та комунікаційних інфраструктур.

В цілому, децентралізована модель управління інформаційною безпекою виступає одночасно гнучким інструментом адаптації до сучасних викликів та складною системою, що потребує постійної координації, синхронізації та

розбудови інституційної інфраструктури. Вона поєднує в собі оперативність, спеціалізацію, технологічну адаптивність та потенціал для інтеграції різних суб'єктів інформаційного простору, що забезпечує високий рівень національної інформаційної безпеки та ефективне реагування на сучасні кібер- та інформаційні загрози.

Міжнародний досвід показує, що децентралізована модель ефективно працює у країнах із сильною автономією секторних органів. У Німеччині, наприклад, відповідальність за кібербезпеку поділена між федеральним урядом і земельними структурами, де Федеральне відомство з безпеки інформаційних технологій (BSI) визначає загальні стандарти, проводить моніторинг і координацію, а регіональні центри реалізують специфічні заходи захисту, що дозволяє враховувати локальні потреби й особливості критичної інфраструктури, а також забезпечує тісну взаємодію з приватним сектором, який безпосередньо контролює технічні засоби захисту. При цьому, на рівні координації забезпечується спільний обмін інформацією про загрози, що дозволяє формувати загальнодержавну стратегію безпеки.

В Японії секторний підхід реалізований через поділ відповідальності між Міністерством внутрішніх справ та комунікацій, Міністерством економіки, торгівлі та промисловості та окремими регуляторами фінансового та енергетичного секторів. Кожна структура має власні програми кіберзахисту та планування кризового реагування, а державний центр кібербезпеки координує міжсекторальну взаємодію та видає загальні рекомендації, що дозволяє швидко реагувати на специфічні загрози в конкретних секторах і зменшує бюрократичне навантаження на центральні органи, водночас, створюючи виклики уніфікації стандартів та контролю за дотриманням правил безпеки.

Маємо зазначити, що в українських умовах децентралізована модель проявляється через діяльність секторних міністерств, регуляторних органів та спеціалізованих центрів, що відповідають за кібербезпеку та інформаційний захист у межах своїх повноважень. Наприклад, Міністерство цифрової

трансформації України (Мінцифра) координує розвиток електронних послуг та кіберзахист державних інформаційних систем (пп. 9.7 п. 4 Постанови КМУ № 856 від 18.09.2019 р. Питання Міністерства цифрової трансформації), Національний банк України здійснює регулювання та захист фінансової інформації (п. 34 ч. 1 ст. 7 Закону України «Про Національний банк України» № 679-XIV), а Державна служба спеціального зв'язку та захисту інформації України відповідає за критичну інформаційну інфраструктуру (абз. 2, абз. 5 ч. 1 ст. 3 Закону України «Про Державну службу спеціального зв'язку та захисту інформації України» № 3475-IV). На додаток, децентралізація дозволяє враховувати специфіку кожного сектору і забезпечує більш гнучке реагування на загрози, зокрема в умовах інформаційної війни.

Однак, існують і певні обмеження децентралізованої моделі. Наприклад, розгалуженість повноважень може призводити до непослідовності у застосуванні стандартів безпеки та створювати прогалини у взаємодії між органами, а відсутність належних, дієвих та проактивних механізмів координації породжує проблему ризику дублювання дій та невикористання синергії між суб'єктами, що ускладнює вироблення узгодженої національної стратегії. На наше переконання, для України потенційно корисним є запозичення елементів координаційних механізмів Німеччини чи Японії, зокрема створення міжвідомчих робочих груп, централізованого обміну аналітичною інформацією та формування загальнодержавних стандартів, обов'язкових для всіх секторів, що дозволить створити національну модель забезпечення інформаційної стабільності, засновану на багатосторонньому реагуванні та респонденції на загрози, побудова котрої базується на, в тому числі, інституційній підготовленості.

Серед переваг децентралізованої моделі слід визначити високий рівень адаптивності та гнучкості, можливість врахування специфіки окремих секторів, швидке реагування на локальні загрози та залучення експертного потенціалу галузевих органів. Слабкими сторонами, на противагу, є ймовірність

розрізненості стандартів, низька узгодженість між органами, ризик втрати оперативного контролю у кризових ситуаціях і потреба у постійному моніторингу та інтеграції даних між усіма суб'єктами системи.

Таким чином, децентралізована модель управління інформаційною безпекою демонструє значний потенціал для адаптації до умов України в інституційно-забезпечувальному розрізі, однак її ефективність значною мірою залежить від створення координаційних механізмів, єдиних стандартів та тісної взаємодії з приватним сектором і громадянським суспільством, що дозволить поєднати гнучкість і оперативність із національною безпековою стратегією.

Натомість, публічно-приватне партнерство у сфері інформаційної безпеки являє собою модель, у межах якої державні органи та приватні суб'єкти спільно розробляють, впроваджують та контролюють заходи щодо захисту інформаційного простору. Дана модель передбачає, що критична інфраструктура, фінансові системи, телекомунікаційні мережі та цифрові платформи перебувають під спільним наглядом держави та приватних операторів, які володіють необхідними технічними та експертними ресурсами. Відмінною рисою публічно-приватного підходу є взаємодія на основі партнерських угод, стандартів кібербезпеки та оперативного обміну інформацією про загрози, що дозволяє забезпечувати комплексний захист від зовнішніх і внутрішніх ризиків.

Міжнародний досвід демонструє ефективність цього підходу у різних країнах. У США, наприклад, критична інфраструктура перебуває під контролем федеральних агентств, таких як раніше зазначене Cybersecurity and Infrastructure Security Agency (CISA), але у тісній співпраці з приватними компаніями, що забезпечують енергетику, фінанси, телекомунікації та інші важливі сектори. У даному контексті CISA організовує спільні робочі групи, проводить навчання для приватних партнерів і здійснює моніторинг кіберзагроз, а приватні компанії надають оперативну інформацію про атаки, уразливості та інциденти, що сукупно надає змогу поєднувати державний контроль і регуляторні

повноваження з технічною експертизою та ресурсами приватного сектору, що значно підвищує стійкість національної системи безпеки.

У Великій Британії публічно-приватне партнерство реалізоване через програму Cyber Security Information Sharing Partnership (CiSP), яка забезпечує безпечний обмін інформацією між урядом, органами правоохоронних структур та приватними компаніями. Партнери мають доступ до аналітичних звітів, рекомендацій щодо захисту критичної інфраструктури та засобів протидії кіберзагрозам, що дозволяє значно зменшити час реагування на інциденти. Крім того, у рамках CiSP реалізуються навчальні програми та тренінги для персоналу компаній, що підвищує рівень кіберстійкості приватного сектору та сприяє формуванню корпоративної культури безпеки.

В українських умовах публічно-приватне партнерство проявляється через взаємодію державних органів, таких як Служба безпеки України, Державна служба спеціального зв'язку та захисту інформації України, Національний банк України, та приватних операторів критичної інфраструктури, як-от телекомунікаційнії компанії, банківські установи, поштові оператори і провайдери хмарних сервісів. У даному випадку, говоримо про змогу отримувати оперативну інформацію про кіберінциденти, координувати спільні заходи протидії загрозам та розробляти стандарти безпеки, що враховують специфіку різних секторів економіки. Особливої актуальності подібна парадигма набуває у контексті гібридних загроз і інформаційних атак, коли час реагування та своєчасне оповіщення партнерів критично впливає на ефективність захисту.

Перевагами моделі публічно-приватного партнерства є інтеграція експертних ресурсів приватного сектору у державну систему безпеки, оперативний обмін інформацією про загрози, можливість швидкої адаптації до нових технологій і загроз, а також формування культури безпеки серед користувачів та компаній. Водночас, до викликів та часткових недоліків можна віднести потребу в законодавчо визначених механізмах захисту даних та

конфіденційної інформації, баланс між контролем та свободою діяльності приватних компаній, забезпечення довіри між державою та бізнесом. Для України актуальним є запозичення практик США та Великої Британії, особливо щодо створення спільних центрів реагування на кіберінциденти, організації регулярного обміну аналітичними даними, спільних навчальних програм та формування стандартів, обов'язкових для всіх учасників партнерства, що надасть змогу державі належним чином керувати інформаційним простором за допомогою інформаційних технологій, що мають ресурсно-інвестиційну афіліацію.

Таким чином, публічно-приватна модель управління інформаційною безпекою дозволяє створити більш гнучку, адаптивну та технічно підготовлену систему, що інтегрує державні повноваження та ресурси приватного сектору. Ефективність цього підходу в Україні, на наше особисте переконання, залежатиме від чіткої нормативної бази, високого рівня довіри між державою та бізнесом, а також від здатності швидко адаптуватися до нових технологій і гібридних загроз, забезпечуючи баланс між захистом критичної інформаційної інфраструктури та правами та свободами громадян.

Розглядаючи сучасні підходи до забезпечення інформаційної безпеки, необхідно виділити ключову проблематику, яка об'єднує всі моделі управління — централізовану, децентралізовану та побудовану на принципах публічно-приватного партнерства. Нею є ті виклики координації та ефективності державних систем у контексті гібридних загроз, що визначаються не лише технологічними факторами, а й складністю взаємодії між різними рівнями державного управління та приватними суб'єктами, котрі беруть участь у формуванні безпечного цифрового середовища.

Першим критичним аспектом є проблематика взаємодії між центральними органами та секторними агентствами. У централізованих моделях, як у США чи Ізраїлі, єдність стратегій та стандартів забезпечується через вертикальне підпорядкування ключових органів, проте навіть тут

виникають ризики конфліктів компетенцій та дублювання функцій на місцевому або секторному рівні, тоді як децентралізовані моделі, які передбачають автономність міністерств, відомств та регуляторних органів у межах їхніх повноважень, створюють додаткову складність у синхронізації заходів безпеки та швидкому реагуванні на кібератаки або кампанії дезінформації. Особливої актуальності зазначене набуває в контексті публічно-приватного партнерства, де приватні компанії залучені до спільного моніторингу та реагування, але водночас мають власні стандарти безпеки та обмеження на передачу конфіденційної інформації. Внаслідок цього, будь-яка модель потребує розвинених механізмів координації, формалізованих каналів комунікації та системи узгодження повноважень між учасниками, щоб уникнути хаотичності дій та затримок у реагуванні на інциденти.

Наступним викликом-контраверсією є питання довіри та взаємодії між державою та приватним сектором, що прямо впливає на ефективність публічно-приватних моделей. Успіх цих систем залежить від прозорості процесів, наявності законодавчо закріплених механізмів захисту даних і конфіденційної інформації, а також чіткої регламентації прав і обов’язків приватних партнерів. В цей же час, недостатність рівня довіри або непрозорість механізмів обміну інформацією можуть призводити до затримок у виявленні загроз, уповільнення реагування та виникнення правових колізій. Так, централізовані системи, які встановлюють єдині стандарти для всіх учасників, здатні зменшити ці ризики, але вони потребують постійного діалогу з приватними компаніями, щоб забезпечити оперативність обміну даними та адаптацію до нових технологій, а децентралізована модель, навпаки, надає секторним органам більшу автономію, що полегшує локальну взаємодію з бізнесом, але вимагає створення координаційних платформ і міжвідомчих робочих груп для забезпечення узгодженості дій у масштабах держави.

Третім ключовим аспектом є інтеграція національного законодавства та міжнародних стандартів кібербезпеки у роботу всіх моделей управління.

Швидкий розвиток технологій, застосування штучного інтелекту, великих даних (big data) та аналітики загроз ставлять перед державою завдання не лише адаптувати нормативно-правову базу, а й забезпечити баланс між захистом інформаційної безпеки та дотриманням прав людини у цифровому середовищі. Централізовані моделі мають перевагу у швидкому прийнятті нормативних рішень, проте ризикують втратити гнучкість у врахуванні специфіки різних секторів та регіонів. Децентралізовані підходи, в свою чергу, дозволяють враховувати локальні та галузеві особливості, однак потребують постійного контролю за узгодженістю правових норм та стандартів. На додаток, публічно-приватне партнерство доповнює ці моделі, забезпечуючи можливість експериментальної імплементації новітніх технологій у рамках державних стратегій безпеки, але одночасно вимагає прозорих правил для обміну інформацією та дотримання конфіденційності.

Наявність цих трьох груп викликів демонструє, що координація та ефективність державних систем інформаційної безпеки неможлива без інтеграції принципів централізації, децентралізації та публічно-приватного партнерства. Централізовані органи визначають стратегічні орієнтири та стандарти, секторні органи адаптують їх до особливостей галузей, а приватний сектор забезпечує технологічну експертизу та оперативний моніторинг загроз. Виключно у поєднанні цих елементів можна створити багаторівневу систему, здатну ефективно реагувати на гібридні загрози, зменшувати час реагування на кіберінциденти та підтримувати високий рівень довіри суспільства до державних інституцій.

Крізь призму наукового виміру, питання координації та ефективності у забезпеченні інформаційної безпеки є фундаментальною складовою державного управління, оскільки сучасний інформаційний простір характеризується високим рівнем складності, динамічними технологічними змінами та постійним ризиком гібридних загроз. Центральна роль у цьому контексті належить не лише органам державної влади, а й приватним та громадським інституціям, що

активно взаємодіють у сфері кібер- та інформаційної безпеки. Науковий аналіз існуючих моделей показує, що жодна з них не може функціонувати ефективно ізольовано: централізація забезпечує єдність стандартів та швидке прийняття рішень, децентралізація дозволяє адаптувати політику до локальних та секторних особливостей, а публічно-приватне партнерство інтегрує технологічну експертизу та оперативне реагування.

Координаційні виклики, що виникають у централізованих моделях, демонструють необхідність створення механізмів міжвідомчого діалогу та постійного моніторингу для уникнення дублювання функцій і конфліктів компетенцій. У децентралізованих системах ключовим аспектом стає синхронізація заходів безпеки між автономними органами, що потребує формалізованих платформ, міжвідомчих робочих груп та уніфікованих протоколів обміну інформацією. Публічно-приватне партнерство, у свою чергу, додає додатковий рівень складності, оскільки приватні компанії мають власні внутрішні стандарти безпеки, обмеження на обмін конфіденційними даними та певні економічні та технологічні пріоритети, що потребує чіткої правової регламентації та прозорості процедур.

На рівні стратегічного управління інтеграція національного законодавства та міжнародних стандартів кібербезпеки є критичною, адже швидкий розвиток технологій, штучного інтелекту та аналітики загроз потребує балансування між забезпеченням безпеки та дотриманням прав людини. Централізовані системи можуть оперативно впроваджувати нові нормативні рішення, але ризикують втратити гнучкість у врахуванні специфіки різних секторів і регіонів, децентралізовані системи забезпечують адаптацію до локальних умов, але вимагають постійного контролю за узгодженістю норм та стандартів. Публічно-приватне партнерство доповнює цей баланс, надаючи можливість тестувати новітні технології та адаптувати їх у державних стратегіях безпеки, водночас забезпечуючи дотримання правил конфіденційності та прозорості обміну даними.

Власний аналітичний висновок полягає у тому, що ефективна багаторівнева система управління інформаційною безпекою повинна поєднувати три виміри: стратегічне централізоване планування, адаптивну децентралізацію та інтеграцію технологічного та експертного потенціалу приватного сектору. Така синергія забезпечує оперативність реагування, зменшує час на виявлення та локалізацію загроз, підвищує стійкість національної інформаційної інфраструктури та формує високий рівень довіри суспільства до державних інституцій.

Додатково, міжнародний вимір посилює необхідність узгодження стандартів та процедур між країнами. В умовах глобалізації інформаційного простору кіберзагрози не мають кордонів, що ставить завдання уніфікації норм та процедур у рамках міжнародних договорів, рекомендацій та коаліцій. У даному контексті, централізовані моделі на національному рівні отримують підтримку міжнародних організацій у вигляді методичних рекомендацій та стандартів, тоді як децентралізовані структури забезпечують локальне впровадження цих норм, а публічно-приватні ініціативи сприяють обміну інформацією та технологічними практиками у реальному часі, що, як слушно зазначає американський дослідник П. Бовен, на синергічному рівні дозволяє підвищити ефективність реагування на кіберінциденти та інтегрувати сучасні технологічні рішення у національну систему безпеки без втрати контролю та узгодженості.

На основі вищезазначеного можна зробити висновок, що міжнародний вимір у сфері інформаційної безпеки є одним із найскладніших аспектів сучасного державного управління, адже глобалізація інформаційних потоків і цифрових технологій зумовлює високий рівень взаємозалежності між країнами. Кіберзагрози у цьому середовищі набувають транснаціонального характеру, що означає, що локальні чи національні дії будь-якої держави без інтеграції з міжнародними механізмами часто є недостатньо ефективними. Узгодження стандартів і процедур на міжнародному рівні виступає ключовим чинником

формування спільної кіберстійкості та захисту критичної інформаційної інфраструктури, оскільки уніфікація норм дозволяє зменшити розриви у підходах різних країн до оцінки загроз, реагування на інциденти та нормативного регулювання.

Централізовані національні моделі, отримуючи рекомендації та стандарти міжнародних організацій, формують стратегічний каркас, який дозволяє швидко і послідовно впроваджувати найкращі практики у національні системи безпеки. Такі моделі забезпечують єдині протоколи обміну інформацією, стандарти сертифікації кіберзахисту та методики оцінки ризиків, що створює базу для більш ефективного міжнародного співробітництва. Однак сам факт централізації не знімає проблеми необхідності врахування локальних та галузевих особливостей, які вимагають децентралізованого підходу.

Децентралізовані моделі відіграють роль «локальних адаптерів» міжнародних стандартів. Вони дозволяють трансформувати глобальні норми під особливості національного законодавства, технологічної інфраструктури та специфіку окремих секторів економіки чи соціальної сфери. Такий підхід дає змогу враховувати національні особливості інформаційного простору, регіональні ризики та локальні загрози, забезпечуючи гнучкість та оперативність реагування на інциденти. При цьому децентралізація створює потребу у високорозвинених механізмах координації та синхронізації дій на міжсекторному рівні, щоб уникнути розрізненості підходів і втрати узгодженості з міжнародними стандартами.

Публічно-приватне партнерство виступає третім ключовим виміром, який дозволяє реалізувати технологічну інтеграцію та обмін практичними рішеннями у реальному часі. Приватний сектор, маючи доступ до новітніх технологій, аналітичних платформ та штучного інтелекту, може прискорювати виявлення загроз і впровадження передових заходів кіберзахисту, тоді як державні органи забезпечують правову та регуляторну основу. Такий симбіоз дозволяє не лише підвищити оперативність реагування, а й інтегрувати нові технології у

національні стратегії безпеки, зберігаючи контроль та узгодженість дій.

Власна аналітика підкреслює, що міжнародна інтеграція у сфері інформаційної безпеки повинна враховувати три взаємопов'язані рівні: стратегічний (централізоване визначення стандартів та нормативів), локальний (деконцентрація для адаптації під національні та регіональні умови) і технологічний (публічно-приватне партнерство для швидкої імплементації та моніторингу загроз). Такий комплексний підхід забезпечує не лише ефективність на національному рівні, а й формує основу для глобальної кіберстійкості та взаємодії між державами. У перспективі, розвиток міжнародних коаліцій, обмін досвідом та уніфікація процедур сприятимуть формуванню глобальної системи протидії кіберзагрозам, де ефективність окремої держави безпосередньо залежатиме від її інтеграції у міжнародний безпековий контекст.

Крім того, інтеграція міжнародного виміру дозволяє враховувати етичні та правові аспекти, зокрема захист персональних даних та дотримання прав людини, що стає особливо актуальним у цифровому середовищі з розвинутими алгоритмічними платформами та соціальними мережами. Впровадження міжнародних стандартів створює механізми підзвітності та контролю, які запобігають зловживанням і підвищують довіру до державних інституцій, одночасно дозволяючи державам ефективно координувати дії у боротьбі з транснаціональними загрозами.

Таким чином, міжнародний вимір не є додатковим або факультативним компонентом системи інформаційної безпеки: він стає інтеграційним чинником, який забезпечує єдність підходів, підвищує оперативність реагування та формує стійку основу для глобальної кіберстійкості, де національні та міжнародні інтереси органічно поєднані у спільній системі безпеки.

Завершальною складовою викликів координації та ефективності державних систем інформаційної безпеки в умовах гібридних загроз є адаптація

навчальних та освітніх програм до реалій координації та ефективності систем інформаційної безпеки. Так, держави, які поєднують централізовані, децентралізовані та публічно-приватні елементи, активно використовують навчальні центри, тренінги та просвітницькі ініціативи для підготовки кадрів, здатних працювати в умовах складних гібридних загроз, чим забезпечується формування кадрового резерву, підвищення професійної готовності усіх ланок системи та сприяння створенню культури кіберстійкості на рівні держави та приватного сектору одночасно.

Тобто, аналіз викликів координації та ефективності в контексті забезпечення інформаційної безпеки в умовах гібридизації загроз демонструє, що інтеграція централізованого управління, автономних секторних структур та публічно-приватного партнерства є ключовим елементом побудови ефективної національної системи інформаційної безпеки. Така багаторівнева, синергетична модель дозволяє поєднати стратегічне планування, локальну адаптацію та оперативну технологічну підтримку, створюючи механізм, здатний адекватно реагувати на сучасні гібридні загрози, мінімізувати ризики дублювання функцій, забезпечувати прозорість та довіру між державою та бізнесом, а також інтегрувати міжнародні стандарти у національні практики без втрати гнучкості та ефективності.

Загалом же, сукупність проаналізованої та вищевикладеної інформації дозволяє нам говорити про те, що у сучасному інформаційному середовищі, котре характеризується високою динамікою технологічних змін, зростанням кількості кібератак та посиленням впливу дезінформаційних кампаній, держави постійно шукають ефективні механізми забезпечення безпеки інформаційного простору. Гібридні загрози, що поєднують військові, політичні, економічні та інформаційні складові, створюють унікальні виклики для національної системи управління, змушуючи переглядати традиційні підходи до централізації, децентралізації та співпраці з приватним сектором.

Однією з ключових проблем, котру нам вдалося виокремити в процесі

аналізу феномену державно-управлінських підходів до забезпечення інформаційної безпеки в умовах гібридних загроз, є необхідність інтегрувати стратегічне планування, оперативне реагування та технологічне забезпечення у єдину систему, яка здатна працювати синхронно на всіх рівнях, що включають центральні органи влади та секторні агентства та приватні партнерства. Означене вимагає не лише формалізованих процедур координації, але й розвитку культури довіри між державними структурами, бізнесом та громадськістю.

У вищеокресленому контексті, державне управління інформаційною безпекою перестає бути суто адміністративною функцією та стає комплексним соціально-технічним феноменом, що включає нормативно-правові засади, організаційну структуру, технологічні інструменти та поведінкові моделі учасників. Важливим елементом стає також взаємодія із міжнародними інституціями та експертними спільнотами, що дозволяє адаптувати національні підходи до стандартів і практик, перевірених на міжнародному рівні.

Водночас, досвід різних країн демонструє, що жодна окрема модель управління не є універсальною. Як вже було зазначено, централізовані системи забезпечують єдність стратегій та стандартизацію, але можуть втрачати гнучкість у локальних умовах, в той час як децентралізовані підходи підвищують автономію секторних органів і враховують специфіку галузей, але потребують додаткових механізмів координації. Натомість, публічно-приватне партнерство відкриває нові можливості для інтеграції технологічної експертизи та ресурсів приватного сектору, однак вимагає прозорих правил взаємодії та дотримання балансу між контролем і свободою бізнесу, проте за умови апропріативного залучення може виступати чинником розвитку дата-захищеності держави та її інституційного, урядово-управлінського апааратів.

Тобто фактично, для держави, що прагне побудувати ефективну систему захисту від гібридних загроз, критично важливо поєднувати всі ці елементи у синергетичну модель управління, де стратегічна цілісність, локальна

адаптивність та оперативна взаємодія приватного та державного секторів стають рівноправними складовими безпеки.

Отже, узагальнюючи, дослідження феномену державно-управлінських підходів до забезпечення інформаційної безпеки в умовах гібридних загроз дозволило нам дійти наступних умовиводів.

По-перше, ефективність національної системи інформаційної безпеки неможлива без синергетичного поєднання централізованих органів, децентралізованих секторних агентств та публічно-приватного партнерства. Кожна з цих складових виконує свою специфічну роль: централізовані структури визначають стратегічні пріоритети та стандарти, секторні органи адаптують їх до потреб окремих галузей, а приватний сектор забезпечує оперативний моніторинг загроз і технологічну підтримку. Тільки інтегроване використання всіх трьох підходів дозволяє створити багаторівневу систему, здатну швидко реагувати на гібридні виклики та мінімізувати ризики дублювання функцій.

По-друге, ключовим фактором успішності таких систем є налагодження ефективної координації та довіри між учасниками. Централізовані органи потребують чітких комунікаційних каналів і механізмів взаємодії із секторними структурами, тоді як децентралізовані агентства мають забезпечити узгодженість своїх дій із загальнонаціональними стандартами. Публічно-приватні партнерства, у свою чергу, вимагають прозорих правил обміну інформацією та захисту конфіденційних даних, що дозволяє зменшити затримки у реагуванні на інциденти та підвищує готовність системи до швидких змін технологічного та інформаційного середовища.

По-третє, інтеграція національного законодавства та міжнародних стандартів кібербезпеки є необхідною умовою забезпечення балансу між захистом державної безпеки та правами людини у цифровому просторі. Впровадження новітніх технологій, таких як штучний інтелект, аналітика великих даних і системи прогнозування загроз, потребує законодавчої

гнучкості та адаптивності структур управління. Централізовані органи забезпечують швидке ухвалення нормативних рішень, децентралізовані структури — локальну адаптацію, а публічно-приватні ініціативи — експериментальне застосування технологій та оперативну взаємодію між державою та бізнесом.

По-четверте, підготовка фахівців та формування культури кіберстійкості виступають фундаментальними елементами комплексного підходу до інформаційної безпеки. Без належної освіти, навчальних програм та тренінгів на всіх рівнях системи управління неможливо забезпечити ефективне використання технологій, дотримання стандартів та оперативну взаємодію між державними та приватними структурами.

По-п’яте, підсумкова оцінка свідчить, що побудова ефективної національної системи інформаційної безпеки в умовах гібридних загроз потребує не лише технічних рішень, а й комплексного управлінського підходу, який поєднує стратегічне планування, локальну адаптацію та синергію між державним і приватним секторами. Така інтегрована модель дозволяє мінімізувати ризики, забезпечує швидке реагування на кіберінциденти та підтримує високий рівень довіри суспільства до державних інституцій.

Після детального аналізу державно-управлінських підходів до забезпечення інформаційної безпеки в умовах гібридних загроз стає очевидним, що ефективність національної системи безпеки не обмежується лише внутрішньодержавними механізмами. Зростання складності кібератак, дезінформаційних кампаній та технологічних загроз підкреслює необхідність комплексного підходу, який поєднує державні інституції, секторні органи, приватні компанії, громадянське суспільство та міжнародні інституції. Саме така багаторівнева координація є ключовою умовою для формування стійкого цифрового середовища та здатності держави швидко реагувати на виклики сучасного інформаційного простору.

У даному розрізі, розгляд механізмів стратегічної взаємодії між

державою, суспільством і міжнародними партнерами набуває особливої актуальності. Включення публічно-приватного партнерства, залучення IT-компаній, телекомунікаційного та банківського секторів дозволяє інтегрувати технологічну експертизу та ресурси приватного сектору у національну систему безпеки. Роль громадянського суспільства, зокрема через проактивну участь у народному волевиявленні, просвітницьких ініціативах та стратегічних комунікаціях, забезпечує формування суспільства «критичного мислення» та підвищення медіаграмотності, що, своєю чергою, зменшує ефективність дезінформаційних атак і підвищує загальну кіберстійкість держави.

Не менш важливим є міжнародний вимір. Інтеграція України у глобальні механізми інформаційної безпеки, участь у структурах НАТО та Європейського Союзу (ЄС), дотримання положень Будапештської конвенції, співпраця з центрами «excellence» та міжнародними організаціями на кшталт ООН сприяє запровадженню єдиних стандартів, обміну даними про загрози та координації з партнерами у разі кібератак або кризових ситуацій. Така інтеграція дозволяє поєднати внутрішні національні ресурси з міжнародними практиками, підвищуючи ефективність національної системи безпеки.

Таким чином, аналіз стратегічної взаємодії держави, суспільства та міжнародних партнерів є логічним продовженням розгляду державного управління інформаційною безпекою. Останній дозволяє визначити оптимальні форми співпраці, інтегрувати різні рівні відповідальності та ресурси, а також створює передумови для комплексної моделі національної цифрової стійкості (resilience), здатної протистояти сучасним гібридним загрозам. Саме на основі такого розуміння доцільно перейти до детального огляду компонентів стратегічної взаємодії, що ляжуть в основу Розділу V даного дисертаційного дослідження.

До механізмів стратегічної взаємодії держави, суспільства та міжнародних партнерів як елементів забезпечення інформаційної безпеки можна віднести публічно-приватне партнерство (про нього ми говорили вище),

громадянське суспільство, міжнародний вимір даного питання та концепція впровадження комплексної моделі «національної цифрової стійкості». Розпочнемо із огляду першої категорії, проте у дещо іншому форматі категоризації, аніж загалом в Розділі V даного дисертаційного дослідження.

Публічно-приватне партнерство у сфері інформаційної безпеки, як ми зазначали раніше, виступає одним із ключових елементів сучасної багаторівневої системи захисту цифрового середовища. З огляду на динамічність технологічного розвитку та зростання складності кіберзагроз, державні органи вже не можуть самостійно забезпечити ефективний контроль над інформаційним простором, що охоплює критичну інфраструктуру, телекомунікаційні мережі, фінансовий сектор та комунікаційні платформи. Окрім того, публічно-приватне партнерство у даній галузі дозволяє інтегрувати ресурси, експертизу та технологічні можливості приватного сектору у державну систему, створюючи умови для більш гнучкого і швидкого реагування на загрози, що актуально у країнах, що перебувають під впливом гібридних загроз, коли атаки здійснюються не лише на державні системи, а й на приватні компанії, які формують критичну частину національної інфраструктури.

Основними учасниками публічно-приватного партнерства у сфері інформаційної безпеки є великі ІТ-компанії, оператори телекомунікацій, банки та інші фінансові установи. Дані суб’єкти, як слушно зазначає український вчений В. Аніщук [285], не лише володіють технологічними платформами, на яких працюють державні та приватні сервіси, але й накопичують значний обсяг даних, необхідних для виявлення кіберзагроз, аналізу поведінки користувачів та прогнозування потенційних атак. В умовах публічно-приватного партнерства, державні органи отримують доступ до оперативної інформації про інциденти, уразливості та спроби несанкціонованого втручання, що дозволяє формувати цілісну картину загроз і своєчасно реагувати на них, а для приватних компаній співпраця з державою забезпечує чіткі стандарти безпеки, правову підтримку та можливість узгодженої участі у заходах протидії

кіберзлочинності.

На основі цього можемо зазначити , що публічно-приватне партнерство (ППП) у сфері інформаційної безпеки сьогодні розглядається як механізм обміну інформацією та багаторівневої взаємодії держави та бізнесу. У сучасному цифровому середовищі, де кіберзагрози мають швидкоплинний характер і здатні трансформуватися в режимі реального часу, ключовим фактором успішного функціонування ППП є оперативність обміну даними між усіма учасниками. Великі ІТ-компанії та оператори телекомунікацій, які контролюють критичну інфраструктуру та цифрові платформи, стають своєрідними «сенсорами» для держави, здатними виявляти аномалії у трафіку, спроби несанкціонованого доступу, розповсюдження шкідливого програмного забезпечення та інші загрози.

Фінансовий сектор у цьому контексті виконує функцію детектора потенційних кібератак, оскільки будь-які несанкціоновані транзакції, втручання у платіжні системи чи спроби фішингових атак швидко відображають тенденції розвитку загроз і дозволяють адаптувати превентивні заходи. Водночас, науковий погляд на ППП вказує на те, що ефективність цієї взаємодії напряму залежить від рівня довіри між державою та приватним сектором, а також від наявності прозорих регламентів обміну інформацією. Недостатня прозорість або нерегламентованість може призводити до затримок у реагуванні на кіберінциденти, а також до потенційних конфліктів щодо обсягу доступу до чутливих даних.

Важливо відзначити, що ППП не обмежується лише оперативним реагуванням. Воно включає елементи стратегічного планування, зокрема спільне моделювання сценаріїв кібератак, тестування новітніх технологічних рішень та розробку стандартів кіберстійкості, які інтегруються у національні політики. Державні органи, отримуючи доступ до аналітичних даних від приватних компаній, можуть ефективно координувати міжвідомчі заходи та формувати єдину концепцію інформаційної безпеки на національному рівні, що

особливо актуально у випадках загроз, які мають потенційно транснаціональний характер.

Крім того, публічно-приватне партнерство сприяє розвитку інновацій у сфері кібербезпеки. Приватні компанії мають можливість швидко впроваджувати нові алгоритми виявлення загроз, рішення на основі штучного інтелекту, аналітику великих даних (big data), тоді як держава забезпечує нормативну, правову та етичну рамку, яка гарантує захист персональних даних, конфіденційної інформації та дотримання прав людини. Такий симбіоз забезпечує баланс між технологічною ефективністю та правовою безпекою, підвищуючи стійкість цифрового простору держави.

На нашу думку, подальший розвиток ППП у сфері інформаційної безпеки потребує уваги до кількох стратегічних аспектів. По-перше, необхідно створювати централізовані платформи для обміну даними, які одночасно підтримують високий рівень кіберстійкості та гарантують захист конфіденційної інформації. По-друге, важливо впроваджувати стандартизовані протоколи взаємодії між державними та приватними структурами, щоб уникнути дублювання функцій і забезпечити швидке реагування на загрози. По-третє, перспективним є використання ППП для навчання та підвищення кваліфікації кадрів як державного, так і приватного сектору у сфері кібербезпеки, що сприяє формуванню культури безпеки на всіх рівнях.

Таким чином, публічно-приватне партнерство виступає не лише інструментом оперативного реагування на кіберзагрози, а й механізмом стратегічного розвитку національної інформаційної безпеки, забезпечуючи інтеграцію технологічної експертизи, нормативного регулювання та практичної взаємодії між державою та бізнесом, що є необхідною умовою для формування стійкої та адаптивної системи захисту цифрового простору.

Суттєвим елементом публічно-приватного партнерства у галузі інформаційної безпеки є формування спільних аналітичних і навчальних платформ, які дозволяють державі та приватним компаніям координувати дії у

режимі реального часу. Такими платформами у багатьох країнах виступають центри кіберстійкості, що забезпечують обмін інформацією про загрози, розробку рекомендацій щодо стандартів безпеки та методів реагування на інциденти (до питання функціонування у Великій Британії Cyber Security Information Sharing Partnership (CiSP), яка забезпечує безпечний обмін інформацією між урядом, правоохоронними органами та приватними компаніями та де працює отримання аналітичних звітів про кіберзагрози, рекомендації щодо захисту критичної інфраструктури та методики протидії сучасним атакам, що дозволяє значно зменшити час реагування на інциденти та підвищити стійкість системи у цілому).

Іншою ключовою формою публічно-приватного партнерства, про що нами також було зазначено вище за текстом дисертаційного дослідження, у галузі інформаційної безпеки та її безпосереднього забезпечення є організація спільних навчальних програм і тренінгів, спрямованих на підвищення компетенцій працівників приватного та державного секторів, що дозволяє стандартизувати знання щодо кібергігієни, процедур реагування на інциденти та протидії дезінформації. У США, наприклад, неодноразово згадуване нами за текстом дисертації Агентство з кібербезпеки та безпеки інфраструктури (CISA) регулярно, як відмічає американський дослідник Л. Келло, проводить навчальні сесії для банківського сектору, телекомунікаційних компаній та IT-фірм, що сприяє формуванню єдиного підходу до оцінки ризиків і реагування на загрози. Аналогічні практики реалізуються в Ізраїлі, де Національний кібердиректорат (INCD) організовує спільні навчання та вправи для урядових структур і приватного сектору, що забезпечує узгодженість дій під час кризових ситуацій.

Водночас, ефективність публічно-приватного партнерства у галузі забезпечення інформаційної безпеки та підтримання її належного рівня залежить не лише від технічної інтеграції, а й від довіри між державою та приватними компаніями. Недостатньо сформовані законодавчі механізми захисту даних, обмеження на обмін інформацією або непрозорі регуляторні

процедури слугують елементом зменшення ефективності співпраці та залучення приватного інструментарію реалізації подібних ітерацій у державний сектор (до питання функціонування відповідного інституційного устаткування). Централізовані системи, що визначають єдині стандарти, здатні зменшити ці ризики, проте вони потребують гнучких механізмів взаємодії з бізнесом, щоб оперативно адаптуватися до нових технологій та загроз, тоді як децентралізовані моделі надають більшу автономію секторним органам і приватним компаніям, але вимагають узгоджених платформ обміну інформацією, формальних процедур координації та контролю за дотриманням правил безпеки, і у цьому контексті публічно-приватне партнерство виступає синергетичною формою, що поєднує централізовані стандарти та децентралізовану автономію, забезпечуючи ефективний баланс між контролем і гнучкістю (власне, це теза, яку ми логічно проводили і за викладом матеріалу в п. 5.2 Розділу V даного дисертаційного дослідження).

Ключовим викликом публічно-приватного партнерства у галузі забезпечення інформаційної безпеки є впровадження конфіденційності та захисту комерційної та персональної інформації. Приватні компанії часто обмежені у можливості передавати дані державним органам через внутрішні політики безпеки, вимоги законодавства про захист даних або конкурентні інтереси. Водночас, держава зобов’язана гарантувати дотримання стандартів кібербезпеки та швидке реагування на загрози, що передбачає оперативний доступ до інформації, і подолання цього протиріччя вимагає створення формалізованих каналів комунікації, договорів про обмін даними та узгоджених процедур реагування на інциденти, які б захищали права обох сторін.

Публічно-приватне партнерство також є важливим інструментом впровадження інноваційних технологій у сферу інформаційної безпеки. Технології штучного інтелекту, великі дані (big data), аналітичні системи прогнозування загроз та автоматизовані платформи реагування на інциденти

вимагають високого рівня технічної експертизи та фінансових ресурсів, які зазвичай є у приватного сектору. Держава, у свою чергу, формує нормативне поле та визначає стратегічні пріоритети, забезпечуючи легітимність та узгодженість впровадження технологій. Таким чином, публічно-приватне партнерство у галузі забезпечення інформаційної безпеки виступає механізмом трансферу знань і ресурсів, що підвищує загальний рівень кіберстійкості та забезпечує гнучкість у реагуванні на гібридні загрози.

Важливим елементом успішного публічно-приватного партнерства є створення систем моніторингу та оцінки ефективності. Наприклад, регулярне проведення аудитів, симуляційних вправ та аналіз інцидентів дозволить оцінювати, наскільки інтеграція приватного сектора у державні системи підвищує стійкість критичної інфраструктури та інформаційного простору. Такі практики сприяють не лише своєчасному виявленню слабких місць, а й формуванню стандартів і процедур, які можна застосовувати на національному рівні у різних галузях, і, на наше переконання, підлягають застосуванню в рамках як України, котра наразі реалізує власну євроатлантичну, демократичну дирекцією публічно-державного та соціального, інформаційного та політичного розвитку.

Підсумовуючи, публічно-приватне партнерство у сфері інформаційної безпеки є багатовимірним та динамічним механізмом, що поєднує централізоване визначення стандартів і стратегічних орієнтирів державою, децентралізовану автономію секторних органів та експертні ресурси приватного сектору. Дана подвійність та синхронність дозволяє забезпечувати ефективний моніторинг кіберзагроз, своєчасне реагування на інциденти, впровадження інноваційних технологій та підвищення загальної кіберстійкості держави. Надалі розглянемо роль громадянського суспільства, міжнародного виміру та концептуальної моделі «національної цифрової стійкості», які разом формують цілісну стратегію безпеки інформаційного простору.

Перехід від аналізу публічно-приватного партнерства у сфері

інформаційної безпеки до розгляду ролі громадянського суспільства є методологічно виправданим і концептуально логічним. Якщо у випадку з бізнесом (ІТ-компаніями, телекомунікаційними операторами, банківським сектором) йдеться про формування технічних та інституційних механізмів захисту критичної інформаційної інфраструктури, то у площині громадянського суспільства домінує інший вимір — соціокультурний та комунікативний. Його завданням є створення так званої «м'якої архітектури кіберстійкості», що проявляється у здатності суспільства виявляти та нейтралізувати інформаційні загрози, підтримувати довіру до демократичних інституцій та формувати культуру відповідального споживання інформації.

Як наголошує згаданий раніше П. Бовен, «успіх у протидії кіберзагрозам залежить не лише від технологій, але й від соціальних інститутів, які формують довіру, стійкість і здатність до колективної відповіді» [215, с. 7]. Він також дотримується думки, що у сфері управління глобальним інтернетом вирішальним чинником є баланс між державними, приватними та громадськими акторами. Саме громадянське суспільство виступає тією ланкою, яка поєднує технологічні та нормативні механізми з культурно-комунікаційними.

Вищенадана позиція підкреслює надзвичайну важливість соціального виміру у забезпеченні інформаційної безпеки. Громадянське суспільство, в розумінні сучасних теорій державного управління, функціонує як ключовий канал між державними інституціями, приватними структурами та широкою аудиторією користувачів цифрового простору. Воно не лише забезпечує зворотний зв'язок щодо ефективності політик кібербезпеки, але й сприяє формуванню критичного ставлення до інформаційних потоків, розвитку медіаграмотності та підвищенню загальної інформаційної стійкості суспільства.

Баланс між державними, приватними та громадськими акторами, як зазначає П. Бовен, виявляється критичним не лише в управлінні інцидентами, а й у стратегічному плануванні кібербезпеки. Держава формує нормативні рамки,

визначає стандарти, регулює діяльність ключових секторів та забезпечує координацію між відомствами. Приватний сектор, з іншого боку, володіє технологічними ресурсами, аналітичними платформами та інноваційними рішеннями, здатними швидко виявляти загрози та реагувати на них. Громадянське суспільство, у свою чергу, виконує функцію моста, який з'єднує державний і приватний рівні з культурними та комунікаційними практиками населення, сприяючи формуванню довіри та підвищенню ефективності взаємодії між усіма акторами.

Крім того, громадянське суспільство забезпечує легітимацію державних та приватних дій у сфері інформаційної безпеки. Воно здатне контролювати прозорість процесів, сигналізувати про порушення прав людини, брати участь у розробці правил цифрової поведінки та впливати на прийняття стратегічних рішень через громадські платформи, організації та ініціативи. Такий підхід підсилює стійкість національних систем до гібридних атак, інформаційних кампаній та дезінформаційних хвиль, оскільки включає активну участь громадян у протидії загрозам, одночасно підвищуючи рівень відповідальності держави та бізнесу.

Важливо також відзначити, що технологічні та нормативні механізми, без участі громадянського суспільства, ризикують залишатися формальними інструментами, недостатньо адаптованими до поведінкових та соціокультурних аспектів інформаційного середовища. Соціальні інститути, що формують довіру, стають каталізаторами синхронізації дій усіх учасників та забезпечують ефективну комунікацію в умовах надзвичайних ситуацій, кіберінцидентів та масштабних атак на інформаційні системи.

На нашу думку, інтеграція громадянського суспільства у систему управління інформаційною безпекою має відбуватися комплексно: через освітні програми з медіаграмотності, створення громадських платформ для моніторингу кіберзагроз, залучення до формування стандартів безпеки та консультаційні механізми, які дозволяють враховувати думку широкого кола

користувачів. Такий підхід забезпечує не лише швидке реагування на загрози, а й формування колективної стійкості, яка є визначальним фактором ефективності національної та глобальної кібербезпеки.

У підсумку, теза П. Бовена про критичну роль громадянського суспільства в управлінні глобальним інтернетом підтверджує необхідність багаторівневого підходу до інформаційної безпеки, де державні та приватні механізми взаємодіють із соціальними структурами, створюючи систему, здатну адаптуватися до нових викликів, підтримувати довіру та забезпечувати стійкість цифрового простору на національному та міжнародному рівнях.

Одним із ключових інструментів громадянського суспільства у сфері інформаційної безпеки є перевірка інформації (даних) на достовірність. Його завдання полягає не лише у перевірці достовірності інформації, що циркулює в медіа- та соціальних мережах, але й у формуванні критичного мислення як стрижневої навички громадянина у цифрову епоху.

В свою чергу, на теренах України розвиток перевірки даних та інформації на достовірність активізувався після 2014 р. Створення таких ініціатив, як StopFake, VoxCheck, «Детектор медіа», забезпечило інституційний каркас незалежного аналізу інформації. Їхня діяльність включає оперативну перевірку фактів, аналітичні звіти про інформаційні кампанії, освітні програми для журналістів і студентів. Повинні відмічати позитивні елементи такого підходу, адже, в першу чергу, країни з розвиненими незалежними фактчекінговими ініціативами значно швидше відновлюють довіру до медіа після інформаційних атак.

На міжнародному рівні перевірка даних та інформації на достовірність підтримується Європейським Союзом (ЄС), зокрема через діяльність East StratCom Task Force, що систематично фіксує випадки російської дезінформації. У США діють організації PolitiFact, FactCheck.org, які задають стандарти професійної перевірки фактів. Як зазначає К. Вордл, «перевірка даних та інформації на достовірність ефективна лише тоді, коли сприймається як

незалежний та позаполітичний інструмент, що ґрунтується на прозорих процедурах» [215, с. 7].

Таким чином, перевірка даних та інформації на достовірність створює необхідний фундамент для кіберстійкості, адже і спростовує окремі непрадиві дані (відомості) та, однлчасно з цим, підвищує стандарти суспільної дискусії, що ускладнює реалізацію масштабних інформаційних операцій.

Іншим напрямом діяльності громадянського суспільства є стратегічні комунікації, що виходять за межі суто оборонної позиції і передбачають активне формування наративів, які протистоять дезінформації та сприяють зміцненню демократичної єдності.

У згаданій Великій Британії цей підхід було інституціоналізовано через Government Communication Service International (GCSI), який координує взаємодію державних органів, медіа та громадянського суспільства у сфері протидії дезінформації [215, с. 7]. Прикладом успішної синергії між державними та недержавними структурами є також країни Балтії, де громадські організації активно долучаються до створення інформаційних матеріалів, що пояснюють аудиторії механізми пропаганди та формують альтернативні позитивні наративи [215, с. 7].

В українському контексті стратегічні комунікації дедалі більше інтегруються у діяльність громадських організацій. Так, волонтерські ініціативи не лише відстежують дезінформацію, але й створюють контент, спрямований на її випередження. Як зазначає В. Аніщук, «стратегічні комунікації в умовах гібридної війни є стратегічним захистом та стратегічним наступом водночас» [285].

Завдяки цьому стратегічні комунікації виконують подвійну функцію: по-перше, забезпечують швидке реагування на інформаційні атаки, і, по-друге — формують позитивні смислові рамки, що зміцнюють суспільну стійкість.

Найбільш фундаментальною сферою участі громадянського суспільства є розвиток медіаграмотності. На відміну від перевірки даних та інформації на

достовірність чи стратегічних комунікацій, що мають переважно реактивний характер, медіаграмотність є довгостроковою інвестицією у людський капітал та здатна позитивно впливати на загальні кон'юнктурні показники інформаційної захищеності державних органів, державних структур та інституційного профілю.

Так, ЮНЕСКО (UNESCO) у 2017 р. визначила медійну та інформаційну компетенцію (цифрову грамотність) як «Media and Information Literacy» у якості універсальної компетенції XXI ст. [215, с. 7]. Її зміст полягає у поєднанні навичок критичного мислення, розуміння інформаційних екосистем, уміння відрізняти достовірні джерела від маніпулятивних.

Натомість, в Україні у 2024 р. Міністерством цифрової трансформації України було ухвалено Стратегію з розвитку медіаграмотності на період до 2026 р., яка передбачає інтеграцію відповідних курсів у систему загальної та вищої освіти, а також розробку спеціальних програм для дорослого населення. Громадські організації, такі як Академія української преси та Internews-Ukraine, виступають в даному випадку засадничими провайдерами освітніх програм. З цього приводу слушно використати наукову позицію згаданого В. Аніщука, який переконаний, що медіаграмотність є оборонним механізмом і передумовою розвитку інноваційного суспільства, здатного до самоорганізації та захисту у період цифрових викликів та викликів дезінформації, що з них органічно походять [285].

Міжнародний досвід також демонструє важливість цього напряму. Наприклад, у Фінляндії медіаосвіта та медіаграмотність є частиною національної навчальної програми ще з 2016 р., що дозволяє з раннього віку формувати у громадян здатність до критичного сприйняття інформації. В свою чергу, Естонія впроваджує подібні програми у рамках концепції «ціфрової держави».

Таким чином, громадянське суспільство виступає ключовим суб'єктом кібербезпеки у трьох вимірах:

1) перевірка даних та інформації на її апропріативність та достовірність (себто – фактчекінг) забезпечує перевірку та спростування дезінформації, підвищує рівень суспільної довіри до медіа;
2) стратегічні комунікації дозволяють не лише реагувати на атаки, але й активно формувати позитивні смислові рамки;
3) медіаграмотність виступає довгостроковим фундаментом, що створює умови для стійкості суспільства у цифрову добу.

У сукупності, ці напрями утворюють «соціальну інфраструктуру кібербезпеки», яка доповнює інституційні та технологічні механізми держави і бізнесу.

Важливим продовженням проблематики ролі громадянського суспільства у забезпеченні інформаційної безпеки є міжнародний вимір, адже саме в умовах глобалізованого та взаємозалежного цифрового середовища стійкість держави неможлива без інтеграції у ширші системи колективної безпеки. Якщо громадянське суспільство виконує функції внутрішньодержавного імунітету, забезпечуючи критичне мислення, перевірку інформації та даних на достовірність, стратегічні комунікації та медіаграмотність населення, то міжнародні інституції та партнерства формують зовнішні захисні бар'єри, що дозволяють національним системам протидіяти загрозам, які значно перевищують внутрішні можливості окремої країни. Іншими словами, ефективна взаємодія громадян на рівні суспільства має знаходити продовження у міжнародних форматах співпраці, які забезпечують системність, координацію та обмін ресурсами.

Інтеграція України у глобальні механізми інформаційної безпеки є одним з ключових напрямів сучасної державної політики. Членство та партнерство у міжнародних організаціях відкриває доступ до колективних ресурсів, експертизи та спільних технологічних рішень, що підсилює національний потенціал. Зокрема, у контексті Організації Північноатлантичного договору (НАТО) Україна поступово набуває досвіду участі у практичних програмах

кіберзахисту, зокрема у діяльності Центру передового досвіду з кібероборони, що дислокується в Таллінні (Естонія). Участь у спільних навчаннях, тренуваннях і розробці стандартів забезпечує можливість гармонізувати національні системи з альянсівськими вимогами та сприяє підвищенню оперативної сумісності. Крім того, НАТО активно підтримує Україну через трастові фонди та інституційні механізми, спрямовані на модернізацію критичної інфраструктури та підготовку фахівців у сфері кібербезпеки.

Не менш важливою є інтеграція в рамки Європейського Союзу (ЄС), де інформаційна безпека розглядається як частина ширшої концепції цифрової безпеки та суверенітету. Як відомо, ЄС формує стандарти у сфері захисту даних через положення Загального регламенту про захист персональних даних GDPR від 2016 р., критичної інфраструктури (NIS2 Directive) та кіберстійкості, які поступово стають еталонними для країн-кандидатів. Для України цей процес означає необхідність гармонізації законодавства із законодавством ЄС як сторони-підписанта Угоди про асоціацію між Україною та ЄС від 21.03.2014 р. (із подальшими змінами; acquis communautaire), що не лише зміцнює внутрішню безпеку, але й відкриває можливості для глибшої економічної та політичної інтеграції. Спільні проєкти ЄС та України у сфері кібербезпеки, включаючи участь у програмі «Цифрова Європа», натомість дозволяють формувати інституційні та технологічні спроможності, необхідні для протидії гібридним загрозам.

Важливу роль відіграють і механізми, вироблені в рамках ООН, зокрема у площині міжнародного права та вироблення універсальних принципів поведінки держав у кіберпросторі. Україна активно підтримує резолюції Генеральної Асамблеї, що визначають базові норми безпечного функціонування цифрового середовища. Це створює умови для того, щоб у перспективі запобігати правовому вакууму в сфері міжнародної кібербезпеки та закріплювати правила, які унеможливлюють використання кіберпростору для агресії проти суверенітету держав.

Особливої ваги для України набуває Будапештська конвенція про кіберзлочинність від 2001 р., що залишається єдиним універсальним міжнародним договором у цій сфері та створює платформу для уніфікації національного законодавства, розбудови механізмів транскордонної співпраці та забезпечення швидкого реагування на кіберзлочини. Для України важливо не лише формально імплементувати положення конвенції, але й практично використовувати її механізми для взаємодії з правоохоронними органами інших країн, адже сучасні злочини у цифровому середовищі зазвичай мають транснаціональний характер.

Необхідно також відзначити роль центрів передового досвіду та спеціалізованих міжнародних платформ, які акумулюють експертний потенціал, аналітичні інструменти та тренувальні можливості (NATO CCDCOE, ECC Europol, ENISA, CISA – ЄС та США відповідно). Для України участь у таких структурах є способом скоротити відставання у впровадженні новітніх технологій захисту та отримати доступ до глобальних баз даних загроз, що критично важливо у протистоянні гібридним атакам.

Загалом же, міжнародний вимір інформаційної безпеки формує «зовнішній каркас» для внутрішніх зусиль держави та суспільства. Без такої інтеграції будь-які ініціативи з підвищення медіаграмотності чи розвитку публічно-приватного партнерства залишатимуться обмеженими у своїй ефективності. Тільки поєднання громадянської активності, бізнес-інновацій та міжнародної координації може створити комплексну модель «національної цифрової стійкості», яка забезпечить довготривалу спроможність держави функціонувати у цифровому середовищі навіть в умовах гібридних загроз.

Невід’ємним підсумком аналізу публічно-приватних форматів взаємодії, ролі громадянського суспільства та міжнародної інтеграції є висновок про потребу переходу від набору різнорідних інструментів до цілісної моделі «національної цифрової стійкості». На наш погляд, остання має стати базисом усвідомленого розуміння механізмів стратегічної взаємодії держави,

суспільства та міжнародних партнерів щодо забезпечення інформаційної безпеки і, водночас, методологічною платформою, на якій у п. 5.3 Розділу V даного дисертаційного дослідження буде сформовано авторську концепцію розвитку механізмів інформаційної безпеки держави. Власне, тут доцільно вести мову про інтегративну рамку, що дозволить узгодити цілі, ролі, процеси й ресурси на рівні тактичної кібергігієни громадянина та міждержавної координації реагування на гібридні операції, і, як наслідок, стане передумовою формування певного стратегічного плану дій, спрямованого на прикладі України.

Концептуально, національна цифрова стійкість поєднує два горизонти. Першим є превентивно-адаптивний складник, мета якого полягає у забезпеченні спроможності системи передбачати ризики, виявляти слабкі місця та вбудовувати механізми самокорекції у нормальні процеси управління. Інший, в свою чергу, реактивно-відновлювальний, гарантує здатність протистояти впливам, локалізувати шкоду, швидко відновлювати функції та навчатися на пережитих інцидентах. На відміну від класичного розуміння «безпеки» як теоретичної надбудови та певною мірою симулякра, що часто фокусується на блокуванні загроз, модель «національної цифрової стійкості» виходить з допущення невідворотності частини інцидентів у складних, пов’язаних мережах і змінює акцент на зменшення впливу, скорочення часу порушення і підвищення якості повернення до нормального режиму. У теоретичному вимірі, така постановка резонує з напрацюваннями дослідників інженерії стійкості та системної безпеки (наприклад, Е. Голлнагел, Е. Медні та А. Джексон) а в державно-управлінському — з євроатлантичними підходами до стійкості демократичних інституцій, включно з базовими вимогами стійкості Організації Північноатлантичного договору (НАТО) та рамкою кіберстійкості Європейського Союзу (ЄС).

Якщо екстраполювати даний дискурсно-науковий логічний підхід на український контекст, національна цифрова стійкість повинна органічно

поєднати три виміри, розглянуті в попередньому підпункті. На рівні держави, наприклад, зазначаємо необхідність забезпечити узгодженість між централізованим стратегічним керівництвом і децентралізованим виконанням у секторах, побудувати прозорі канали горизонтальної координації, спільні ситуаційні картини та єдині протоколи обміну даними про загрози, що сукупно дозволять впровадити оперативне реагування на кіберінциденти та кіберзагрози, створювані насамперед державою-агресором (рф) з метою деморалізації суспільного духу та підриву авторитетності, компетентності української влади. На рівні суспільства вбачаємо за необхідне наголосити на необхідності перетворення медіаграмотності і перевірки даних та інформації на достовірність на перманентні, інституціалізовані практики, що вбудовані у шкільну й університетську освіту, державну службу та корпоративний сектор (мета – створення повноцінної бази інформаційно-безпекової едукації, опрацювання Інтернет-джерел та викликів, генерованих глобальною мережею). На рівні міжнародної взаємодії, в свою чергу, необхідно забезпечити практичну інтероперабельність із структурами НАТО та ЄС, імплементувати норми Будапештської конвенції про кібезлочинність, підтримувати участь у центрах передового досвіду (CCDCOE) не як символічну, а як навчально-операційну рутину.

Управлінське ядро такої моделі передбачає перехід від «каскадних» політик до циклу безперервного вдосконалення [27, с. 102-104] з окремим рівнем стратегічної аналітики, що працює на випередження. Для України це означає посилення можливостей національної кіберстійкості та галузевих центрів перевірки інформації та спростування неправдивої (недостовірної) інформації, розвиток механізмів швидкого сповіщення та взаємної підтримки між регуляторами, критичними операторами та приватними провайдерами хмарних сервісів, а також впровадження стандартизованих іспитів на стійкість — від перевірки кваліфікації до складних міжвідомчих навчань за сценаріями гібридних операцій (поєднання кібератак, інформаційно-психологічних впливів

та фізичних інцидентів). Усе вищезазначене, на наше особисте переконання, працює із формуванням явища і прецеденту інформаційної стійкості на практиці, нівелюючи контекст та характер декларативного інформаційного навчання, котрого в умовах глобальних викликів сьогодення та інформаційної агресії, зокрема, рф проти України може бути недостатньо.

Ключовим операційним принципом цифрової стійкості є багатоконтурність захисту і відповідальності, що у випадку із генерацією моделі національної цифрової стійкості, може проявлятися у поєднанні технологічних, організаційних та поведінкових надбудов. Так, технологічна надбудова передбачає мінімізацію «єдиних точок відмови» (single points of failure), використання сегментації мереж, нульової довіри (zero trust), криптографічних стандартів і георознесених резервувань, тоді як організаційний генерує ритм взаємодії: політики обміну інформацією про загрози, правові угоди та двосторонні державно-приватні домовленості між державою та бізнесом, протоколи кризових комунікацій, а поведінковий формує дисципліну безпеки у повсякденних практиках користувачів та управлінців, знижуючи частку інцидентів, причиною генерації котрих є «людське походження», себто – людський фактор. Відтак, національна цифрова стійкість є симбіозом технологій та культури, де правильні дії відбуваються за замовчуванням та відлагодженим погодженням, адже процеси спроектовані синхронно – насамперед, з метою формування прецеденту простоти безпечної поведінки порівняно із небезпечною.

Додаткової важливості у контексті формування моделі національної цифрової стійкості в розрізі одного із механізмів стратегічної взаємодії держави, суспільства та міжнародних партнерів щодо забезпечення інформаційної безпеки виступає економіка стійкості. Так, Україна, будучи відкритою цифровою економікою, на наш погляд, має вибудувати механізми розподілу витрат і вигод між державою, операторами критичної інфраструктури та платформними компаніями. Страхування кіберризиків,

фіскальні стимули для інвестицій у безпеку, стандартизовані аудити постачальницьких ланцюгів, вимоги до прозорості програмних компонентів — це інструменти, що переводять національну цифрову стійкість у контексті, де безпека перестає бути «витратами на відповідність», а стає елементом конкурентоспроможності. Для держави тут постає завдання тонкого регулювання, де необхідно задати стандарт і залишити простір для інновацій, установити обов'язок звітування про інциденти — і водночас гарантувати правові запобіжники від зайвого розкриття комерційних таємниць. Окресливши індивідуальне бачення цензу теоретико-практичного впровадження даного підходу в Україні, принагідно зазначимо, що практико-інституціна модель забезпечення інформаційної стійкості в Україні буде представлена у п. 5.3 Розділу V даного дисертаційного дослідження.

Складником, який замикає концепцію-модель національної цифрової стійкості, у ідеально-стратегічному вимірі є інформаційна стійкість як сенсова архітектура. У ній перевірка даних та інформації на достовірність та стратегічні комунікації виконують роль імунітету проти дезінформації, а цифрова освіта створює прецедент рамкування системи та, відповідно, респондеції громадянського суспільства на виклики інформаційного характеру. Як наслідок, у моделі національної цифрової стійкості потрібна постійна інституційна присутність громадянського суспільства — у дорадчих радах, у спільних аналітичних хабах, у навчальних програмах для держслужбовців та журналістів. Подібний стан справ є функціональною необхідністю, адже без громадського компонента неможливо підтримувати довіру, так як це є головним ресурсом, на якому тримаються як демократичні інститути, так і координація під час криз (до питання феномену інклюзування інформаційного простору як частини описаної нами моделі).

Міжнародна співмірність цієї моделі забезпечується участю у стандартах і спільних механізмах реагування. Для України це означає не лише імплементацію європейського та євроатлантичного доробку (Загальний

регламент про захист даних GDPR 2016 р., NIS2, базові вимоги Організації Північноатлантичного договору НАТО до стійкості), а й активне експортне використання спроможностей — від участі у навчаннях типу Locked Shields до внеску у спільні аналітичні продукти центрів передового досвіду. Інтеграція до транснаціональних каналів обміну індикаторами компрометації, правова сумісність із режимами електронних доказів, узгоджені протоколи кризових комунікацій, відтак, є практичними елементами, що роблять даний процес не декларованою, а дієвою.

У підсумку національна цифрова стійкість може бути розглянута як операційна філософія держави та суспільства, що визнає складність, приймає невизначеність і конструює управління навколо здатності витримувати удари, швидко відновлюватися і навчатися ефективному реагуванню на інформаційні та технологічні подразники. Саме тому, цей підхід пропонується як основний у контексті даного підпункту: він з'єднує державні, громадські та міжнародні зусилля в єдину логіку, перетворює «мости» між секторами на «контури», що працюють постійно, а не лише в момент кризи, і створює методологічний фундамент, на якому у п. 5.3 Розділу V даного дисертаційного дослідження буде розгорнуто авторську концепцію розвитку механізмів інформаційної безпеки України. Така концепція спиратиметься на викладені вище принципи: інтегроване управління ризиком, багатоконтурну архітектуру захисту, економіку безпеки, інституціалізовану участь громадянського суспільства та міжнародну інтероперабельність. Лише у цій рамці розрізнені політики, на наше персональне бачення, набувають системної сили, а інформаційна безпека перестає бути відокремленою сферою та галуззю, стаючи властивістю державного управління та суспільного життя в цілому.

5.3. Формування концепції розвитку механізмів інформаційної безпеки держави

Сучасні реалії воєнної агресії проти України, гібридних впливів та багатовимірних інформаційно-психологічних операцій зумовлюють нагальну потребу вдосконалення системи інформаційної безпеки та механізмів її забезпечення. Наявна архітектура, хоча й зазнала суттєвої еволюції після 2014 р. (початок гібридної війни рф проти України) та особливо – 2022 р. (повномасштабне вторгнення рф до України), все ще характеризується фрагментарністю, нерівномірністю розвитку складових, браком єдиної координаційної рамки та системності у взаємодії між державними органами, приватним сектором і громадянським суспільством. Означене, відповідно, знижує ефективність протидії як зовнішнім загрозам, так і внутрішнім ризикам, зокрема поширенню дезінформації, кібератак, кризам довіри до державних інституцій.

У цьому контексті, пропонується авторська концепція розвитку механізмів інформаційної безпеки України, яка ґрунтується на ідеї інтегральної трирівневої моделі (стратегічний, тактичний та операційний рівні), поєднаній із принципами проактивності, багаторівневої координації, гнучкості та демократичного контролю. Ключова новизна концепції полягає у вибудовуванні синергії державного управління, приватного сектору та громадянського суспільства, що дозволяє сформувати цілісну, стійку та адаптивну систему інформаційної безпеки. Надалі розпочнемо її багатовекторний огляд.

Вихідним підґрунтям для побудови цілісної системи інформаційної безпеки України слугує чинна Доктрина інформаційної безпеки України 2016 р., затверджена Указом Президента України № 47/2017 від 29.12.2016 р. (поточна ред. від 30.12.2021 р.), яка визначає базові цілі та напрями державної політики у цій сфері. Водночас реалії повномасштабної агресії проти України,

стрімка динаміка розвитку інформаційних технологій та гібридних загроз виявили, що закладені у зазначеному документі положення потребують модернізації та конкретизації у частині інституційної взаємодії, інструментального забезпечення й інтеграції зусиль держави, приватного сектору і суспільства. Таким чином, необхідним кроком є розроблення концептуально нової моделі, що враховує попередні напрацювання, проте виходить за межі їх рамковості та пропонує операціоналізовану архітектуру інформаційної безпеки.

Авторська концепція, натомість, передбачає впровадження інтегральної трирівневої моделі реалізації інформаційної безпеки, що охоплює стратегічний, тактичний та операційний рівні.

Стратегічний рівень визначає базові принципи, пріоритети й цілі державної політики у сфері інформаційної безпеки. Тут формується єдина візія інформаційної стійкості України, забезпечується демократичний контроль, координація діяльності всіх суб'єктів та інтеграція із загальною системою національної безпеки.

Тактичний рівень забезпечує узгодженість між стратегією і практичною реалізацією через інституційні механізми: міжвідомчу координацію, секторальні плани дій, адаптивне регулювання та створення спільних ситуаційних центрів.

Операційний рівень охоплює конкретні інструменти протидії загрозам і швидкого реагування: системи моніторингу, реагування на інциденти, комунікаційні протоколи кризового менеджменту, а також заходи з формування безпекової культури серед користувачів та управлінців.

На відміну від наявних документів, інтегральна трирівнева модель не обмежується декларативними завданнями, а встановлює чітку логіку взаємозв'язку між рівнями, що дозволяє мінімізувати прогалини між стратегічними орієнтирами і практикою реалізації. Її новизна полягає у побудові системи синергії, де державне управління, приватний сектор та

громадянське суспільство взаємодіють як рівноправні суб’єкти єдиного простору інформаційної безпеки (Стратегія-модель «національної цифрової стійкості»).

Запропонована Стратегія-модель національної цифрової стійкості України спирається на чотири ключові принципи, які формують методологічний каркас побудови сучасної та дієвої системи інформаційної безпеки. Останні функціонують в режимі взаємного доповнення один одного, утворюючи інтегральну парадигму без реалізаційної ізоляції, у якій стратегічні орієнтири поєднуються з тактичною адаптивністю та операційною ефективністю. До них належить принцип проактивності, принцип багаторівневої координації, принцип гнучкості та принцип демократичного контролю. Розглянемо кожен із них більш детально нижче.

Концептуально, передумови для формування такої моделі обумовлені не лише технічними чи нормативними аспектами, а й глибокими соціокультурними, організаційними та когнітивними факторами, які визначають функціонування інформаційного простору як цілісної системи. Інформаційна безпека у такому контексті постає не як набір ізольованих процедур чи технологій, а як комплексна екосистема, у якій взаємодіють різні рівні управління, соціальні інститути, технологічні платформи та культурні практики населення. Важливим аспектом є усвідомлення того, що кожна зміна у технічних чи нормативних параметрах системи може мати каскадний ефект на рівні поведінки користувачів, структури потоків інформації та інституційних взаємозв’язків.

Крім того, будь-яка сучасна концепція інформаційної безпеки повинна враховувати мультифакторну динаміку загроз, яка включає технологічні, організаційні, психосоціальні та геополітичні компоненти. Це означає, що стратегічне планування має здійснюватися з урахуванням непередбачуваності цифрового середовища, високої швидкості розвитку технологій, постійної зміни векторів загроз та взаємозалежності національних систем з глобальним

інформаційним простором. Такі підходи дозволяють формувати більш стійкі та адаптивні моделі, які не обмежуються локальним аналізом ризиків, а інтегрують перспективу системного впливу та сценарного прогнозування.

Важливою складовою є також концептуальна інтеграція людського чинника. Люди у системі інформаційної безпеки виступають не лише кінцевими користувачами чи суб'єктами ризику, а й активними учасниками, здатними впливати на ефективність заходів, процесів та стратегій. З огляду на це, будь-яка модель цифрової стійкості має враховувати соціальну поведінку, рівень медіаграмотності, когнітивні обмеження та потенціал громадянського суспільства у протидії інформаційним загрозам. Лише така комплексна орієнтація дозволяє сформувати багаторівневу систему, у якій технічні, організаційні та соціальні елементи функціонують у взаємозв'язку.

Не менш значущим є аспект культурної та стратегічної адаптивності. Інформаційна безпека в сучасних умовах не може бути статичною; вона повинна передбачати можливість швидкого переналаштування на нові загрози, технологічні зміни, міжнародні стандарти та сценарії кризових ситуацій. Це передбачає формування процедур гнучкого реагування, постійного моніторингу та оцінки ефективності політик, що в сукупності створює ефект безперервного вдосконалення та підвищення резилієнтності системи.

Таким чином, концептуальна межа між визначенням ключових принципів Стратегії та їхнім подальшим детальним аналізом полягає у формуванні розуміння інформаційної безпеки як інтегрованої, багатовимірної, динамічної та соціально-технологічно обумовленої системи. Вона охоплює технічні засоби, організаційні структури, нормативне поле та поведінкові моделі учасників, забезпечуючи підґрунтя для реалізації принципів проактивності, багаторівневої координації, гнучкості та демократичного контролю. Саме таке ширше розуміння дозволяє створювати політики та моделі, здатні ефективно протидіяти сучасним кібер- та інформаційним загрозам, а також інтегруватися у міжнародний контекст цифрової безпеки.

Почнемо з того, що в сучасному інформаційному середовищі класичний підхід, що орієнтується виключно на реагування на вже здійснені загрози, виявився недостатнім. Врахоуючи, що сучасні кібер- та інформаційні атаки мають багаторівневий характер, застосовують приховані механізми впливу та ґрунтуються на використанні вразливостей людського фактору, інфраструктурних слабкостей або ж політичних і соціальних криз. Саме принцип проактивності стає основою побудови ефективної моделі цифрової стійкості.

Проактивність передбачає дії держави на випередження, від ідентифікації нових типів загроз до створення інституційних і технологічних механізмів їхнього попередження ще до того, як вони набудуть руйнівного ефекту. Йдеться про розвиток механізмів горизонтальної (багатовекторної) перевірки, аналізу даних та штучного інтелекту, що дозволяють виявляти тенденції і прогнозувати можливі сценарії атак, що, у свою чергу, потребує формування національної школи прогнозної аналітики у сфері інформаційної безпеки, яка здатна інтегруватися з європейськими та трансатлантичними підходами.

Важливою складовою проактивності як складника Стратегії-моделі національної цифрової стійкості України є формування «культури безпеки» у суспільстві: системної медіаосвіти, підвищення рівня цифрової грамотності, розвитку компетенцій критичного мислення. Без цього технологічні інструменти проактивності залишаються обмеженими, оскільки кінцевим бар’єром перед дезінформацією та маніпуляціями виступає виключно індивід Таким чином, проактивність набуває подвійного виміру: технологічного (моніторинг, аналітика, превентивне блокування загроз) і соціального (зміцнення резистентності громадян), предметом реалізації котрого є безпосередньо інформаційна галузь та інформаційна безпека.

Водночас, проактивність не може бути ефективною без чіткої системи управління, а саме багаторівневої координації. В умовах складного інформаційного середовища відмічаємо неможливість забезпечення стійкості

виключно за допомогою централізованих механізмів. Український досвід протидії гібридній та повномасштабній військовій та інформаційній агресії рф проти України, водночас, демонструє, що надмірна вертикалізація управління може призводити до надмірних затримок у прийнятті рішень, тоді як локальні інциденти потребують негайної реакції на рівні окремих інституцій або навіть окремих секторів.

Принцип багаторівневої координації передбачає узгодженість між стратегічним рівнем (державна політика, національні пріоритети), тактичним рівнем (секторальні стратегії, міжвідомча взаємодія) та операційним рівнем (конкретні інструменти реагування). У результаті можемо говорити про формування системи, де стратегічні цілі трансформуються у тактичні завдання та операційні дії без втрати швидкості, прозорості та ефективності.

Особливого значення в даному випадку набуває горизонтальна координація: взаємодія між державними структурами, приватним сектором, академічними установами і громадянським суспільством. Це дозволяє створювати спільні ситуаційні картини, формувати уніфіковані бази даних про загрози та забезпечувати взаємне інформування у режимі реального часу. Такі підходи вже довели ефективність у Європейському Союзі (ЄС), де діють моделі взаємодії ENISA, CERT-EU та національних центрів кібербезпеки, що вбачаємо доцільним до упровадження і в рамках України за допомогою запропонованої нами Стратегія-модель національної цифрової стійкості.

Для України, на додаток, важливо побудувати власну модель багаторівневої координації, яка поєднує централізоване стратегічне керівництво з гнучким децентралізованим виконанням з метою уникнення дублювання функцій, розпорошення ресурсів і водночас гарантувати швидкість реагування. Саме тут доцільно говорити про принцип гнучкості як складову інтегративну частину Стратегії-моделі національної цифрової стійкості України.

Концептуалізацію такої апропріації розпочинаємо з того, що стійкість

інформаційної системи передбачає здатність адаптуватися до змін зовнішнього середовища, технологічних новацій та еволюції загроз. Гнучкість передбачає не лише технічну модернізацію інфраструктури, а й інституційну спроможність швидко переглядати політики, протоколи і регламенти.

Гнучка система інформаційної безпеки не розглядає нормативну базу як закостенілу структуру, а формує її як адаптивну платформу. Зазначене передбачає перехід від традиційного «каскадного» регулювання до циклу безперервного вдосконалення, де кожен інцидент стає підставою для корекції норм і процедур. Тут-таки говоримо про необхідність приведення у євроатлантичну формацію таких актів законодавства, як Закон України «Про основні засади забезпечення кібербезпеки України» № 2163-VIII, Закон України «Про електронні комунікації» № 1089-IX, Стратегія кібербезпеки України від 2021 р. та Закон України «Про захист персональних даних» № 2297-VI. Більш детально пропоновані нами видозміни даної нормативної бази будуть розглянуті в концептуально-принциповій складовій п. 5.3 Розділу V даного дисертаційного дослідження.

Додамо, що гнучкість також означає технологічну диверсифікацію: мінімізацію «єдиних точок відмови», впровадження нульової довіри, багаторівневого резервування і сегментації мереж. Важливо, щоб у цій сфері Україна орієнтувалася на міжнародні стандарти (ISO, ENISA guidelines), адаптуючи їх до власних реалій.

Окремим аспектом гнучкості є кадрова політика, де в умовах дефіциту спеціалістів критично важливим стає запровадження механізмів постійного навчання, перепідготовки та залучення фахівців з приватного сектору і наукових установ до державних проектів у сфері інформаційної безпеки.

Водночас, потужна динаміка загроз у цифровому середовищі часто створює спокусу для держави вдаватися до надмірної централізації, що може загрожувати правам і свободам людини. Саме тому ключовим принципом побудови Стратегії-моделі національної цифрової стійкост України ми

визначаємо демократичний контроль.

Даний принцип передбачає прозорість формування політик, наявність механізмів громадського нагляду та парламентського контролю, а також дотримання міжнародних стандартів прав людини у сфері інформаційної безпеки. Він включає в себе формальні інститути та предметно-практичну практику залучення громадянського суспільства до розробки і моніторингу стратегій, а також про створення відкритих каналів комунікації між державою і громадянами.

На наш погляд, саме демократичний контроль повинен виконувати функцію запобіжника проти надмірної секретизації. Застосовність останнього також може бути корисною в ситуаціях, коли інформаційна безпека може ставати прикриттям для обмеження політичної конкуренції або свободи слова, що дозволить забезпечити баланс між безпекою та демократією, котра є невід'ємним складником євроатлантичного вибору та вітчизняного євроінтеграційного поступу.

Для України, яка перебуває у стані героїчного відбиття військової агресії рф, описаний принцип є особливо чутливим, адже захист від інформаційної агресії не підлягає трансформації у внутрішні обмеження демократичного розвитку, через що важливо закласти у модель цифрової стійкості механізми регулярної оцінки впливу політик безпеки на права громадян, що відповідатиме європейській практиці оцінки впливу (impact assessment), про що, власне, ми і зазначали вище.

Таким чином, проактивність, багаторівнева координація, гнучкість і демократичний контроль є джерелом ґенерації чотирибічний фундамент Стратегії-моделі національної цифрової стійкості України. Їхнє поєднання дозволить перейти від фрагментарних заходів до системного підходу, що одночасно забезпечує ефективність, адаптивність та відповідність демократичним стандартам.

Після визначення концептуальних принципів Стратегії-моделі

національної цифрової стійкості України, на наш погляд, наступним кроком є розгляд інструментів реалізації цієї моделі. Останні де-факто є механізмами, які перетворюють принципи на практичні дії, забезпечують координацію на всіх рівнях та дозволяють державі швидко адаптуватися до змін у кіберсередовищі. Виходячи з попереднього акценту на проактивність, багаторівневу координацію, гнучкість та демократичний контроль, пропонується виділити три основні інструменти: Єдиний національний центр стратегічних комунікацій (ЄНЦСК), адаптивну нормативну базу та системи швидкого реагування. Кожен із них забезпечує конкретні функції, але в сукупності формує інтегровану, ефективну систему інформаційної безпеки, яка здатна протидіяти гібридним загрозам та підтримувати цифрову стійкість держави.

Так, нами ропонується створення Єдиного національного центру стратегічних комунікацій (ЄНЦСК) як ключової інституції, що координує інформаційні потоки, забезпечує синхронізацію дій державних органів, приватного сектору та громадянського суспільства, а також формує стратегічні комунікації під час кризових ситуацій.

З метою виконання поставлених завдань та цілей, що визначені вище, ЄНЦСК повинен виконувати такі функції, як : 1) моніторинг та аналіз загроз — збір оперативної інформації про кібератаки, спроби дезінформації, вразливості державних та приватних систем; 2) координація міжрівневих дій — забезпечення горизонтальної взаємодії між міністерствами, відомствами, приватними операторами та центрами передового досвіду; 3) стратегічні комунікації та просвітницькі програми — трансляція достовірної інформації у суспільство, організація тренінгів для медіа, освітніх установ та громадян; 4) аналітична підтримка прийняття рішень — розробка сценаріїв реагування та рекомендацій для органів влади.

Подібна структура, за прикладом центру Агентства з кібербезпеки та безпеки інфраструктури (CISA) в США або Європейського агентства з кібербезпеки (ENISA) у Європейському Союзі (ЄС), дозволяє забезпечити

уніфіковану платформу обміну інформацією, зменшити дублювання функцій і підвищити швидкість реакції на інциденти. В реаліях України, наприклад, ЄНЦСК може інтегруватися з існуючими координаційними органами, такими як Служба безпеки України (СБУ), Рада національної безпеки і оборони України (РНБО) та Міністерство цифрвоої трансформації України (Мінцифра), формуючи єдину ситуаційну картину загроз.

Другим важливим інструментом є адаптивна нормативна база, що дозволить Україні належним чином реагувати на нові виклики без необхідності тривалого процедурного оновлення законодавства. Гнучка нормативна платформа будується на принципах циклу безперервного вдосконалення, де кожен інцидент стає підставою для внесення змін та доповнень у законодавчі та підзаконні акти.

У межах запропонованої моделі ми вбачаємо за доцільне висловити такі пропозиції, які при цьому мають бути розподілені на два кластери – пропозиції щодо змін до законодавчих актів України та пропозиції щодо нових стратегій національної кібер- та інформаційної безпеки. Розпочнемо із пропозиції щодо змін до законодавчих актів України :

1) до Закону України «Про основні засади забезпечення кібербезпеки України» № 2163-VIII вбачаємо за доцільне додати статтю про обов’язкове щоквартальне оновлення національних сценаріїв реагування на гібридні загрози, що інтегрує державні та приватні джерела інформації;

2) вважаємо за необхідне внести зміни до ст. 8 щодо формування спільних міжвідомчих аналітичних груп як частини електронної регуляторної платформи (для актуалізації процедур та забезпечення інформаційної безпеки) Закону України «Про електронні комунікації» № 1089-IX;

3) пропонуємо запровадити в даному нормативно-правовому акті пункт про обов’язкову перевірку і адаптацію процедур сегментації мереж та практик zero trust щорічно;

4) ввжаємо апропріативним додати норму про гнучке погодження

каналів передачі інформації між державними органами та приватними операторами;

5) до Закону України «Про захист персональних даних» № 2297-VI доцільно додати статтю про оперативне узгодження процедур обміну даними між державними структурами та приватними партнерами у випадку надзвичайних кіберінцидентів, з дотриманням міжнародних стандартів Загального регламенту про захист персональних даних GDPR 2016 р.

Водночас, у контексті положень пропозиції щодо нових стратегій національної кібер- та інформаційної безпеки пропонуємо, своєю чергою, такі видозміни :

6) впровадити щорічний цикл адаптивного планування інцидентів, де кожен інцидент аналізується, і до програми забезпечення інформаційної респонсивності та стабільності держави додаються нові механізми реагування (доцільно в контексті Стратегії кібербезпеки України від 2021 р.

7) до положень Стратегії кібербезпеки України від 2021 р. рекомендуємо включити розділ про інтеграцію громадянського суспільства у процеси превентивного моніторингу та фактчекінгу, що забезпечує гнучке реагування на інформаційні загрози;

8) розробити та схвалити нову Стратегію кібербезпеки України та Стратегію інформаційної безпеки з урахуванням воєнних викликів та загроз, спираючись на нові підходи стратегічного планування на державному рівні, інтегральність та взаємоузгодженість стратегічних цілей та показників їх виконання, визначених у Концепції національної системи стратегічного планування, схваленій розпорядженням КМУ від 13 серпня 2025 р. № 853-р.

Ми вважаємо, що такі зміни дозволять трансформувати нормативну базу України у галузі забезпечення інформаційної безпеки в динамічний інструмент, що одночасно гарантує правові підстави для дій держави і забезпечує гнучкість для адаптації до нових технологій та гібридних загроз.

Третім інструментом, як ми зазначали раніше, є системи швидкого

реагування, що здатні забезпечити оперативне локалізування інцидентів, координацію між учасниками та мінімізацію негативних наслідків. Для України доцільно створити:

а) Національний центр кіберреагування (НЦКР) – як підрозділ ЄНЦСК, який забезпечує 24/7 моніторинг загроз, аналіз інцидентів та координацію оперативного реагування;

б) мобільні оперативні групи у складі представників державних органів, приватного сектору та громадських експертів, які здатні в короткі строки локалізувати кібератаки;

в) Єдину платформу обміну загрозовими індикаторами (threat intelligence), що дозволяє реалізувати автоматизоване реагування на типові атаки і формувати рекомендації для приватного та державного секторів;

г) симуляційні навчання та тренування на базі міжнародних практик, таких як Locked Shields, про які ми уже зауважували за текстом п. 5.4 Розділу V дисертаційного дослідження та EU Cyber Exercises, що підвищують готовність українських органів реагування.

Поєднання таких інструментів, як ЄНЦСК, адаптивна нормативна база та системи швидкого реагування, відтак, створює інтегровану модель управління інформаційною безпекою, здатну ефективно протидіяти гібридним загрозам, підтримувати цифрову стійкість та забезпечувати синергію між державою, приватним сектором і громадянським суспільством.

Важливою складовою авторської розробки є представлення Стратегії-моделі національної цифрової стійкості України у візуалізованому вигляді. Якщо концептуальні принципи та інструменти реалізації відображають методологічні й організаційні аспекти забезпечення інформаційної безпеки, то у даному випадку ключовим акцентом стає інтеграція суб’єктів у єдину функціональну систему. Авторська новизна моделі полягає у відмові від традиційного трактування публічного управління як ізольованого чи домінуючого кластера. Натомість пропонується розглядати його як динамічний

компонент, вбудований у взаємодію з приватним сектором та громадянським суспільством. Такий підхід дозволяє зробити реагування не лише адміністративно-законодавчим, а й більш стрес-практичним, орієнтованим на швидку апробацію нових методів, їх гнучку адаптацію та інтеграцію у функціональні процеси держави.

Особливе місце у цій системі посідає громадянське суспільство, яке в даній моделі не лише відіграє допоміжну чи суто контрольну роль, а виступає інтегратором змін та реалізатором суспільного волевиявлення. Це відображає сучасні тенденції у сфері інформаційної безпеки, де питання не обмежуються технічним захистом мереж чи цифровою грамотністю населення. Значну вагу мають також проактивність громадян, участь у процесах раннього виявлення загроз, фактчекінгу та поширення достовірної інформації, що створює додатковий шар захисту від дезінформаційних кампаній і гібридних атак. У результаті виникає трикутник взаємодії «держава — бізнес — громадянське суспільство», де жодна ланка не є самодостатньою, а ефективність формується виключно завдяки їх синергії.

Таким чином, у розробленій авторській моделі цифрова стійкість постає не як статична конструкція, а як динамічна екосистема, здатна реагувати на зовнішні виклики комплексно і гнучко. Вона поєднує в собі формальні механізми управління, підприємницьку інноваційність і суспільну активність. Варто також додати, що, із урахуванням сучасного підходу до зменшення кількості стратегічних документів та інтеграції управлінських процесів, реалізація положень з інформаційної та кібербезпеки пропонується здійснювати також якраз-таки через існуючу Стратегію-модель національної цифрової стійкості України, про яку говорили вище і положення щодо якої будуть, відповідно, підсумовані нижче. Кібербезпека в ній розглядається як складова інформаційної безпеки, що забезпечує комплексний підхід до захисту інформаційного середовища та реагування на гібридні загрози, а також гарантує узгодженість стратегічних цілей та показників виконання

Усе відображене у Розділі V дисертації представляємо рисунок 5.1, де зображена Стратегія-модель національної цифрової стійкості України.

У контексті дисертаційного дослідження, використання поняття «Стратегія-модель» є обґрунтованим, оскільки воно поєднує два взаємодоповнювальні виміри – з одного боку, пропонований підхід має стратегічний характер, адже передбачає формування цільової візії, пріоритетів та принципів довгострокового розвитку системи публічного управління у сфері інформаційної та цифрової безпеки, з іншого – модельний аспект дозволяє представити цю структуру у вигляді операційно-функціональної архітектури, яка описує конкретні механізми, інституційні ролі, логіку управлінських процесів і взаємодію між суб'єктами забезпечення безпеки. Таким чином, «стратегія-модель» підкреслює інтегративний характер підходу, у межах якого стратегічні цілі набувають практичної реалізації через конкретизовану функціональну модель.

Водночас, запропонована Стратегія-модель не обмежується суто інформаційною безпекою, оскільки феномен цифрової стійкості є ширшим за своїм змістом. Цифрова стійкість включає здатність держави, суспільства та інституцій функціонувати, адаптуватися та відновлюватися в умовах комплексних цифрових, інформаційних, кібернетичних, технологічних і соціальних викликів. Інформаційна безпека становить один із ключових, проте не єдиний її компонент. До сфери цифрової стійкості належать також питання кіберзахисту критичної інфраструктури, управління даними, технологічної сумісності, регулювання цифрових платформ, розвитку цифрових компетентностей та взаємодії держави з приватним сектором. Саме тому застосування ширшої категорії «національна цифрова стійкість» є методологічно виправданим і дозволяє інтегрувати інформаційну безпеку в комплексну систему публічного управління цифровими ризиками.

Отже, кореляційні риси запропонованої Стратегії-моделі національної цифрової стійкості України полягають у її комплексності та інтегративності. На

відміну від традиційних моделей інформаційної безпеки, що концентруються переважно на технічних чи правових аспектах, ця модель забезпечує синергію між державним управлінням, приватним сектором та громадянським суспільством.

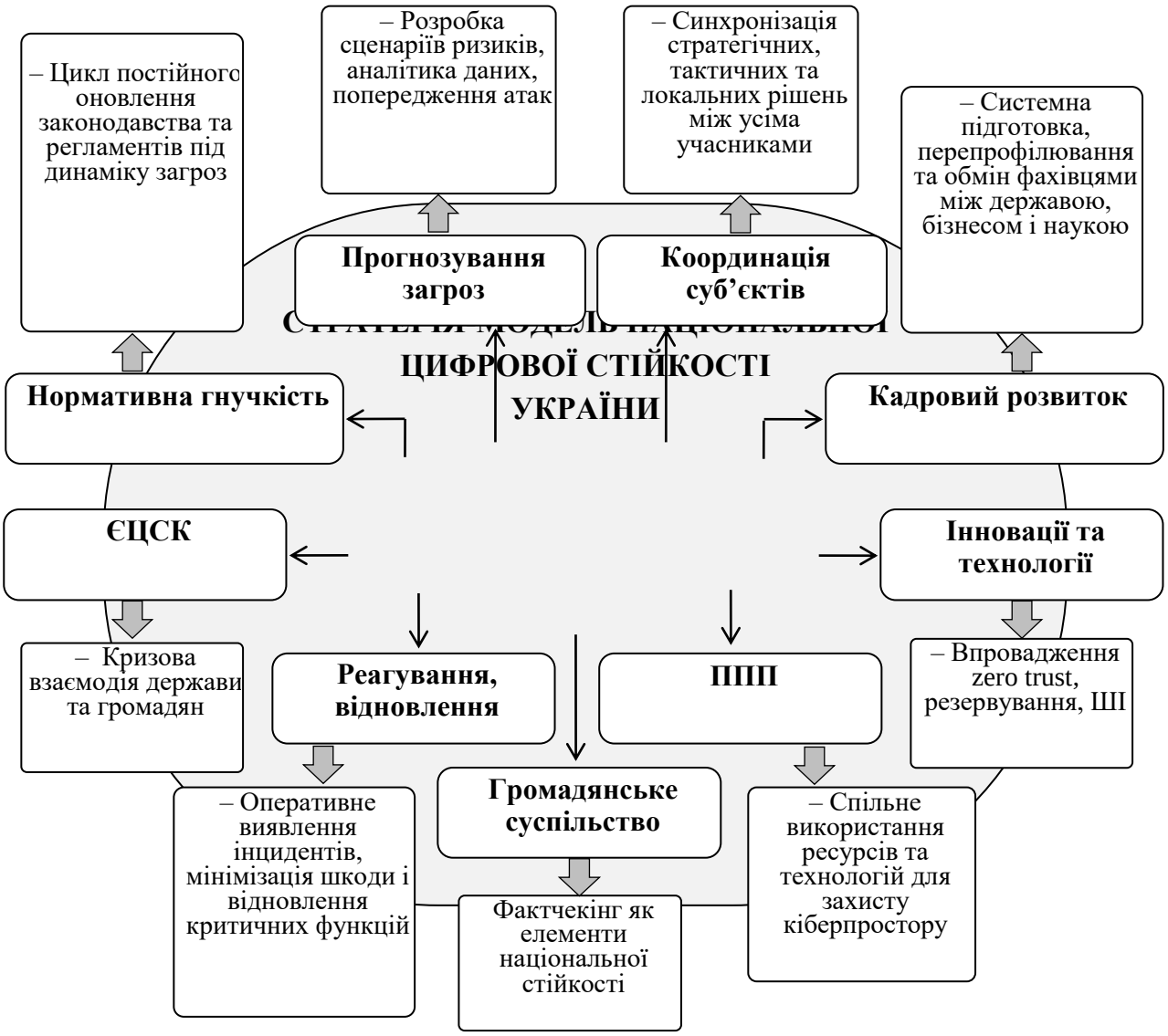

Рисунок 5.1. Стратегія-модель національної цифрової стійкості України.

У ширшому розумінні, комплексний підхід передбачає, що кожен елемент моделі не існує ізольовано, а постійно взаємодіє із рештою структурних компонентів, формуючи динамічний механізм реагування на сучасні виклики цифрової епохи.

Важливим аспектом цієї парадигми є здатність до саморегуляції та самоаналізу: система постійно оцінює ефективність своїх стратегічних орієнтирів, тактичних рішень та операційних дій, виявляючи слабкі місця та забезпечуючи їх корекцію без втрати загальної узгодженості.

Також, слід підкреслити, що інтегративність моделі означає не лише взаємодію різних суб'єктів інформаційного простору, а й поєднання різнорівневих ресурсів, технологій та знань. Вона враховує людський фактор, культурний та освітній контекст, інноваційний потенціал приватного сектору, науково-дослідний компонент, а також існуючі та потенційні ризики національного та міжнародного масштабу. У цьому сенсі модель функціонує як органічна система, де кожен рівень інформаційного забезпечення підпорядковується спільним цілям, але водночас зберігає автономію у прийнятті рішень відповідно до специфіки свого функціонування.

Додатково, багаторівнева координація в моделі створює основу для оперативного обміну інформацією, швидкого виявлення та нейтралізації загроз, а також гнучкого розподілу ресурсів відповідно до поточних пріоритетів. Цей підхід дозволяє уникати вузького фокусування на окремих аспектах безпеки, забезпечуючи збалансованість між превентивними заходами, реагуванням на кризові ситуації та довгостроковим плануванням. Водночас система передбачає механізми контролю, моніторингу та оцінки ефективності кожного рівня, що підсилює її стійкість і дозволяє формувати адаптивні стратегії в умовах високої змінності цифрового середовища та потенційної невизначеності міжнародної безпекової ситуації.

У контексті сучасних викликів, таких як кіберзагрози, інформаційні атаки, дезінформаційні кампанії, а також технологічні інновації, ця стратегічно інтегровані модель стає своєрідним «щитом», здатним забезпечити стійкість держави та суспільства. Вона створює умови для прогнозування і нейтралізації ризиків, координації спільних дій у масштабах усієї країни та підтримки взаємної довіри між державними органами, приватним сектором та

громадянським суспільством. Такий підхід дозволяє не лише реагувати на сучасні загрози, а й активно формувати інформаційне середовище, яке відповідає принципам національної безпеки, демократичного контролю та технологічної ефективності.

Таким чином, запропонована Стратегія-модель не є статичною конструкцією, а виступає як динамічна і системна рамка, що забезпечує синхронізацію між стратегічними орієнтирами, тактичними завданнями та оперативними діями, інтегруючи різні рівні та суб'єкти у процес формування стійкої, надійної та ефективної системи інформаційної безпеки держави.

Водночас, слід зазначити, що комплексний характер запропонованої Стратегії-моделі національної цифрової стійкості України дозволяє розглядати її не лише як практичний інструмент забезпечення безпеки, а й як концептуальну основу формування нового підходу до державного управління в умовах високої технологічної динаміки. Такий підхід передбачає, що кожен рівень моделі – стратегічний, тактичний і операційний – функціонує у постійному діалозі із іншими рівнями, забезпечуючи безперервний обмін інформацією, аналіз загроз та адаптацію до змін у зовнішньому та внутрішньому середовищі. Саме інтеграція цих рівнів створює ефект синергії, який дозволяє підвищити ефективність реагування на загрози та забезпечити гнучкість системи у випадку появи нових технологічних або соціальних викликів.

Особливо важливою є роль багаторівневої координації у контексті взаємодії різних суб'єктів інформаційної екосистеми. Вона передбачає не лише узгодження дій між державними органами, а й інтеграцію з приватним сектором, науковими установами та громадянським суспільством, що у свою чергу формує багатокомпонентну мережу реагування. У такій системі кожен елемент отримує можливість не тільки виконувати свою функцію, а й впливати на процес ухвалення рішень на інших рівнях, створюючи динамічний та адаптивний механізм, здатний до самонавчання та самоорганізації. Цей аспект

набуває особливої ваги у сучасному світі, де інформаційні загрози мають транснаціональний характер, а швидкість їхнього поширення перевищує можливості традиційних моделей централізованого управління.

Крім того, інтегративна модель дозволяє усвідомити взаємозалежність між різними сферами безпеки: технічною, правовою, соціальною та культурною. Вона формує умови для того, щоб технологічні рішення не розглядалися ізольовано від нормативної бази, освітніх програм і соціального контексту. Такий підхід сприяє усвідомленню того, що інформаційна безпека є не лише питанням технічного забезпечення, а й складовою загальної стратегії державної політики, яка включає розвиток медіаграмотності громадян, підтримку критичного мислення, формування довіри до державних інститутів та створення культурного середовища, сприятливого для протидії дезінформації та кіберзагрозам.

Додатково, концептуальний характер моделі передбачає постійне прогнозування потенційних сценаріїв розвитку цифрового середовища та загроз, які виникають унаслідок інновацій у сфері інформаційно-комунікаційних технологій, штучного інтелекту та інтернету речей. Стратегія передбачає не лише реагування на існуючі ризики, а й формування превентивних заходів, що дозволяють зменшити ймовірність негативного впливу на національні інтереси. У цьому сенсі модель виступає як гнучкий та адаптивний каркас, який здатний підтримувати рівновагу між потребами держави, приватного сектору та громадянського суспільства.

Не менш важливим аспектом є те, що комплексність моделі створює можливості для формування універсальних механізмів контролю та оцінки ефективності всіх компонентів системи. Такий контроль здійснюється як на стратегічному рівні, визначаючи довгострокові цілі та пріоритети, так і на тактичному та операційному рівнях, де відбувається щоденне управління ресурсами, аналіз загроз та оперативне реагування. Водночас інтеграція принципу демократичного контролю забезпечує прозорість процесів та

підзвітність дій усіх учасників інформаційного середовища, що формує додатковий рівень стійкості та надійності системи.

У ширшому плані, запропонована стратегія-модель відображає сучасний підхід до концептуалізації інформаційної безпеки як динамічного процесу, який поєднує інноваційні технології, правові механізми, соціальні інститути та міжнародні стандарти. Вона демонструє, що побудова національної цифрової стійкості неможлива без комплексного розуміння взаємодії всіх учасників інформаційного простору та без постійного вдосконалення методологічних, організаційних і технологічних інструментів для забезпечення безпеки у мінливих умовах цифрового середовища.

Таким чином, модель виступає не просто як набір правил або рекомендацій, а як концептуальна платформа, здатна поєднувати довгострокову стратегію із поточними оперативними рішеннями, підтримуючи інтеграцію державних, приватних та громадських ресурсів у єдину, скоординовану і високоефективну систему національної цифрової стійкості.

Варто відзначити, що багатокомпонентність запропонованої Стратегії-моделі національної цифрової стійкості створює унікальні умови для всебічного розуміння сучасного підходу до інформаційної безпеки, у якому технологічні, організаційні, соціальні та правові аспекти не розглядаються окремо, а постійно перебувають у взаємодії. Такий підхід дозволяє трансформувати інформаційне середовище держави із статичного набору процедур у динамічну систему, здатну до адаптації, самонавчання та гнучкого реагування на загрози різного рівня та типу. Підкреслюється, що будь-яка інша модель, яка обмежується виключно технічними або нормативними рішеннями, не здатна забезпечити необхідний рівень системної стійкості, адже сучасні виклики інформаційного простору поєднують технологічні, соціальні та політичні компоненти, що впливають на поведінку індивіда, колективів та інституцій.

Важливою характеристикою моделі є її здатність інтегрувати різнорівневі

підходи до управління інформаційною безпекою, включно із стратегічним плануванням на рівні державних політик, тактичними рішеннями у межах окремих секторів та оперативним реагуванням на інциденти у реальному часі. Така багаторівнева структура створює не лише когерентність дій, а й відкриває можливості для безперервного аналізу ефективності системи, адаптації до нових технологічних і соціальних викликів та прогнозування потенційних ризиків. Це означає, що модель передбачає не лише ретроспективне оцінювання подій, а й активне формування сценаріїв розвитку цифрового середовища, що дозволяє зменшувати ймовірність негативного впливу на національні інтереси.

У межах інтегративного підходу особлива увага приділяється взаємодії між державним сектором, приватними компаніями та громадянським суспільством. Кожен із цих елементів інформаційної екосистеми виконує специфічні функції, які, проте, стають максимально ефективними лише у взаємодії та координації з іншими. Державні органи формують нормативно-правові рамки, встановлюють стандарти безпеки та здійснюють стратегічний моніторинг загроз. Приватний сектор, у свою чергу, надає технологічні ресурси, оперативні дані про інциденти та практичні інструменти для виявлення та запобігання загрозам. Громадянське суспільство забезпечує соціальну складову безпеки, поширюючи медіаграмотність, формуючи критичне мислення та контроль за дотриманням прав людини у цифровому просторі. Взаємодія цих компонентів не є статичною: вона постійно піддається адаптації залежно від змін у технологічному середовищі, загрозовій динаміці та соціокультурному контексті.

Особливої уваги заслуговує принцип гнучкості, який лежить в основі Стратегії-моделі. Гнучкість передбачає не лише можливість швидкої реакції на кіберінциденти, а й здатність системи змінювати пріоритети, розподіляти ресурси та коригувати методи управління у залежності від поточної ситуації. У сучасному світі, де цифрові технології та соціальні мережі швидко змінюють інформаційне середовище, гнучкість стає не абстрактною характеристикою, а

критичною умовою виживання та ефективності державних систем безпеки. Вона також дозволяє інтегрувати новітні технологічні досягнення, такі як штучний інтелект, великі дані, інтернет речей та аналітичні платформи прогнозування загроз, без створення надмірної бюрократичної складності.

Не менш важливою є роль принципу багаторівневої координації, який забезпечує синхронізацію стратегічного, тактичного та оперативного управління. Така координація передбачає створення чітких каналів комунікації, системи обміну інформацією у режимі реального часу та механізмів прийняття рішень, здатних забезпечити одночасне виконання завдань на різних рівнях управління. На практиці це означає, що стратегічні орієнтири формуються з урахуванням поточних операційних викликів, а оперативні дії базуються на аналітичних даних, зібраних у межах тактичних планів. Такий підхід створює ефект «живої системи», яка постійно адаптується до змін у зовнішньому середовищі та внутрішньому контексті, зменшуючи ймовірність виникнення критичних розривів у безпековому ланцюгу.

Принцип проактивності у рамках моделі виступає ключовим для створення системи, що не лише реагує на загрози, а й прогнозує їх появу та вплив. Проактивний підхід передбачає формування превентивних заходів, аналіз потенційних сценаріїв розвитку інформаційного простору та постійне оновлення стратегій реагування на підставі нових даних та технологічних тенденцій. Це дозволяє зменшити ймовірність критичних інцидентів і забезпечити більш стабільне та передбачуване функціонування національної цифрової екосистеми.

Не можна ігнорувати і принцип демократичного контролю, який гарантує прозорість дій усіх учасників системи та підзвітність прийнятих рішень. Демократичний контроль забезпечує баланс між безпекою та правами громадян, створює умови для участі суспільства у визначенні пріоритетів безпеки та підтримує довіру до державних інституцій. У сучасному цифровому середовищі, де інформаційні потоки миттєво поширюються у глобальному

масштабі, довіра громадян є критично важливою для ефективності будь-яких заходів, спрямованих на протидію дезінформації та кібератакам.

Крім того, важливою особливістю моделі є її здатність враховувати міжнародний вимір інформаційної безпеки. Глобалізація цифрового середовища створює нові виклики, пов'язані з уніфікацією стандартів, обміном технологічними практиками та забезпеченням сумісності систем між державами. Модель передбачає, що національна цифрова стійкість не може існувати ізольовано від міжнародних процесів, і тому інтеграція з глобальними стандартами та коаліціями стає невід'ємною складовою ефективного управління.

Синтез усіх вищезазначених елементів – гнучкості, багаторівневої координації, проактивності та демократичного контролю – формує унікальний каркас, здатний поєднувати стратегічні цілі держави з оперативними можливостями, технологічними інструментами та соціальною складовою. Такий комплексний підхід дозволяє створити не просто систему безпеки, а адаптивну екосистему, здатну протистояти гібридним загрозам, забезпечувати цифрову стійкість та підтримувати довгострокову національну безпеку у мінливих умовах сучасного інформаційного середовища.

Врешті-решт, запропонована Стратегія-модель виступає як концептуальна платформа, яка інтегрує технології, управлінські механізми та соціальні інститути у єдину скоординовану систему. Вона демонструє, що ефективна національна цифрова стійкість неможлива без поєднання стратегічного бачення, адаптивної організаційної структури та взаємодії всіх зацікавлених сторін – держави, приватного сектору та громадянського суспільства. Саме така інтеграція створює умови для стійкого розвитку інформаційної інфраструктури, підвищує здатність держави протидіяти новітнім кібернетичним та різного роду загрозам.

Також, новизну формує нормативна гнучкість, що трактує правові механізми не як статичні обмеження, а як адаптивні інструменти, здатні

змінюватися відповідно до появи нових викликів. У цій площині пропонується відхід від каскадного підходу до регулювання на користь циклу безперервного вдосконалення.

Додатковим виміром моделі є стрес-практична спрямованість, тобто пріоритет оперативного реагування, відновлення та навчання на пережитих інцидентах, що, на наш погляд, переводить акцент із суто захисної функції на формування активної, динамічної культури безпеки.

Таким чином, дана модель відрізняється від наявних аналогів тим, що розглядає інформаційну безпеку не лише як технологічний чи управлінський процес, а як живу систему цифрової стійкості, яка постійно еволюціонує завдяки взаємодії різних секторів суспільства.

Формування авторської концепції розвитку механізмів інформаційної безпеки держави в Україні дозволило нам дійти наступних умовиводів.

По-перше, сучасні виклики інформаційної безпеки в умовах гібридних загроз потребують переходу від фрагментарних підходів до єдиної інтегральної моделі, що охоплює стратегічний, тактичний та операційний рівні управління. Запропонована нами Стратегія-модель національної цифрової стійкості України враховує потребу у формуванні системи, здатної діяти превентивно, своєчасно реагувати на загрози та забезпечувати швидке відновлення критичних функцій. На відміну від наявних концепцій, вона виходить не з ідеї абсолютної захищеності, що практично недосяжна, а з принципу адаптивної стійкості, коли система навчається на кризових ситуаціях, удосконалюючи себе. Це відповідає новітнім міжнародним тенденціям, де «resilience» розглядається як ключ до ефективної інформаційної безпеки [411, 412].

По-друге, концептуальними засадами моделі виступають проактивність, багаторівнева координація, гнучкість та демократичний контроль, які у своїй сукупності забезпечують баланс між ефективністю управління та збереженням демократичних цінностей. Проактивність дозволяє прогнозувати й запобігати загрозам ще до їх прояву, що особливо актуально в умовах динамічної війни у

кіберпросторі. Багаторівнева координація створює основу для скоординованої взаємодії органів центральної влади, секторних агентств та регіональних структур. Гнучкість трактується як здатність нормативної бази адаптуватися до змінних реалій, що зумовлює необхідність регулярного перегляду законодавства та підзаконних актів з урахуванням досвіду інцидентів. Демократичний контроль забезпечує прозорість і підзвітність дій державних органів, а також сприяє довірі з боку суспільства та міжнародних партнерів, що є визначальним чинником ефективності будь-якої безпекової політики.

По-третє, реалізація цієї моделі передбачає використання конкретних інструментів, що підсилюють її практичний вимір. У першу чергу, йдеться про створення Єдиного національного центру стратегічних комунікацій, який виступатиме координаційним ядром у протидії дезінформації та в управлінні кризовими комунікаціями. Другою складовою є адаптивна нормативна база, що інтегрує зміни до ключових законів (Закон України «Про основні засади забезпечення кібербезпеки України» № 2163-VIII, Закон України «Про електронні комунікації» № 1089-IX, Стратегія кібербезпеки України від 2021 р. та Закон України «Про захист персональних даних» № 2297-VI) та урядових програм у напрямі гнучкого й циклічного вдосконалення. Третьою — створення систем швидкого реагування, які забезпечують технічну, організаційну та кадрову готовність до локалізації загроз у найкоротші терміни. Взаємодія цих елементів у межах єдиної стратегії формує підґрунтя для підвищення національної цифрової стійкості України.

По-четверте, авторська новизна нашої моделі полягає у синергії державного управління, приватного сектору і громадянського суспільства як рівноправних учасників системи інформаційної безпеки. Державне управління виступає ядром формування політики та координації, приватний сектор забезпечує технологічні рішення та інновації, а громадянське суспільство створює атмосферу проактивності, критичного мислення та довіри. Таке поєднання виходить за межі класичного публічно-приватного партнерства,

адже включає громадянські ініціативи як інтегратор змін, що закладає основу для довготривалої цифрової стійкості.

По-п’яте, впровадження даної моделі в Україні дозволяє узгодити національні інтереси з міжнародними стандартами, зокрема рамками Європейського Союзу (ЄС), Організації Північноатлантичного договору (НАТО) та Організації Об’єднаних Націй (ООН) у сфері інформаційної та кібербезпеки, що створює потенціал для не лише внутрішньої модернізації, але й посилення ролі України як активного суб’єкта у глобальних безпекових процесах. Водночас, модель враховує особливості українського контексту: наявність гібридної війни, значну роль суспільних ініціатив у протидії дезінформації, а також потребу в зміцненні довіри між державою та бізнесом.

Отже, розроблена нами Стратегія-модель національної цифрової стійкості України є не лише науковою пропозицією, але й практичною дорожньою картою для трансформації державної системи інформаційної безпеки. Вона поєднує адаптивність і структурованість, технологічність і гуманітарний вимір, міжнародні стандарти і національну специфіку. Її імплементація сприятиме формуванню не просто безпечного, а стійкого цифрового середовища, здатного витримати сучасні й майбутні виклики.

Висновки до розділу 5

1. Узагальнено та систематизовано сучасні виклики та тенденції розвитку механізмів інформаційної безпеки держави, що дозволило: класифікувати та поглибити аналіз сучасних інформаційних ризиків за трьома основними вимірами, акцентуючи на їхній взаємозалежності та кумулятивному ефекті (глобально-політичні ризики: розкрито як систему взаємопов'язаних загроз: гібридні війни (поєднання військових, кібернетичних та інформаційних засобів), дезінформація та інформаційна асиметрія (дисбаланс між швидкістю поширення та здатністю суспільства до критичного осмислення); технологічні

ризики: визначено штучний інтелект (ШІ) як інструмент подвійної дії (можливість для захисту vs. інструмент для автоматизованих фішингових схем), аналітику великих даних (Big Data) як джерело монополізації інформації та deepfake-технології як чинник «кризи достовірності»; соціально-комунікаційні ризики: доведено, що соціальні мережі та цифрові платформи є феноменом подвійної природи (канал демократизації та арена гібридних атак), а їхня алгоритмічна архітектура є каталізатором поляризації та поширення сенсаційного контенту, що вимагає регулювання не лише контенту, а й самих алгоритмічних процесів); обґрунтувати необхідність інтеграції нових підходів до зміцнення кіберстійкості суспільства та сформувати двопланову модель протидії ризикам (поведінковий/освітній вимір: акцентовано на інформаційній гігієні та медіаграмотності як базових елементах зменшення вразливості громадян (приклад Швеції та Фінляндії); інституційно-правовий вимір: систематизовано нові регуляторні механізми (зокрема, Digital Services Act (DSA) та Data Governance Act (DGA) ЄС), які створюють інституційну рамку для боротьби з дезінформацією та забезпечення прозорості алгоритмів, що є прикладом збалансованого регулювання).

2. Удосконалено теоретико-методологічні засади формування механізмів забезпечення інформаційної безпеки шляхом: систематизації та критичного аналізу трьох основних управлінських моделей (централізованої, децентралізованої та публічно-приватного партнерства) у контексті протидії гібридним загрозам, з виокремленням їхніх переваг і обмежень для України (централізована модель (США, Ізраїль): визначено як ефективну для швидкого реагування та уніфікації стандартів, але вказано на ризики бюрократизації та дублювання повноважень в українських умовах (СБУ, РНБО); децентралізована модель (Німеччина, Японія): обґрунтовано її переваги у гнучкості та врахуванні секторної специфіки (Мінцифра, НБУ, ДССЗЗІ), проте виявлено ключовий недолік — ризик розрізненості стандартів та низька узгодженість без належних координаційних механізмів; публічно-приватне партнерство (США – CISA,

Велика Британія – CiSP): обґрунтовано його як критично важливий механізм для оперативного обміну інформацією про загрози та інтеграції технологічної експертизи приватного сектору, що є необхідним для протидії сучасним інформаційним та кіберзагрозам).

3. Розроблено та науково обґрунтовано стратегію-модель національної цифрової стійкості України, яка є інтегральною трирівневою системою (стратегічний, тактичний та операційний рівні) та забезпечує синергію між державним управлінням, приватним сектором і громадянським суспільством у протидії гібридним загрозам, включає чотири ключові принципи (проактивність, багаторівнева координація, гнучкість, демократичний контроль), що формують методологічний каркас стратегії-моделі, забезпечуючи перехід від реактивного до прогнозно-превентивного управління інформаційною безпекою, та інституційно-інструментальне забезпечення (створення Єдиного національного центру стратегічних комунікацій як ключової координуючої інституції, що інтегрує моніторинг загроз, міжрівневу координацію та стратегічні комунікації).

4. Виявлено низку системних недоліків і структурних обмежень, що знижують ефективність державної політики у сфері ІБ. Передусім йдеться про фрагментарність нормативно-правового регулювання, відсутність узгоджених стандартів між суб’єктами сектору безпеки та оборони, недостатній рівень формалізованих процедур обміну інформацією між державними органами та приватним сектором, а також про брак цілісної моделі стратегічної координації. Окремим викликом є технологічна нерівність та різний рівень зрілості цифрових платформ і інституцій, що створює несиметричні вразливості всередині державної системи.

Сукупність виявлених недоліків формує комплекс загроз, які мають як внутрішній, так і зовнішній характер. До пріоритетних загроз належать: посилення гібридних інформаційних операцій з використанням ШІ та deepfake-технологій; зростання залежності критично важливих інфраструктур від

цифрових сервісів без достатнього рівня їхнього захисту; наростання інформаційної поляризації та зниження суспільної довіри; інституційна розмитість відповідальності між державними органами; а також підвищення уразливості державного управління до маніпулятивних або деструктивних впливів через недостатню інтегрованість аналітичних та технологічних компонентів ІБ.

Для подолання зазначених викликів та усунення системних недоліків запропоновано комплекс стратегічних кроків, що узгоджуються з кращими світовими практиками та враховують українські реалії. Серед ключових напрямів:

– кодифікація нормативно-правової бази інформаційної безпеки з метою усунення фрагментарності та дублювання повноважень;

– створення постійно діючої міжсекторальної координаційної платформи за участі держави, приватного сектору та громадянського суспільства;

– формування інтегрованої системи моніторингу та прогнозування інформаційних загроз із застосуванням інструментів штучного інтелекту;

– підвищення рівня цифрової стійкості через інституційне закріплення процедур кризового управління, обмін даними у режимі реального часу та стандартизацію кіберзахисту критичної інфраструктури;

– розвиток компетентнісного потенціалу державних службовців та підвищення рівня інформаційної грамотності населення як довгострокового інструменту зниження вразливостей.

Зазначені положення дозволяють не лише окреслити проблемні аспекти функціонування механізмів інформаційної безпеки, але й визначити чіткі напрями їх удосконалення, що формує цілісну рамку стратегічного розвитку державної політики у сфері ІБ

.

ВИСНОВКИ

У ході проведеного наукового дослідження було системно розглянуто проблематику інформаційної безпеки як складової національної безпеки держави, її нормативно-правові засади та інституційні механізми реалізації. Формування висновків ґрунтується на досягненні цілей і виконанні завдань, визначених у дисертації, що дозволяє консолідувати отримані результати та окреслити основні тенденції, виклики й перспективи розвитку системи забезпечення інформаційної безпеки в Україні в контексті публічного управління.

1. Розроблено інтегративну модель механізмів реалізації інформаційної безпеки у системі публічного управління України, яка, на відміну від існуючих, ґрунтується на міжсекторальному та комунікаційно-стратегічному підходах та включає: удосконалену інституційно-правову конструкцію ключових суб'єктів забезпечення інформаційної стійкості (РНБО, Центр протидії дезінформації; Міністерство культури України); критерії функціональної діагностики управлінських обмежень в умовах воєнного стану; комплексну концепцію стратегічного управління інформаційною безпекою, що забезпечує синергію між захистом критичної інфраструктури та підтримкою інформаційної гігієни громадянського суспільства.

2. Узагальнено теоретико-методологічні засади дослідження інформаційної безпеки у системі публічного управління шляхом системного аналізу її подвійної природи та авторського структурування її ключових елементів: інформаційна безпека як система суспільних відносин: Здійснено комплексне розмежування та структурування її елементів (суб'єкти: держава, громадянське суспільство, бізнес; об'єкт: інформаційне середовище; регулювання; інститути; цілі), а також ідентифіковано її ключові особливості

(суб’єктна взаємозалежність, громадянська участь, інформаційна грамотність, етика та відповідальність), що дозволяє перейти від статичного опису до динамічного управління процесами; інформаційна безпека як об'єкт правової охорони: Проаналізовано та систематизовано вітчизняні та зарубіжні наукові парадигми (кримінально-правова, цифрова, адміністративно-правова) та запропоновано науково-обґрунтовані рекомендації щодо її ефективної правової охорони, які включають необхідність законодавчого ототожнення термінів «інформаційна безпека держави» та «інформаційна безпека громадянина» як де-факто об’єктів правової охорони.

3. Розроблено підходи до інституційного механізму забезпечення інформаційної безпеки в системі публічного управління шляхом: розробки та обґрунтування мультифункціональної архітектурної моделі взаємодії ключових суб’єктів — Служби безпеки України (СБУ), Ради національної безпеки та оборони України (РНБО) та Міністерства цифрової трансформації України (Мінцифри) — виведеної за тривимірним кластерним співвідношенням (моніторинг-координація-впровадження), що дозволяє перейти від лінійного переліку функцій до системного розуміння механізму забезпечення національної інформаційної стійкості; концептуалізації соціальної ролі Міністерства культури та стратегічних комунікацій України (Мінкульт) як повноправного суб’єкта забезпечення інформаційної безпеки, який виконує стратегічну місію із забезпечення культурно-інформаційної стійкості та нормативно-правового регулювання інформаційної політики, доповнюючи техніко-правовий та правоохоронний сегменти (СБУ, Нацполіція).

4. Систематизовано та концептуалізовано методологічні засади дослідження інформаційної безпеки у системі публічного управління, що дозволило: розширити та уточнити зміст таких ключових методологічних підходів (системність, міждисциплінарність, комплексність) шляхом додавання до них прогностично-моделювального та кореляційно-взаємодоповнювального елементів, що є критично важливим для аналізу ІБ в умовах динамічних

гібридних загроз; науково обґрунтувати та ввести до наукового обігу принципи дослідження інформаційної безпеки (комплексність, прогнозованість та глобальність) у контексті публічного управління, розкривши їхню суть через орієнтацію на майбутні виклики (принцип прогнозованості) та потенційну рецепцію міжнародних стандартів і досвіду (принцип глобальності) у національно-правове та інституційне поле України; актуалізувати застосування філософських основ дослідження ІБ, зокрема, через призму ціннісної парадигми інформації як активу та діалектичного співставлення категорій «безпека» та «свобода» як конституційно гарантованого прояву інформаційної політики.

5. Концептуалізовано сутнісне призначення механізму правового регулювання ІБ через: 1) інтеграцію двох ключових функціональних кластерів: регулювання інформаційної діяльності (включно з обов'язком державних органів дотримуватись ІБ-законодавства) та розвиток інформаційного середовища (орієнтація на інновації та формування "інформаційного суспільства"); 2) теоретичне обґрунтування власного підходу до кореляції між механізмом правового регулювання ІБ та правом людини на інформацію як взаємного забезпечення прав, де реалізація права на інформацію громадян детермінує діяльність інституцій ІБ-парадигми, а інформаційна безпека має на меті конституційну непорушність цього права; 3) систематизації та початкового опису дванáдцяти ключових принципів побудови механізму правового регулювання забезпечення інформаційної безпеки в Україні, які інтегрують правовий, управлінський та технологічний аспекти (законності, захисту прав та свобод людини, національного суверенітету, прозорості, превентивності, технологічної адаптивності, міжвідомчої координації, співпраці та інтеграції, пропорційності, відповідальності, безперервності); 4) концептуалізацію моделі державного управління ІБ в умовах воєнного стану через систематизацію його основних закономірностей (пріоритетність загальнонаціональних інтересів, превенція дезінформації, інституціоналізація та оперативність управління), а

також запропоновано шляхи його розвитку шляхом інтеграції механізмів громадського контролю та підвищення прозорості державних заходів для посилення суспільної довіри.

6. Систематизовано та науково обґрунтовано методичні підходи протидії загрозам інформаційній безпеці України в умовах військової агресії, що виражається у кластеризації методичних підходів протидії загрозам інформаційній безпеці у системі публічного управління, виділивши п'ять взаємодоповнюючих кластерів: нормативно-правові та організаційні механізми (через аналіз ЗУ «Про національну безпеку України» та ЗУ «Про основні засади забезпечення кібербезпеки України»); технічні засоби та методологія кіберзахисту (використання SIEM, IDS/IPS, міжнародна кооперація, наприклад, із NATO CCDCOE та Microsoft DART); інформаційно-психологічна безпека та протидія дезінформації (підвищення медіаграмотності, діяльність Центру протидії дезінформації, використання VoxCheck та StopFake); освітні ініціативи та підвищення цифрової грамотності (аналіз ініціативи «Дія. Цифрова освіта» та застосування ідеологічного контролю в ЗВО, наприклад, через обмеження використання месенджера Telegram); інтеграція міжнародної співпраці (положення Угоди про асоціацію з ЄС, долучення до Cyber Rapid Response Teams, співпраця з Google, Amazon, Microsoft.

7. Розроблено концептуальну модель переходу до адаптивної архітектури забезпечення ІБ (на основі концепції adaptive security governance), яка передбачає формалізацію нової архітектури інформаційної безпеки на засадах прозорості та гласності та впровадження трирівневої структури управління: стратегічний рівень (створення аналітичного центру з прогнозування ІБ (орієнтація на передбачення та сценарне планування); оперативний рівень (створення спільних міжвідомчих центрів реагування (забезпечення синхронізованої відповіді); тактичний рівень (розробка локальних сценаріїв дій на рівні відомств та територіальних громад (гнучке реагування).

8. Розвинуто теоретичні засади стратегічного управління інформаційною

безпекою шляхом систематизації та компаративного аналізу міжнародних моделей, що дозволило: уточнити сутність стратегічного управління забезпеченням ІБ як процесу синхронізації юридичних, організаційних та технічних засобів для захисту державних, економічних і соціальних інтересів, із ключовим акцентом на пошуку оптимального балансу між нормативним закріпленням та фактичним впровадженням безпекової карти; розробити типологію міжнародних моделей стратегічного управління ІБ на основі аналізу досвіду США, ЄС, Великої Британії, Ізраїлю та Китаю; систематизувати мету стратегічного управління ІБ на три взаємопов'язані рівні (захист (базовий): нейтралізація загроз та забезпечення довіри до інформаційного середовища; розвиток (інноваційний): сприяння інноваціям та технологічному розвитку (ІКТ та ШІ) в ІБ; стійкість (соціальний): підвищення обізнаності населення та розвиток культури інформаційної безпеки (кібергігієни); виокремити чотири ключові особливості стратегічного управління ІБ у розвинених державах світу: правове регулювання, інституційна структура, міжнародна співпраця (Будапештська конвенція) та використання інновацій (ШІ та ІКТ).

9. Узагальнено та систематизовано сучасні виклики та тенденції розвитку механізмів інформаційної безпеки держави, що дозволило: класифікувати та поглибити аналіз сучасних інформаційних ризиків за трьома основними вимірами, акцентуючи на їхній взаємозалежності та кумулятивному ефекті (глобально-політичні ризики: розкрито як систему взаємопов'язаних загроз: гібридні війни (поєднання військових, кібернетичних та інформаційних засобів), дезінформація та інформаційна асиметрія (дисбаланс між швидкістю поширення та здатністю суспільства до критичного осмислення); технологічні ризики: визначено штучний інтелект (ШІ) як інструмент подвійної дії (можливість для захисту vs. інструмент для автоматизованих фішингових схем), аналітику великих даних (Big Data) як джерело монополізації інформації та deepfake-технології як чинник «кризи достовірності»; соціально-комунікаційні ризики: доведено, що соціальні мережі та цифрові платформи є феноменом

подвійної природи (канал демократизації та арена гібридних атак), а їхня алгоритмічна архітектура є каталізатором поляризації та поширення сенсаційного контенту, що вимагає регулювання не лише контенту, а й самих алгоритмічних процесів); обґрунтувати необхідність інтеграції нових підходів до зміцнення кіберстійкості суспільства та сформувати двопланову модель протидії ризикам (поведінковий/освітній вимір: акцентовано на інформаційній гігієні та медіаграмотності як базових елементах зменшення вразливості громадян (приклад Швеції та Фінляндії); інституційно-правовий вимір: систематизовано нові регуляторні механізми (зокрема, Digital Services Act (DSA) та Data Governance Act (DGA) ЄС), які створюють інституційну рамку для боротьби з дезінформацією та забезпечення прозорості алгоритмів, що є прикладом збалансованого регулювання).

10. Обґрунтовано теоретико-методологічні засади формування механізмів забезпечення інформаційної безпеки шляхом: систематизації та критичного аналізу трьох основних управлінських моделей (централізованої, децентралізованої та публічно-приватного партнерства) у контексті протидії гібридним загрозам, з виокремленням їхніх переваг і обмежень для України (централізована модель (США, Ізраїль): визначено як ефективну для швидкого реагування та уніфікації стандартів, але вказано на ризики бюрократизації та дублювання повноважень в українських умовах (СБУ, РНБО); децентралізована модель (Німеччина, Японія): обґрунтовано її переваги у гнучкості та врахуванні секторної специфіки (Мінцифра, НБУ, ДССЗЗІ), проте виявлено ключовий недолік — ризик розрізненості стандартів та низька узгодженість без належних координаційних механізмів; публічно-приватне партнерство (США – CISA, Велика Британія – CiSP): обґрунтовано його як критично важливий механізм для оперативного обміну інформацією про загрози та інтеграції технологічної експертизи приватного сектору, що є необхідним для протидії сучасним інформаційним та кіберзагрозам).

11. Розроблено та науково обґрунтовано концепцію Стратегії-моделі

національної цифрової стійкості України як узагальнюючого результату дослідження механізмів інформаційної безпеки, де пропонується поєднання стратегічного (нормативно-прогностичного) та модельного (структурно-організаційного) підходів. Показано, що цифрова стійкість охоплює ширшу систему, ніж інформаційна безпека, включаючи кіберзахист, управління даними, безпеку цифрових публічних послуг, цифрову етику та адаптивність суспільства до інформаційних, технологічних і комунікаційних ризиків. У цьому контексті інформаційна безпека розглядається як базовий структурний елемент цифрової стійкості, що визначає її нормативну та інституційну основу. Запропонована стратегія-модель передбачає трирівневу архітектуру управління (стратегічний рівень — формування довгострокових цифрових безпекових пріоритетів; тактичний — координація дій суб'єктів публічної влади; операційний — реагування на цифрові інциденти та загрози), а також спирається на чотири ключові принципи: проактивність, багаторівневу координацію, гнучкість та демократичний контроль. Її концепція вибудувана у логічному зв'язку з визначеними у дисертації завданнями, зокрема щодо удосконалення інституційних механізмів ІБ, модернізації правового регулювання, інтеграції міжнародних стандартів та формування адаптивної моделі цифрового врядування.

СПИСОК ВИКОРИСТАНИХ ДЖЕРЕЛ

1. Аналітичний портал «Слово і Діло». Законопроект про дезінформацію: за що передбачена кримінальна та адміністративна відповідальність. Офіційний веб-сайт АП «Слово і Діло». 28.01.2020.

2. Андрущенко, В. Я. Взаємодія публічного та приватного секторів у забезпеченні національної кібербезпеки. Економіка та держава. 2022. № 11. С. 140–148.

3. Антонюк, В. Основні науково-методологічні підходи до дослідження державної політики інформаційної безпеки. Інвестиції : практика та досвід. Серія : Державне управління. № 20. 2013. С. 143-147. С. 144-145.

4. Архипов, О., Архипова, Є. Особливості розуміння понять «інформаційна безпека» та «безпека інформації». Інформаційні технології та безпека : основи забезпечення інформаційної безпеки (ІТБ-2014) : Матеріали XIV міжнародної науково-практичної конференції. ІПРІ НАН України. Київ. 2014. С. 18-30.

5. АТ «Укрпошта». Корпоративний звіт про управління за 2023 рік. АТ «Укрпошта», 2023. 23 с.

6. Бабкіна, В. М. Механізми інформаційної безпеки в діяльності державних органів: виклики та шляхи оптимізації. Державне управління: теорія та практика. 2024. № 2. С. 135–145.

7. Бакуменко, В. Д. Стратегічне управління національною безпекою України в умовах глобалізації. Київ : Видавництво НАДУ, 2021. 450 с. (С. 210–245).

8. Баран, М. Інформаційна безпека як предмет адміністративно-правового регулювання. Соціально-правові студії. № 3 (13). 2021. С. 50-56.

9. Білоус, О. С. Інформаційна безпека держави: сутність, механізми, стратегії. Харків : Право, 2020. 380 с. (С. 110–135).

10. Бондар, М. І. Хмарні технології у публічному секторі: механізми безпекового контролю. Електронне урядування. 2024. Т. 8. № 1. С. 30–40.

11. Брацук, І. Міжнародно-правове регулювання забезпечення інфор-

маційної безпеки в рамках ООН. Вісник КНУ ім. Т. Г. Шевченка. Серія : Юридичні науки. № 1 (25). 2023. С. 21-26. С. 23-25.

12. Бугай, С. О. Кадрове забезпечення як елемент механізму інформаційної безпеки публічної служби. Вісник Хмельницького національного університету. Серія Економічні науки. 2020. № 5. С. 245–253.

13. Бурик, З. О. Концепція змін і реформ у системі публічного адміністрування. Public Management and Policy. 2025. № 5(9). С. 50–59.

14. Валюшко, І. Інформаційна безпека України : трансформація законодавства після російського вторгнення. Історико-політичні студії. Серія: Політичні науки : збірник наукових праць. КНЕУ. Київ. 2017. № 2. С. 30-43.

15. Вареня, Н. А. Публічне управління в умовах військових загроз: український досвід адаптації до кризових ситуацій. Public Management and Policy. 2024. № 2. С. 35–45.

16. Василенко, О. В. Юридичні механізми протидії дезінформації в системі публічного управління. Європейські перспективи. 2023. № 4. С. 55–63.

17. Вітер, Д., Гузонова, В., Шевчук, В., Молочко, Т., Кутова, М. Механізми публічного управління для забезпечення національної та інформаційної безпеки. Management Theory and Studies for Rural Business and Infrastructure Development. 2025. Vol. 47, No. 2. С. 260–269.

18. Войціховський, А. Інформаційна безпека як складова системи національної безпеки (міжнародний і зарубіжний досвід). Вісник Харківського національного університету імені В.Н. Каразіна. Серія : Право. № 29. 2020. С. 281-288.

19. Волков, Г. П. Застосування технології блокчейн для підвищення прозорості та безпеки державних реєстрів. Інноваційні технології в управлінні. 2023. № 11. С. 175–185.

20. Ворона, О. В. Механізми публічного управління кібербезпекою критичної інфраструктури. Дніпро : Монографія, 2023. 415 с. (С. 150–180).

21. Гаврильців, М. Інформаційна безпека держави в системі національної безпеки України. Юридичний науковий електронний журнал. № 2. 2020. С. 200-203.

22. Главком. Заборона Telegram. Які університети обмежили використання месенджера. 06.11.2024 р. Офіційний веб-портал Главком.

23. Глоба, Д. П'ять головних проблем державних реєстрів України. Українська правда. 07.03.2024 р. Офіційний веб-портал «Українська правда».

24. Голобородько, В. А. Огляд політик кібербезпеки у публічному секторі: виклики та шляхи вирішення. A Review of Cybersecurity Policies in the Public Sector: Challenges and Solutions. 2025. С. 1–15.

25. Гончаров, М. Дослідження поняття «інформаційна безпека». Науковий вісник Ужгородського національного університету. Серія : Право. Вип. 82 (1). С. 34-37. С. 35.

26. Грабар, Н. Механізми інформаційної безпеки України в умовах інформаційного глобалізму. Право та державне управління. № 2 (35). 2019. С. 168-173. С. 170-171.

27. Григоренко, М. С. Організаційно-правові механізми захисту критичної інформаційної інфраструктури України. Право та державне управління. 2023. № 5(43). С. 88–97.

28. Григоренко, О. В. Діджиталізація та кібербезпека: виклики для публічного адміністрування. Київ : Ліра-К, 2024. 352 с. (С. 60–90).

29. Грицак, Н. Ю. Діджиталізація публічного управління та ризики інформаційної безпеки: управлінський аспект. Науковий вісник публічного та приватного права. 2023. № 5. С. 201–209.

30. Демидова, Л. Кримінально-правова охорона інформаційної безпеки : європейські стандарти. Юридичний електронний науковий журнал. № 7. 2023. С. 354-357.

31. Демченко, І. В. Кібергігієна та навчання персоналу як нетехнічний механізм інформаційної безпеки. Державне управління та національна безпека. 2024. № 6. С. 120–128.

32. Детектор медіа. Російські хакери повторно атакували телемарафон «Єдині новини». 09.11.2023 р. Офіційний веб-портал «Детектор медіа».

33. Довгань, О., Ткачук, Т. Правове забезпечення інформаційної безпеки держави як підгалузь інформаційного права : теоретичний дискурс. Інфор-

мація і право. № 2 (25). 2018. С. 73-85.

34. Дрозденко, І. Г. Управління кібербезпекою в умовах інтеграції до Єдиного цифрового ринку ЄС. Європейські студії та право. 2025. № 1. С. 45–56.

35. Європейська правда. Як Україна співпрацює з НАТО у сфері кіберзахисту. 06.07.2022 р. Офіційний веб-портал «Європейська правда».

36. Жадько, К. Управління інформаційною безпекою підприємств-постачальників електронних комунікаційних послуг. Агросвіт. № 14. 2024. С. 21-27. С. 24.

37. Журавльов, Р. І. Правові засади використання криптографічних засобів захисту в державних інформаційних системах. Часопис Київського університету права. 2021. № 2. С. 135–144.

38. Заблоцький, Д. І. Використання штучного інтелекту для підвищення ефективності механізмів інформаційного захисту. Наукові записки Інституту законодавства ВРУ. 2024. № 4. С. 75–83.

39. Загородня А.С., Котляров В. Управління економічною безпекою: стратегічні цілі та механізми реалізації. Київ: Національний університет біоресурсів і природокористування, 2024. 200 с.

40. Задувайло, О. Реалізація права на доступ до інформації, що містить державні секрети в світовій практиці. Державне управління: удосконалення та розвиток. № 2. 2017.

41. Задувайло, О. Реалізація права на доступ до інформації, що містить державні секрети в світовій практиці. Державне управління: удосконалення та розвиток. № 2. 2017. http://www.dy.nayka.com.ua/?op=1&z=1037

42. Зайцев, К. В. Впровадження системи ідентифікації та автентифікації користувачів у державних інформаційних системах. Технологічна безпека. 2025. № 1. С. 50–60.

43. Закон України «Про доступ до публічної інформації» № 2939-VI від 13.01.2011 р. (поточна ред. від 08.10.2023 р.). Відомості Верховної Ради. URL: https://zakon.rada.gov.ua/laws/show/2939-17#Text

44. Закон України «Про електронну ідентифікацію та електронні довірчі послуги» № 2155-VIII від 05.10.2017 р. (ред. від 18.12.2024 р.). Відомості

Верховної Ради. URL: https://zakon.rada.gov.ua/laws/show/2155-19#Text

45. Закон України «Про захист інформації в інформаційно-комунікаційних системах» № 80/94-ВР від 05.07.1994 р. (ред. від 28.06.2024 р.). Відомості Верховної Ради. URL: https://zakon.rada.gov.ua/laws/show/80/94-%D0%B2%D1%80#Text

46. Закон України «Про захист персональних даних» № 2297-VI від 01.06.2010 р. (ред. від 18.01.2025 р.). Відомості Верховної Ради. URL: https://zakon.rada.gov.ua/laws/show/2297-17#Text

47. Закон України «Про інформацію» № 2657-XII від 02.10.1992 р. (поточна ред. від 15.11.2024 р.). Відомості Верховної Ради. URL: https://zakon.rada.gov.ua/laws/show/2657-12#Text

48. Закон України «Про медіа» № 2849-IX від 13.12.2022 р. (поточна ред. від 01.01.2025 р.). Відомості Верховної Ради. URL: https://zakon.rada.gov.ua/laws/show/2849-20#Text

49. Закон України «Про національну безпеку України» № 2469-VIII від 21.06.2018 р. (ред. від 09.08.2024 р.). Відомості Верховної Ради. URL: https://zakon.rada.gov.ua/laws/show/2469-19#Text

50. Закон України «Про Національну поліцію України» № 580-VIII від 02.07.2015 р. (поточна ред. від 16.08.2024 р.). Відомості Верховної Ради. URL: https://zakon.rada.gov.ua/laws/show/580-19#Text

51. Закон України «Про основні засади забезпечення кібербезпеки України» № 2163-VIII від 05.10.2017 р. (ред. від 28.06.2024 р.). Відомості Верховної Ради. URL: https://zakon.rada.gov.ua/laws/show/2163-19#Text

52. Закон України «Про поштовий зв’язок» № 2759-XII від 03.11.2022 р. (поточна ред. від 21.06.2024 р.). Відомості Верховної Ради. URL: https://zakon.rada.gov.ua/laws/show/2759-12#Text

53. Закон України «Про Раду національної безпеки та оборони України» № 183/98-ВР від 05.03.1998 р. (поточна ред. від 29.07.2023 р.). Відомості Верховної Ради. URL: https://zakon.rada.gov.ua/laws/show/183/98-%D0%B2%D1%80#Text

54. Закон України «Про Службу безпеки України» № 2229-XII від

25.03.1992 р. (поточна ред. від 29.06.2024 р.). Відомості Верховної Ради. URL: https://zakon.rada.gov.ua/laws/show/2229-12#Text

55. Захаренко, К. Категорія інформаційної безпеки безпеки у вітчизняному філософсько-політологічному дискурсі. Гуманітарний вісник ЗДІА. № 72. 2018. С. 44-52. С. 47-48.

56. Захаренко, К. Категорія інформаційної безпеки безпеки у вітчизняному філософсько-політологічному дискурсі. Гуманітарний вісник ЗДІА. № 72. 2018. С. 44-52. С. 47-48.

57. Захаров, А. П. Штучний інтелект у публічному управлінні: виклики кібербезпеки та вразливості. Integrating Artificial Intelligence into Public Administration: Challenges and Vulnerabilities. 2024. Vol. 15, Iss. 4. С. 149–160.

58. Згуровський, М. З. Глобальна та національна кібербезпека: теоретико-практичні аспекти. Київ : НТУУ "КПІ", 2020. 530 с. (С. 400–435).

59. Зицик, С. Правове регулювання інформації з обмеженим доступом. Юридичний науковий електронний журнал. № 5. 2023. С. 220-223. С. 221.

60. Золотар, О. Ґенеза суспільних відносин щодо інформаційної безпеки людини. Інформація і право. № 1 (24). 2018. С. 139-148.

61. Іванов, А. О. Адміністративно-правове регулювання механізмів захисту критичної інформаційної інфраструктури. Право України. 2024. № 3. С. 115–123.

62. Іванченко, Н., Подскребко, О. Особливості реалізації системи управління інформаційною безпекою. Collection of scientific papers «SCIENTIA». Zagreb, Republic of Croatia. 24 March 2023. P. 19-21. С. 20.

63. Ільницька, У. Інформаційна безпека України : сучасні виклики, загрози та механізми протидії негативним інформаційно-психологічним впливам. Політичні науки. № 2 (1). 2016. С. 27-32.

64. Капля, О. Правове регулювання інформаційної безпеки громадянина під час воєнного стану. Експерт: парадигми юридичних наук і державного управління. № 6 (24). 2023. С. 16-20. С. 17-18.

65. Карагіоз, Р., Вдовиченко, О. Розроблення поняття «інформаційна безпека» у правовому напрямі : теоретичний аналіз. Південноукраїнський прав-

ничий часопис. Серія : Правова система : теорія і практика. № 2. 2018. С. 34-36.

66. Качковська, Л., Вознюк, Є. Протидія інформаційним загрозам в Україні : актуальні питання для вирішення на державному рівні. Міжнародні відносини, суспільні комунікації та регіональні студії. № 1 (18). 2024. С. 85-102. С. 89-90.

67. Кіндратець, О. С. Інформаційні війни та механізми захисту публічного управління від маніпуляцій. Харків : ФОП Петров, 2023. 320 с. (С. 65–90).

68. Кірєєв, О. С. Механізми швидкого реагування на кіберінциденти в державному управлінні. Безпека інформації. 2024. № 5. С. 100–110.

69. Коваленко, І. Г. Державна політика у сфері кібербезпеки: інституційні та правові механізми забезпечення. Публічне управління та адміністрування. 2023. № 4. С. 87–96.

70. Коваль, В. І. Теоретико-методологічні засади формування державної політики у сфері інформаційної безпеки. Одеса : Гельветика, 2022. 510 с. (С. 250–280).

71. Ковальов К. Інформаційна безпека: міжнародно-правовий аспект. Інформація і право. -Київ. НДЦПІ НАПН України. № 4. 2023. С.159-167.

72. Ковальчук, Д. І. Роль ENISA у формуванні механізмів кібербезпеки публічного управління в ЄС: досвід для України. ENISA SINGLE PROGRAMMING DOCUMENT 2025–2027. 2025. С. 8–18.

73. Кондращенко, І. Зовнішні та внутрішні загрози інформаційній безпеці України. Юрист України. № 2. 2018. С. 27-32. С. 29.

74. Кононенко, В. та ін. Інформаційна безпека як стан. Науковий вісник Ужгородського національного ун-ту. Серія : Право. № 2 (76). С. 244-250.

75. Копійка, М. Стратегічні ризики інформаційної безпеки європейських країн. Міжнародні та політичні дослідження. Вип. 32. 2019. С. 85-102. С. 103-104.

76. Копійка, М. Стратегічні ризики інформаційної безпеки європейських країн. Міжнародні та політичні дослідження. Вип. 32. 2019. С. 85-102. С. 103-104.

77. Корецька, В., Жебка, В. Цифрова грамотність населення як фунда-

мент цифровізації держави. Телекомунікаційні та інформаційні технології. № 3 (76). 2022. С. 12-20. С. 17-18.

78. Коробейнікова, Т., Цар, О. Аналіз сучасних відкритих систем виявлення та запобігання вторгнень. Грааль науки. № 27. 2023. С. 317-325. С. 323.

79. Корпан, Я. Класифікація загроз інформаційній безпеці в комп'ютерних системах при віддаленій обробці даних. Реєстрація зберігання і обробка даних. Вип. 17 (2). 2015. С. 39-46. С. 42-43.

80. Коруц, У. Запобігання та протидія пропаганді війни та інформаційним загрозам в Україні. Публічне право. № 2 (38). 2020. С. 80-87. С. 84.

81. Костенко, І. Г. Правові основи забезпечення кібербезпеки в Україні. Київ : Юрінком Інтер, 2021. 360 с. (С. 140–165).

82. Костенко, Р. П. Формування системи кібербезпеки в органах місцевого самоврядування. Місцеве самоврядування та регіональний розвиток. 2024. № 3. С. 110–118.

83. Котерлін, І. Сутність механізму правового регулювання інформаційних відносин. Право та державне управління. № 1 (1). 2020. С. 72-76. С. 73-74.

84. Котляров В.О. Еволюція міжнародно-політичної взаємодії у сфері інформаційних відносин. Публічне управління і адміністрування в Україні. 2023. Вип. 37. С. 76–81. URL: http://www.pag-journal.iei.od.ua/37-2023

85. Котляров В.О. Інформаційна безпека в системі стратегічного управління державою. Економіка та держава. 2024. № 1. С. 120–124. URL: https://www.economy.in.ua/pdf/1_2024/26.pdf

86. Котляров В.О. Інформаційна безпека в системі управління інноваційними ризиками. Економіка та держава. 2024. № 5. С. 104–108. URL: https://www.economy.in.ua/pdf/5_2024/22.pdf

87. Котляров В.О. Інформаційна безпека в системі управління репутаційними ризиками. Економіка та держава. 2024. № 3. С. 112–116. URL: https://www.economy.in.ua/pdf/3_2024/24.pdf

88. Котляров В.О. Інформаційна безпека в системі управління ризиками підприємства. Економіка та держава. 2024. № 2. С. 116–120. URL:

https://www.economy.in.ua/pdf/2_2024/25.pdf

89. Котляров В.О. Інформаційна безпека в системі управління стратегічними ризиками. Економіка та держава. 2024. № 4. С. 108–112. URL: https://www.economy.in.ua/pdf/4_2024/23.pdf

90. Котляров В.О. Інформаційна безпека в системі управління фінансовими ризиками. Економіка та держава. 2024. № 6. С. 100–104. URL: https://www.economy.in.ua/pdf/6_2024/21.pdf

91. Котляров В.О. Інформаційна безпека в умовах глобальної взаємозалежності. Наукові перспективи. 2025. № 7(17). С. 474–486. DOI: 10.52058/3041-1254-2025-7(17)-474-486

92. Котляров В.О. Інформаційна безпека України: адаптація до стандартів ЄС і НАТО. Наукові перспективи. 2025. № 8(48). С. 180–192. DOI: 10.52058/2786-5274-2025-8(48)-180-192

93. Котляров В.О. Інформаційна безпека як елемент економічної безпеки держави. Економіка та держава. 2023. № 12. С. 114–118. URL: https://www.economy.in.ua/pdf/12_2023/24.pdf

94. Котляров В.О. Інформаційна безпека як система правовідносин. Наукові перспективи. 2025. № 8(38). С. 245–259. DOI: 10.52058/2786-6300-2025-8(38)-245-259

95. Котляров В.О. Інформаційне забезпечення безпеки вітчизняної та світової спільноти. Наукові праці МАУП. Політичні науки та публічне управління. 2024. № 1(73). С. 45–52. DOI: 10.32689/2523-4625-2024-1(73)-6

96. Котляров В.О. Категоріальний апарат інформаційної безпеки. Наукові перспективи. 2025. № 8(16). С. 615–629. DOI: 10.52058/3041-1572-2025-8(16)-615-629

97. Котляров В.О. Кібертероризм як загроза міжнародній безпеці. Український журнал прикладної економіки та техніки. 2023. Т. 8, № 2. С. 314–321. DOI: 10.36887/2415-8453-2023-2-45

98. Котляров В.О. Кібертероризм як загроза національній безпеці України. Інвестиції: практика та досвід. 2023. № 21. С. 122–126. URL: https://www.investplan.com.ua/pdf/21_2023/27.pdf

99. Котляров В.О. Комплексний підхід щодо розуміння інформаційної безпеки. Публічне управління і адміністрування в Україні. 2023. Вип. 38. С. 168–172. URL: http://www.pag-journal.iei.od.ua/archives/2023/38-2023/30.pdf

100. Котляров В.О. Методологічні засади дослідження інформаційної безпеки. Наукові перспективи. 2025. № 9(49). С. 187–199. DOI: 10.52058/2786-5274-2025-9(49)-187-199

101. Котляров В.О. Механізми раннього виявлення інформаційних атак. Наукові перспективи. 2025. № 8(18). С. 443–455. DOI: 10.52058/3041-1254-2025-8(18)-443-455

102. Котляров В.О. Механізми управління репутаційними ризиками. Наукові перспективи. 2025. № 9(17). С. 624–637. DOI: 10.52058/3041-1572-2025-9(17)-624-637

103. Котляров В.О. Особливості категорії «Інформаційна безпека» у міжнародному контексті. Наукові праці МАУП. Політичні науки та публічне управління. 2023. № 4(70). С. 21–26. DOI: 10.32689/2523-4625-2023-4(70)-3

104. Котляров В.О. Правовий механізм забезпечення інформаційної безпеки: структура, принципи та інституційна модель України. Наукові перспективи. 2025. № 8 (62). С. 907-919. URL: https://doi.org/10.52058/2708-7530-2025-8(62)-907-919.

105. Котляров В.О. Система забезпечення інформаційної безпеки України. Наукові праці МАУП. Політичні науки та публічне управління. 2024. № 1(73). С. 40–44. DOI: 10.32689/2523-4625-2024-2(74)-6

106. Котляров В.О. Стратегічне управління інформаційною безпекою в умовах цифрової трансформації. Економіка та держава. 2023. № 11. С. 118–122. URL: https://www.economy.in.ua/pdf/11_2023/25.pdf

107. Котляров В.О. Стратегічні цілі інформаційної безпеки. Наукові перспективи. 2025. № 8(13). С. 903–914. DOI: 10.52058/3041-1793-2025-8(13)-903-14

108. Котляров В.О. Теоретичні засади сутності та концепції інформаційної безпеки. Наукові перспективи. 2023. № 6(36). С. 131–142. URL: http://perspectives.pp.ua/index.php/np/article/view/5276/5306

109. Котляров В.О. Формування державної політики кібергігієни. Наукові перспективи. 2025. № 7(61). С. 162–174. DOI: 10.52058/2708-7530-2025-7(61)-162-174

110. Кочубей, Л. Інформаційна безпека держави : інструменти захисту українського інформаційного поля (на прикладі особливостей інформаційно-комунікаційних технологій у сучасному Донбасі). ІПіЕНД ім. І. Ф. Кураса НАН України. Наукові записки. № 3 (77). 2015. С. 220-237.

111. Кравчук, О. В. Захист інформації у системі кібербезпеки як стратегічний пріоритет державних механізмів. Public Administration and Regional Development. 2025. № 27. С. 45–55.

112. Кривцов, В. Інформаційні заходи оборони держави в сучасних умовах. Часопис Київського ун-ту права. Серія : Теорія та історія держави і права. Філософія права. № 1. 2023. С. 30-33.

113. Крупнова, А. Правове регулювання сфери забезпечення інформаційної безпеки в Україні. Аналітично-порівняльне правознавство. № 5. 2023. 7 с.

114. Кудрявцев, Б. В. Механізми протидії маніпулятивному впливу в публічному управлінні. Стратегічна панорама. 2021. № 3. С. 99–107.

115. Кузнєцов, А. В. Адміністративно-правові механізми захисту інформаційних ресурсів публічного сектору. Львів : Новий Світ-2000, 2023. 420 с. (С. 190–220).

116. Кузьменко, М. С. Організаційно-технічні механізми аудиту інформаційної безпеки в державних органах. Електронне урядування. 2020. Т. 7. № 1. С. 25–34.

117. Кулик, А. С. Міжнародна співпраця як механізм підвищення кіберстійкості публічного управління. Міжнародні відносини. 2024. № 1. С. 40–50.

118. Лавриненко, В. Ю. Аналіз механізмів фінансування заходів кібербезпеки у публічному секторі. Економіка та фінанси. 2023. № 10. С. 201–210.

119. Лисенко, І. Л. Проблеми імплементації міжнародних стандартів кібербезпеки в національне законодавство України. Інформація і право. 2020. № 1(29). С. 78–86.

120. Лопатченко, І. та ін. Державне регулювання у сфері інформаційної безпеки України в умовах воєнного стану. Вісник НУЦЗУ. Серія : Державне управління. № 1 (20). 2024. С. 14-24.

121. Мазуренко, Л. Інформаційна безпека в умовах російсько-української війни : виклики та загрози. Вісник Харківського національного університету імені В. Н. Каразіна. Серія : «Питання політології». № 42. 2022. С. 50-57.

122. Макаренко, Л. К. Механізми управління кіберризиками в органах державної влади. Науковий вісник публічного управління. 2023. № 4. С. 75–84.

123. Марущак, А. І. Інформаційна безпека та захист персональних даних: європейські стандарти та українська практика. Київ : ФОП Лисенко М.М., 2020. 480 с. (С. 310–340).

124. Марченко, Л. С. Правові механізми забезпечення безпеки персональних даних в електронному урядуванні. Інформація і право. 2024. № 3(49). С. 60–70.

125. Махепа, С. Забезпечення інформаційної безпеки в Україні : перспективи адміністративно-правововго регулювання. Актуальні проблеми правознавства. № 1 (37). 2024. С. 92-97. С. 94.

126. Мельник, О. М. Забезпечення стійкості інформаційної інфраструктури органів публічної влади. Теорія та практика державного управління. 2024. № 1(85). С. 45–54.

127. Міністерство цифрової трансформації України (Мінцифра). Уряд затвердив Положення про Єдиний державний портал цифрової освіти. 01.12.2021 р. Офіційний веб-портал Мінцифри.

128. Нашинець-Наумова, А. Інформаційна безпека : питання правового регулювання : монографія. Київський ун-т ім. Б. Грінченка. Київ. 2017. 168 с.

129. Нечипоренко, А. В. Дотримання вимог GDPR у публічному управлінні України: правовий механізм. Науковий вісник Ужгородського національного університету. Серія Право. 2025. Вип. 72. С. 250–259.

130. Олійник, П. М. Адміністративна відповідальність за порушення вимог інформаційної безпеки у публічному секторі. Право України. 2023. № 8. С.

150–160.

131. Олійник, Р. С. Державне управління у сфері кібербезпеки: правові та організаційні аспекти. Харків : Економіка, 2024. 330 с. (С. 95–115).

132. Онищенко, Г. М. Цифровізація в системі публічного адміністрування та її вплив на інформаційну безпеку. Digitalization in the Public Administration System. 2025. С. 1–11.

133. Орленко, П. С. Державне регулювання захисту інформаційних ресурсів в умовах гібридних загроз. Право та державне управління. 2023. № 1(32). С. 101–110.

134. Павленко, Л. Д. Методологія оцінки ризиків інформаційної безпеки в органах державної влади. Вінниця : ВНТУ, 2023. 305 с. (С. 170–195).

135. Пам'ятайте: Всі дані, особливо сторінки та роки, є ілюстративними (приблизними) і потребують обов'язкової перевірки за оригінальними джерелами.

136. Панченко, О. Інформаційна безпека держави як складник розвитку суспільних відносин. Публічне управління і адміністрування в Україні. № 17. 2020. С. 135-139.

137. Пашинський, В. Рада національної безпеки і оборони України як суб’єкт забезпечення оборони держави. Порівняльно-аналітичне право. № 5. 2017. С. 259-262. С. 260.

138. Пащенко, О. Кримінально-правова охорона інформаційної безпеки нормами розділу І Особливої частини КК України. Питання боротьби зі злочинністю. № 47. 2024. С. 11-17.

139. Перун, Т. Структурні чинники механізму інформаційної безпеки держави. Юридичний вісник. № 4. 2020. С. 117-124. С. 120.

140. Перун, Т. Структурні чинники механізму інформаційної безпеки держави. Юридичний вісник. № 4. 2020. С. 117-124. С. 119-120.

141. Петров, В. В. Удосконалення управлінських механізмів інформаційної безпеки в умовах воєнного стану. Вісник Національної академії державного управління. 2022. Вип. 2. С. 112–125.

142. Подорожна, Т. Забезпечення інформаційної безпеки України в умо-

вах сучасних викликів та загроз з боку рф. Електронне наукове видання «Аналітично-порівняльне правознавство». Розділ VII. Адміністративне право і процес; Фінансове право; Інформаційне право. Вип. 12 (87). 2023. С. 491-497. С. 493.

143. Позняк, Т. Б. Багаторівневі системи контролю доступу як елемент механізму захисту даних. Проблеми інформатизації. 2023. № 2. С. 155–163.

144. Поліщук, Т. В. Впровадження системи управління інформаційною безпекою (СУІБ) в органах публічної влади. Наукові праці НУ "Одеська юридична академія". 2022. № 3. С. 170–179.

145. Постанова КМУ № 518 від 19.06.2019 р. «Про затвердження Загальних вимог до кіберзахисту об’єктів критичної інфраструктури» (ред. від 07.09.2022 р.). Відомості Верховної Ради.

146. Постанова КМУ № 856 від 18.09.2019 р. Питання Міністерства цифрової трансформації (поточна ред. від 19.12.2024 р.). Відомості Верховної Ради.

147. Постанова КМУ № 885 від 16.10.2019 р. Деякі питання діяльності Міністерства культури та стратегічних комунікацій (поточна ред. від 24.09.2024 р.). Відомості Верховної Ради.

148. Пугачов, О. Проблеми забезпечення інформаційної безпеки України в сучасних умовах. Проблеми сучасних трансформацій. Серія: право, публічне управління та адміністрування. Вип. 12. 2024. 5 с. С. 3.

149. Рада національної безпеки і оборони України. Національний координаційний центр кібербезпеки посилює співпрацю із міжнародними виробниками кібер-технологій. 06.09.2020 р. Офіційний веб-портал РНБО.

150. Радіо Свобода. Загроза для Європи і світу: удари по енергетичній системі України можуть спричинити ядерну катастрофу. 24.11.2022 р. Офіційний веб-портал «Радіо Свобода».

151. Руденко, С. І. Інституціоналізація механізмів кіберзахисту в системі національної безпеки. Вісник Національного університету цивільного захисту. 2024. № 4. С. 80–90.

152. Русакевич, А. Інформаційна безпека в умовах воєнного стану у аспекти забезпечення інформаційних прав громадян. Держава та регіони. № 2

(80). 2023. С. 177-180. С. 178-179.

153. Рябчук, Л. І. Кіберстійкість державних інформаційних систем: організаційні механізми та їх оцінка. Безпека інформації. 2024. № 3. С. 67–78.

154. Савчук, В. Б. Моделювання загроз інформаційній безпеці для прийняття управлінських рішень. Безпека інформації. 2023. № 1. С. 40–49.

155. Саліюк-Кравченко, О. Г. Перспективи забезпечення національної енергетичної безпеки: реформування механізмів публічного управління та адміністрування. Public Management and Policy. 2025. № 9(13). С. 15–23.

156. Семенов, А. В. Управління інформаційною безпекою в державних інформаційно-комунікаційних системах: навчальний посібник. Київ : Освіта України, 2021. 290 с. (С. 120–145).

157. Семенюк, О. Класифікація таємної інформації. Інформація і право. № 1 (16). 2016. С. 44-51. С. 47.

158. Сидоренко, К. В. Концептуальні засади формування механізмів кіберзахисту в системі електронного урядування. Державне управління: удосконалення та розвиток. 2021. № 7. С. 1–10.

159. Сидоренко, О., Панченко, Г. Удосконалення комунікацій у публічному адмініструванні в контексті реалізації антикорупційної політики. Public Management and Policy. 2025. № 7-8(11-12). С. 180–189.

160. Ситник, Г. та ін. Системний підхід дослідження феномену інформація в державному управлінні. Проблеми сучасних трансформацій. Серія : право, публічне управління та адміністрування. № 11. 2024. 8 с. С. 4.

161. Сіленко, А. Реалізація цілей стратегії інформаційної безпеки України в умовах воєнного стану. Сучасні політичні процеси: глобальний та національний виміри : матеріали ІІ Міжнародної науково-практичної Інтернет-конференції (м. Одеса, 29 квіт. 2022 р.). МОН України та НОЮА. С. 28-34. С. 33.

162. Скулиш, Є. Д., Доронін, І. В. Протидія кіберзагрозам в публічному секторі: монографія. Київ : ДП "НТЦ", 2022. 390 с. (С. 225–255).

163. Слободянюк, О. В. Архітектура кібербезпеки в системі електронного урядування. Житомир : ЖДТУ, 2024. 375 с. (С. 85–105).

164. Степаненко, Р. С. Загрози для публічного сектору у 2025 році: аналіз кіберризиків та механізми захисту. Top Cyber Security Challenges for the Public Sector in 2025. 2025. С. 1–12.

165. Суспільне Новини. 7,5 млрд запитів за три доби — DDoS-атака на Monobank припинилася. 19.08.2024 р. Офіційний веб-портал Суспільне Новини.

166. Тимошенко, О. Г. Проблеми імплементації міжнародних договорів щодо кіберзлочинності в Україні. Міжнародне право. 2025. № 2. С. 115–125.

167. Ткаченко, А. Р. Роль центрів реагування на кіберінциденти (CERT) у механізмах публічного управління. Проблеми інформатизації та управління. 2024. № 2. С. 110–118.

168. Ткачук, А. П. Системи захисту інформації: принципи побудови та функціонування. Львів : Магнолія, 2020. 460 с. (С. 280–310).

169. Ткачук, Т. Сучасні загрози інформаційній безпеці держави : теоретико-правовий аналіз. Підприємництво, господарство і право. Серія : Інформаційне право. № 10. 2017. С. 182-186. С. 184.

170. Торічний, В. Особливості побудови державної системи інформаційної безпеки. Публічне управління і адміністрування в Україні. Серія : Державне управління у сфері державної безпеки та охорони громадського порядку. № 11. 2019. С. 183-185.

171. Угода про асоціацію між Україною, з однієї сторони, та Європейським Союзом, Європейським співтовариством з атомної енергії і їхніми державами-членами, з іншої сторони № 984_011 від 21.03.2014 р. (ред. від 30.11.2023 р.). Відомості Верховної Ради.

172. Угода про асоціацію між Україною, з однієї сторони, та Європейським Союзом, Європейським співтовариством з атомної енергії і їхніми державами-членами, з іншої сторони № 984_011 від 21.03.2014 р. (ред. від 30.11.2023 р.). Відомості Верховної Ради.

173. Указ Президента України «Про рішення Ради національної безпеки і оборони України від 14 травня 2021 року "Про Стратегію кібербезпеки України» № 447/2021. Відомості Верховної Ради.

174. Указ Президента України «Про рішення Ради національної безпеки

і оборони України від 15 жовтня 2021 року "Про Стратегію інформаційної безпеки» № 685/2021. Відомості Верховної Ради.

175. Указ Президента України № 187/2021 «Питання Центру протидії дезінформації» від 07.05.2021 р. Відомості Верховної Ради.

176. Укрінформ. Кібератака на Київстар: компанія Veon втратила майже $100 мільйонів. 18.01.2024 р. Офіційний веб-сайт Укрінформ.

177. Укрінформ. Укрпошта планує за два роки провести повну цифровізацію. 01.07.2021 р. Офіційний веб-портал Укрінформ.

178. Укрпошта. Політика конфіденційності. Офіційний веб-портал АТ «Укрпошта».

179. Укрпошта. Укрпошта встановить нову фронт-офісну систему замість старого програмного забезпечення 2006 року випуску. 26.10.2021 р. Офіційний веб-портал АТ «Укрпошта».

180. Укрпошта. Укрпошта першою серед компаній приєдналась до онлайн-платформи «Факторинг Хаб». 30.07.2020 р. Офіційний веб-портал АТ «Укрпошта».

181. Усенко, І. В. Механізми управління комунікаційними ризиками в умовах інформаційного протиборства. Стратегічна панорама. 2024. № 1. С. 95–105.

182. Федоренко, В. О. Кіберстійкість та управління інцидентами: механізми публічного реагування. Дніпро : Університет ім. А. Нобеля, 2023. 340 с. (С. 50–75).

183. Федоренко, Л. Д. Міжнародний досвід формування механізмів кібербезпеки публічного управління. Міжнародний науковий журнал "Інтернаука". 2023. № 1(131). С. 55–63.

184. Федорчук, Ю. В. Розробка та впровадження політик інформаційної безпеки в органах публічної влади. Публічне управління та адміністрування. 2023. № 6. С. 190–200.

185. Фролов, С. М. Забезпечення кібербезпеки публічного сектору: проблеми гібридної IT-інфраструктури. Security and privacy concerns challenge public sector's efforts to modernize. 2025. С. 1–9.

186. Харченко, В. А. Оцінка ефективності механізмів захисту від інсайдерських загроз у публічному секторі. Державне управління: удосконалення та розвиток. 2025. № 3. С. 1–11.

187. Хатнюк, Ю. Аналіз сучасних загроз національній безпеці України. Науковий вісник Міжнародного гуманітарного університету. Серія : Юриспруденція. 2020. № 43. С. 65-68. С. 67.

188. Цимбалюк, В., Бабінська, А. Правове регулювання інформаційної безпеки в Україні : проблеми теорії та практики. На часі. Серія : Адміністративне право і процес. № 2(8). 2014. С. 22-30.

189. Цимбалюк, О. П. Аудит та моніторинг стану інформаційної безпеки як елементи управлінського механізму. Науковий вісник публічного адміністрування. 2024. № 4. С. 70–80.

190. Чугунов, В. О. Глобальні процеси та національна кібербезпека: монографія. Київ : ЦНЛ, 2024. 445 с. (С. 300–330).

191. Чумак, В. Л. Використання Open Source Intelligence (OSINT) для моніторингу інформаційних загроз у публічному секторі. Науковий журнал "Інтернаука". 2024. № 10(148). С. 98–105.

192. Чумаченко, В. С. Управління ризиками інформаційної безпеки в контексті євроінтеграції. Збірник наукових праць Університету ДФС України. 2021. № 4. С. 200–208.

193. Шабетя, С., Несін, В. Правові питання забезпечення інформаційної безпеки особи в Україні. Юридичний науковий електронний журнал. № 4. 2021. С. 293-296. С. 294.

194. Швець, Д. В. Європейський досвід забезпечення інформаційної безпеки в публічному управлінні. Ужгород : Видавництво Закарпаття, 2022. 310 с. (С. 100–125).

195. Шевчук, М. До питання ґенези поняття інформаційної безпеки як складової національної безпеки. Науковий вісник Ужгородського національного ун-ту. Серія : Право. № 78 (2). С. 134-139.

196. Шевчук, П. М. Роль правоохоронних органів у системі забезпечення інформаційної безпеки публічного сектору. Науковий вісник Ужгородського

національного університету. Серія Право. 2022. Вип. 70. Т. 2. С. 150–158.

197. Шемчук, В. Механізм забезпечення інформаційної безпеки держави: теоретично-методологічні основи. Філософські та методологічні проблеми права. № 1 (17). 2019. С. 51-59.

198. Шопіна, І. Поняття інформаційної безпеки : концептуальні підходи до визначення. Науково-інформаційний вісник Івано-Франківського університету права ім. Короля Данила Галицького. Серія : Право. № 13 (25). 2022. С. 133-140. С. 135.

199. Шульга, Т. Д. Формування культури кібербезпеки серед державних службовців. Теорія та практика державного управління. 2023. Вип. 4(82). С. 140–150.

200. Юдкова, К. Принципи забезпечення інформаційної безпеки України. Юридичний вісник. Серія : Конституційне і адміністративне право. № 4 (41). 2016. С. 72-78. С. 75.

201. Яковенко, Л. Г. Методологічні підходи до оцінки зрілості кібербезпеки в органах публічного управління. Проблеми інформатизації. 2025. № 2. С. 45–55.

202. Ярмакі, Х., Музика, С. Класифікація конфіденційної інформації. Південноукраїнський правничий часопис. Правова система: теорія і практика. № 1. 2021. С. 94-98. С. 95.

203. Ярошенко, О. І. Глобальний огляд кібербезпеки: виклики 2025 року та механізми реагування. Global Cybersecurity Outlook 2025. 2025. С. 15–25.

204. Ярошенко, С. А. Міжнародне співробітництво у сфері кібербезпеки: механізми та форми взаємодії. Київ : Видавничий дім «Слово», 2021. 388 с. (С. 175–200).

205. Ahmed, N. M. The globalization of insecurity : how the international economic order undermines human and national security on a world scale. HAOL. Vol. 5. 2004. P. 113-126.

206. AIN.ua. Tranzzo реалізувала для «Укрпошти» P2P-перекази за номером телефону. 15.02.2022 р. Офіційний веб-портал AIN.ua. Режим доступу :

207. Alla, C., Valentina, V., Oleksandr, C., Yulia, O., Iryna, D., Kotliarov, V.

(2024). Impact of Artificial Intelligence on the Level of Socio-Economic Security of Ukraine in the Conditions of Current European Integration Challenges. In: Alareeni, B., Hamdan, A. (eds) Navigating the Technological Tide: The Evolution and Challenges of Business Model Innovation. ICBT 2024. Lecture Notes in Networks and Systems, vol 1082. Springer, Cham. https://doi.org/10.1007/978-3-031-67434-1_30.

208. Arvatz, A. The Battle for Your Computer. Israel and the Growth of the Global Cyber-Security Industry. Wiley. 2023. 320 p. С. 121.

209. Aslaner, M. Cybersecurity Strategies and Best Practices : A Comprehensive Guide to Mastering Enterprise Cyber Defense Tactics and Techniques. Packt Publishing. 2024. 252 p. С. 112.

210. BBC. Атака на Monobank. Що відомо. 18.08.2024 р. Офіційний веб-портал BBC. Режим доступу : .

211. BBC. Відключення електроенергії в Україні було хакерською атакою. 11.01.2017 р. Офіційний веб-портал BBC. 2 с.

212. Bigoli, H. Handbook of Information Security, Threats, Vulnerabilities, Prevention, Detection, and Management. Wiley. 2006. 1152 p.

213. Bjereld, U., Möller, U. 32 Swedish Foreign Policy: The Policy of Neutrality and Beyond (Chapter from The Oxford Handbook of Swedish Politics, ed. By J. Pierre. 2016. P. 433-446. С. 442.

214. Bondarenko, S. et al. The Legal Mechanisms for Information Security in the context of Digitalization. Journal of Information Technology Management. Vol. 2. 2022. JITM (Online). 17 p.

215. Bowen, P. et al. Information Security Guide For Government Executives. U.S. Department of Commerce. Technology Administration. Jan. 2007. 11 p. С. 7.

216. Brummer, A. The Great British Reboot. How the UK Can Thrive in a Turbulent World. Yale University Press. 2020. 256 p. С. 97-98.

217. Bytov V., Horbach L., Kotliarov V.O. Production as a Main Source of Consumer Goods to Society in the Current Environment. Economic Forum. 2022. Vol. 12, No. 3. P. 138–144. DOI: 10.36910/6775-2308-8559-2022-3-18.

218. Cankaya, E. C. Security and Privacy in Three States of Information. Intechopen Online Journal. Chapter : Security and Privacy From a Legal, Ethical, and Technical Perspective. Vol. 10. 2019. 23 p.

219. Cavelty, M.D., Wenger, A. Cyber Security Politics. Socio-Technological Transformations and Political Fragmentation. Taylor & Francis. 2022. 286 p.

220. Creemers, R. The Chinese Conception of Cybersecurity: A Conceptual, Institutional, and Regulatory Genealogy. Journal of Contemporary China. Vol. 33. (146). 2024. P. 173-188. C. 181.

221. Cremer, F. et al. Cyber risk and cybersecurity: a systematic review of data availability. Geneva Pap Risk Insur Issues Pract. Feb 17;47(3). 2022. P. 698–736. C. 700-701

222. Cuihong, K. Cybersecurity in the Chinese Context. Changing Concepts, Vital Interests, and Prospects for Cooperation. World Century Publishing Corporation and Shanghai Institutes for International Studies China Quarterly of International Strategic Studies, Vol. 1, No. 3. 2015. P. 471–496. C. 480.

223. Daricili, A. B., Erendor, M. E. The Cyber Security Strategy of Israel. Magazine Questions of History. Vol. 11 (3). 2021. P. 233-246. C. 242.

224. Darwish, A., Romaniuk, S. N. Cyber security in the French Republic. Routledge Companion to Global Cyber-Security Strategy. Vol. 12. Dec. 2020. P. 62-72. C. 69.

225. Davies, P.H.J. Intelligence and Government in Britain and the United States : A Comparative Perspective [2 Volumes]. :Bloomsbury Publishing. 2012. 864 p. C. 139.

226. Deloitte. Strategies for Data Compliance in China. October 2024. Deloitte Digital official survey. Режим доступу :

227. DigiChina. Stanford University. National Security Law of the People’s Republic of China. Stanford University official website. 37 p.

228. DigiChina. Stanford University. Translation: Cybersecurity Law of the People’s Republic of China (Effective June 1, 2017). Stanford University official website. Режим доступу :

229. Dziundziuk, V. et al. State Information Security Policy (Comparative Legal Aspect). Cuestiones Políticas. Vol. 39 (71). 2021. P. 166-186. C. 178.

230. EurLex. Consolidated text: Directive (EU) 2022/2555 of the European Parliament and of the Council of 14 December 2022 on measures for a high common level of cybersecurity across the Union, amending Regulation (EU) No 910/2014 and Directive (EU) 2018/1972, and repealing Directive (EU) 2016/1148 (NIS 2 Directive) (Text with EEA relevance)Text with EEA relevance. EurLex official website. 23 p.

231. European Commission. EU Cybersecurity Strategy 2020. EC official website. 55 p.

232. European Commission. EU vs Disinfo. EUD official website. 2 p.

233. European Cybersecurity Competence Centre and Network (ECCC). Enhanced EU-Ukraine cooperation in Cybersecurity. 08.12.2023. ECCC official website.

234. European Investment Bank (EIB). Ukrposhta modernization and digitalization. EIB official website. 27 Feb 2020. Режим доступу : https://www.eib.org/en/projects/all/20170553?form=MG0AV3&form=MG0AV3

235. Fahey, E. The evolution of EU–US cybersecurity law and policy: on drivers of convergence. Journal of European Integration. Vol. 46. (7). 2024. P. 1073-1088. C. 1080.

236. Farrell, H., Newman, A. L. Of Privacy and Power : The Transatlantic Struggle Over Freedom and Security. Princeton University Press. 2021. 248 p.

237. Farshadkhah, S., Maynard-Patrick, S. Role of Human Resource Management in Information Security Compliance Behavior. Association for Information Systems AIS Electronic Library (AISeL). MWAIS 2024 Proceedings. 29. Peoria, Illinois, May 16-17, 2024. 5 p. C. 3.

238. Fazlida, M.R., Said, J. Information Security: Risk, Governance and Implementation Setback. Procedia Economics and Finance. Vol. 28. 2015. P. 243-248. C. 245.

239. Fitzgerald, T. Information Security Governance Simplified. From the Boardroom to the Keyboard. CRC Press. 2016. 431 p.

240. Fitzgerald, T. Information Security Governance Simplified. From the

Boardroom to the Keyboard. CRC Press. 2016. 431 p. C. 133.

241. Foster, H. H. The Relation and Correlation of Freedom and Security. West Virginia Law Review. Vol. 58 (4). 1956. P. 325-351. C. 333-334.

242. Freilich, C. D. et al. Israel and the Cyber Threat. How the Startup Nation Became a Global Cyber Power. Oxford University Press. 2023. 422 p. C. 177-178.

243. Goodman, S. et al. Information Security Policy, Processes, and Practices. Taylor & Francis. 2016. 288 p. C. 139-140.

244. Government of Canada. Access to Information Act (R.S.C., 1985, c. A-1). Government of Canada official website. 10 p.

245. Government of Canada. THE CONSTITUTION ACTS 1867 to 1982. Government of Canada official website. 11 p.

246. Grama, J. L. Legal and Privacy Issues in Information Security. Jones & Bartlett Learning, LLC. 2020. 552 p.

247. Guariniello, C., DeLaurentis, D. Communications, Information, and Cyber Security in Systems-of-Systems: Assessing the Impact of Attacks through Interdependency Analysis. Procedia Computer Science. Vol. 28. 2014. p. 720-727. C. 725.

248. Guariniello, C., DeLaurentis, D. Communications, Information, and Cyber Security in Systems-of-Systems: Assessing the Impact of Attacks through Interdependency Analysis. Procedia Computer Science. Vol. 28. 2014. p. 720-727. C. 726.

249. Hung (Bosco), H. T. Multilateral cooperation in building critical infrastructure security and resilience: case of American deterrence of Chinese cyberthreats. Journal of Cyber Policy. 2025. P. 1-26. C. 14.

250. ISO. ISO/IEC 27001:2022. Information security, cybersecurity and privacy protection — Information security management systems — Requirements. 2022. ISO official website. 15 p.

251. Israeli National Security Archive. Government of Israel, Resolution No. 3611, "Advancing National Cyberspace Capabilities," August 7, 2011. Unclassified. INSA official website. 7 p.

252. IT-Enterprise. В АТ «Укрпошта» відзначили стратегічне значення цифровізації, яку проводить команда IT-Enterprise. 10.05.2023 р. Офіційний веб-портал IT-Enterprise.

253. Jewish Virtual Library. A project of AICE. Basic Laws of Israel: Defense Service Law (1986). JWL official website. 12 p.

254. Jiang, M. Cybersecurity Policies in China. CyberBRICS. University of North Carolina at Charlotte. Vol. 1. 2021 p. 183-226. С. 190-191.

255. Kamariotou, M., Kitsios, F. Information Systems Strategy and Security Policy: A Conceptual Framework. Electronics. Vol. 12 (382). 2023. 12 p. С. 5-7.

256. Kaypak, S. Security Understanding of a New Dimension in the Globalization Process and Environmental Effects. Afyon Kocatepe University Journal of Social Sciences. Vol. 21 (3). 2019. P. 855-868.

257. Kiefer, K. Information Security. A Legal, Business, and Technical Handbook. American Bar Association. 2004. 82 p.

258. Kotliarov V.O. Strategic Security of the Enterprise. 3rd International Conference on Corporation Management (ICCM-2023). 29.06.2023. Estonia. URL: https://conf.scnchub.com/index.php/ICCM/ICCM-2023/paper/view/547

259. Kotliarov V.O., Kovalchuk O.V., Kovalchuk O.V., Kovalchuk T.V., Kovalchuk O.V. Study of Structural Imbalances in Agricultural Engineering. E3S Web of Conferences. 2022. Vol. 363. Article 01037. URL: https://doi.org/10.1051/e3sconf/202236301037.

260. Legislation. gov. Data Protection Act 2018. UK legislation official website. Режим доступу :

261. Liedtke, T. Information Security. Opportunities and Limitations. Springer. 2024. 207 p. С. 109-110.

262. Long, W. J., Quek, M. P. Personal data privacy protection in an age of globalization: the US-EU safe harbor compromise. Journal of European Public Policy. Vol. 9 (3). 2002. P. 325-344.

263. Markopoulou, D., Papakonstantinou, V. The regulatory framework for the protection of critical infrastructures against cyberthreats: Identifying shortcomings and addressing future challenges: The case of the health sector in

particular. Computer Law & Security Review. Vol. 41. 2021. P. 105-502. C. 213.

264. Martinkauppi, L. B. et al. On the Design and Performance of Chinese OSCCA-approved Cryptographic Algorithms. DIVA Portal. Vol. 3. 2020. 6 p. C 4.

265. Matlary, J. H., Johnson, R. The United Kingdom's Defence After Brexit. Britain's Alliances, Coalitions, and Partnerships. Springer International Publishing. 2018. 261 p. c. 101.

266. Merkow, M. S. Information Security : Principles and Practices. Pearson Education. 2014. 368 p. C. 223.

267. Paananen, H. et al. State of the art in information security policy development. Computers & Security. Vol. 88. 2020. P. 101-608.

268. Reznik N.P., Kotliarov V.O. Information Security: Challenges to the Global Information Society. ICEAF-2023. 15.12.2023. Estonia. URL: https://conf.scnchub.com/index.php/ICEAF/ICEAF-2023/paper/view/696.

269. Reznik N.P., Kotliarov V.O. Аспекти державної системи стратегічного планування національної безпеки України. III International Scientific and Practical Conference «Collective Thinking: Unifying Scientific Approaches in Multifaceted Research». 29.11–01.12.2023. Амстердам, Нідерланди. URL: https://isu-conference.com/en/archive/collective-thinking-unifying-scientific-approaches-in-multifaceted-research; PDF.

270. Reznik N.P., Kotliarov V.O. Особливості системи забезпечення стратегічної безпеки компанії. II International Scientific and Practical Conference «Modern Approaches to Problem Solving in Science and Technology». 15–17.11.2023. Варшава, Польща. URL: https://isu-conference.com/en/archive/modern-approaches-to-problem-solving-in-science-and-technology; PDF.

271. Ripsman, N. M., Paul, T. V. Introduction: National Security State in the Era of Globalization. Oxford Academic Journal. Vol. 2. 2010. P. 3-19.

272. Roberts, M. J. The Cyber Threat and Globalization: The Impact on U.S. National and International Security. By Jack A. Jarmon and Pano Yannakogeorgos. Lanham, MD: Rowman & Littlefield, 2018. Strategic Security. Vol. 11 (4). 2019. P. 85-88. C. 86.

273. Rogovskii, I., Kotliarov, V., Bondarenko, V., Havrylyuk, V., Gaojiang,

C., Zehao, L. (2024). Engineering and Security Management of Smart Technology of Agrotronics of Crop Production. In: Mansour, N., Bujosa Vadell, L.M. (eds) Green Finance and Energy Transition. Contributions to Finance and Accounting. Springer, Cham. https://doi.org/10.1007/978-3-031-75960-4_10

274. Sahid, A. et al. Strategic Information System Agility. From Theory to Practices. Emerald Publishing Limited. 2020. 208 p. C. 73-74.

275. Shumaker, L. U.S. actions against China's Huawei : rep. by A. Alper. Reuters, 2022. 7 p.

276. Stitzlein, S. M. American Public Education and the Responsibility of Its Citizens Supporting Democracy in the Age of Accountability. Oxford University Press. 2017. 224 p. C. 95-97.

277. Sveriges Riksdag. Kungörelse (1974:152) om beslutad ny regeringsform. ustitiedepartementet L6. Sveriges Riksdag official website.

278. Swissinfo.ch. У Швейцарії стартував збір підписів під «ініціативою про нейтралітет». 16. 11.2022 р. Офіційний веб-портал Swissinfo.ch. 3 с. С. 2.

279. Szczepaniuk, E., K. et al. Information security assessment in public administration. Computers & Security. Vol. 90. 2020. P. 101-709. C. 523.

280. Tabansky, L., Ben Israel, I. Cybersecurity in Israel. Springer International Publishing. 2015. 77 p. C. 23-24.

281. Talimonchik, V. Legal Aspects of International Information Security. InteChopen (Online). Vol. 4. 2019. InteChopen official website.

282. Tanwar, R. et al. Information Security and Optimization. CRC Press. 2020. 224 p. C. 78.

283. The Government Secretary. Government Resolution No. 2444 of February 15, 2015. 33rd Government of Israel. Resolution: Advancing the National Preparedness for Cyber Security. The Government Secretary official website. Режим доступу :

284. The White House. Executive Order 14028 «Improving the Nation's Cybersecurity» 2021. WH official website.

285. The defense industrial complex as the basis of the national security of the state / Dmytro Zhuravlov, Viktoriia Anishchuk, Denys Chyzhov, Volodymyir

Pashynskyi, Mykola Zaitsev // Journal of Security and Sustainability Issues Volume 9 Number 3, March, 2020, p. 829-845 (Scopus) / URL: https://doi.org/10.9770/jssi.2020.9.3(9)

286. Tschider, C. A. International Cybersecurity and Privacy Law in Practice. Wolters Kluwer. 2023. 536 p.

287. UK Cyber Security Council. The CyberFirst Programme. UK CSC official website.

288. UK HM Government. UK National Cyber Security Strategy 2022-2030. HM official website.

289. UNODC. Israeli Computer Law of 1995. UNODC official website.

290. Urgessa, W. F. Multilateral cybersecurity governance: Divergent conceptualizations and its origin. Computer Law & Security Review. Vol. 36. 2020. 15 p. C. 12-13.

291. US Congress. Cybersecurity and Infrastructure Security Agency Act 2018. USC official website.

292. Walters, R., Novak, M. Cyber Security, Artificial Intelligence, Data Protection & the Law. Springer Nature Singapore. 2021. 458 p.

293. Ward, D. Public Security in Modern China. NCJRS Virtual Library. April 1997. 5 p. C. 3.

294. Whitman, M. E., Mattord, H. J. Principles of Information Security. Course Technology, Cengage Learning. 2012. 619 p. C. 217.

295. Wilkowski, M. Information (Filter) Bubbles and other Factors Conducive to Disinformation and Manipulation. Hi-Story Lessons covered by ENRS. 2023. 8 p. C. 5.

296. Workman, M. Information Security Management. Jones & Bartlett Learning. 2021. 462 p. C. 319-320.

297. Wright, M., Kakalik, J. S. Information Security : Contemporary Cases. Jones and Bartlett. 2009. 214 p.

298. ZakonOnline. Акт № 998_115 від 08.11.1815 Акт щодо визнання та гарантії постійного нейтралітету Швейцарії та недоторканності її території. Офіційний веб-портал ZakonOnline.

299. Zimmer, B. The protection of net neutrality in Canada. Report of the Standing Committee on Access to Information, Privacy and Ethics. House of Commons Canada. 42nd Parliament, 1st Session. May 2018. 36 p. C. 11.

300. Züfle, N. The Growth of Uncertainty After the End of the Cold War and Its Impact on the Security Environment of States. GRIN Verlag. 2011. 45 p.

ДОДАТКИ

СПИСОК ПУБЛІКАЦІЙ ЗА ТЕМОЮ ДИСЕРТАЦІЇ
Наукові праці, в яких опубліковані основні наукові результати дисертації

Монографії:

37. Загородня А.С., Котляров В. Управління економічною безпекою: стратегічні цілі та механізми реалізації. Київ: Національний університет біоресурсів і природокористування, 2024. 200 с. *Особистий внесок: розроблено механізми управління економічною безпекою в системі публічного управління.*

Статті у наукових періодичних виданнях, проіндексованих у базах даних Web of Science Core Collection та/або Scopus:

38. Zbarsky, V.K., Reznik, N.P., Ostapchuk, A.D., Alekseieva, K.A., Kotliarov, V.O. (2025). Institutional and Informational Prerequisites of Secure Development of Farms in the Agrarian Economy Model of Ukraine. In: Alareeni, B., Elgedawy, I. (eds) Opportunities and Risks in AI for Business Development. Studies in Systems, Decision and Control, vol 546. Springer, Cham. https://doi.org/10.1007/978-3-031-65207-3_53. *Особистий внесок: розроблено концептуальну модель інформаційної безпеки аграрних господарств, адаптованої до умов цифрової трансформації та європейських стандартів.*

39. Rogovskii, I., Kotliarov, V., Bondarenko, V., Havrylyuk, V., Gaojiang, C., Zehao, L. (2024). Engineering and Security Management of Smart Technology of Agrotronics of Crop Production. In: Mansour, N., Bujosa Vadell, L.M. (eds) Green Finance and Energy Transition. Contributions to Finance and Accounting. Springer, Cham. https://doi.org/10.1007/978-3-031-75960-4_10 *Особистий внесок: формалізовано ризики кібербезпеки в агротехнологічних системах та розробці алгоритмів управління інформаційними загрозами в агровиробництві.полягає у формалізації ризиків інформаційної безпеки в агротроніках.*

40. Cherep A., Voronkova V., Cherep O., Ohrenych Y., Dashko I., Kotliarov V. (2024). Impact of Artificial Intelligence on the Level of Socio-Economic Security of Ukraine in the Conditions of Current European Integration Challenges. In: Alareeni, B., Hamdan, A. (eds) Navigating the Technological Tide: The Evolution and Challenges of Business Model Innovation. ICBT 2024. Lecture Notes in Networks and Systems, vol 1082. Springer, Cham. https://doi.org/10.1007/978-3-031-67434-1_30. *Особистий внесок: визначено критичні точки впливу штучного інтелекту на соціально-економічну стабільність України та розробці рекомендацій щодо інформаційного захисту.*

41. Kotliarov V.O., Kovalchuk O.V., Kovalchuk O.V., Kovalchuk T.V., Kovalchuk O.V. Study of Structural Imbalances in Agricultural Engineering. E3S Web of Conferences. 2022. Vol. 363. Article 01037. URL:

https://doi.org/10.1051/e3sconf/202236301037. *Особистий внесок: виявлено інформаційні дисбаланси у системах агроінжинірингу та обґрунтуванні напрямів їх оптимізації з точки зору стратегічної безпеки.*

Статті у наукових виданнях, включених до Переліку наукових фахових видань України:

42. Котляров В.О. Еволюція міжнародно-політичної взаємодії у сфері інформаційних відносин. Публічне управління і адміністрування в Україні. 2023. Вип. 37. С. 76–81. DOI: 10.32782/pma2663-5240-2023.37.14

43. Котляров В.О. Комплексний підхід щодо розуміння інформаційної безпеки. Публічне управління і адміністрування в Україні. 2023. Вип. 38. С. 168–172. DOI https://doi.org/10.32782/pma2663-5240-2023.38.30

44. Котляров В.О. Особливості категорії «Інформаційна безпека» у міжнародному контексті. Наукові праці МАУП. Політичні науки та публічне управління. 2023. № 4(70). С. 21–26. DOI: 10.32689/2523-4625-2023-4(70)-3

45. Котляров В.О. Система забезпечення інформаційної безпеки України. Наукові праці МАУП. Політичні науки та публічне управління. 2024. № 2(74). С. 40–44. DOI: 10.32689/2523-4625-2024-2(74)-6

46. Котляров В.О. Інформаційне забезпечення безпеки вітчизняної та світової спільноти. Наукові праці МАУП. Політичні науки та публічне управління. 2024. № 1(73). С. 45–52. DOI: 10.32689/2523-4625-2024-1(73)-6

47. Котляров В.О. Теоретичні засади сутності та концепції інформаційної безпеки. Наукові перспективи. 2023. № 6(36). С. 131–142. DOI: 10.52058/2708-7530-2023-6(36)-131-142

48. Котляров В.О. Формування державної політики кібергігієни. Наукові перспективи. 2025. № 7(61). С. 162–174. DOI: 10.52058/2708-7530-2025-7(61)-162-174

49. Котляров В.О. Категоріальний апарат інформаційної безпеки. Суспільство та національні інтереси. 2025. № 8(16). С. 615–629. DOI: 10.52058/3041-1572-2025-8(16)-615-629

50. Котляров В.О. Стратегічні цілі інформаційної безпеки: державне планування та механізми моніторингу ефективності. Національні інтереси України. 2025. № 8(13). С. 903–914. DOI: 10.52058/3041-1793-2025-8(13)-903-914%20

51. Котляров В.О. Інформаційна безпека України: цілі, механізми та адаптація до стандартів ЄС і НАТО. Наукові інновації та передові технології. 2025. № 8(48). С. 180–192. DOI: 10.52058/2786-5274-2025-8(48)-180-192

52. Котляров В.О. Інформаційна безпека як система правовідносин: теоретико-правовий вимір. Актуальні питання у сучасній науці. 2025. № 8(38). С. 245–259. DOI: 10.52058/2786-6300-2025-8(38)-245-259

53. Котляров В.О. Механізми раннього виявлення інформаційних атак: роль штучного інтелекту в прогнозуванні. Успіхи і досягнення у науці. 2025. №

8(18). С. 443–455. DOI: 10.52058/3041-1254-2025-8(18)-443-455

54. Котляров В.О. Інформаційна безпека в умовах глобальної взаємозалежності: міжнародно-правовий контекст та стратегічні практики. Успіхи і досягнення у науці. 2025. № 7(17). С. 474–486. DOI: 10.52058/3041-1254-2025-7(17)-474-486

55. Котляров В.О. Механізми управління репутаційними ризиками у державній інформаційній політиці. Суспільство та національні інтереси. 2025. № 9(17). С. 624–637. DOI: 10.52058/3041-1572-2025-9(17)-624-637

56. Котляров В.О. Методологічні засади дослідження інформаційної безпеки в умовах трансформаційних викликів. Наукові інновації та передові технології. 2025. № 9(49). С. 187–199. DOI: 10.52058/2786-5274-2025-9(49)-187-199

57. Котляров, В.О. Кібертероризм як загроза міжнародній безпеці. Наукові праці Міжрегіональної Академії управління персоналом. Політичні науки та публічне управління, 2023, 5(71), 46-54. DOI: 10.32689/2523-4625-2023-5(71)-6

58. Котляров В.О. Правовий механізм забезпечення інформаційної безпеки: структура, принципи та інституційна модель України. Наукові перспективи. 2025. № 8 (62). С. 907-919. DOI: 10.52058/2708-7530-2025-8(62)-907-919.

59. Котляров В.О. Проблеми інформаційної боротьби у контексті забезпечення національних інтересів. Наукові інновації та передові технології. 2023, № 1(15), DOI: 10.52058/2786-5274-2023-1(15)-499-51

60.

Статті в інших періодичних виданнях України

61. Котляров, В.О. Стратегічне управління інформаційною безпекою України. Київський економічний науковий журнал, 2024, 6, 66-69. DOI: 10.32782/2786-765X/2024-6-9

62. Котляров В.О. Стратегічне управління безпекою організацій. Mechanism of an Economic Regulation, 2024, 1 (103), 41-45. DOI: 10.32782/mer.2024.103.06

63. Котляров В.О. Особливості державної системи стратегічного планування національної безпеки в умовах інформатизації суспільства. Український журнал прикладної економіки та техніки. Том 7, № 4, 2022, С. 225–233. DOI: 10.36887/2415-8453-2022-4-33.

64. Котляров В.О. Стратегічна безпека підприємства: підходи, особливості, механізм та проблеми забезпечення. Український журнал прикладної економіки та техніки. 2022. №3. 214-222 pp. DOI: 10.36887/2415-8453-2022-3-29.

65. Котляров В.О. Поняття стратегічного управління національною безпекою. Український журнал прикладної економіки та техніки. 2023. №1. 159-165 pp. DOI: 10.36887/2415-8453-2023-1-23

66. Котляров В.О. Кібертероризм як загроза міжнародній безпеці. Укра-

їнський журнал прикладної економіки та техніки. 2023. №2. 314-321 pp. DOI: 10.36887/2415-8453-2023-2-45

67. Bytov V., Horbach L., Kotliarov V.O. Production as a Main Source of Consumer Goods to Society in the Current Environment. Economic Forum. 2022. Vol. 12, No. 3. P. 138–144. DOI: 10.36910/6775-2308-8559-2022-3-18. *Особистий внесок: розроблено аналітичну модель взаємозв'язку між виробничими процесами та рівнем забезпечення суспільства споживчими товарами, з урахуванням інформаційно-економічних чинників сучасного середовища.*

68. Котляров В.О. Механізм стратегічного управління економічною безпекою підприємства. Наука та освіта як основа модернізації світоустрою, 2023, № 25-01, с. 183–194. DOI: 10.30890/2709-2313.2023-25-00-024

69. Котляров, В.О. Принципи управління безпекою організацій. Mechanism of an Economic Regulation, 2023, 4 (102), 25-28. DOI: 10.32782/mer.2023.102.04

Тези конференцій:

70. Kotliarov V.O. Strategic Security of the Enterprise. 3rd International Conference on Corporation Management (ICCM-2023). 29.06.2023. Estonia. URL: https://conf.scnchub.com/index.php/ICCM/ICCM-2023/paper/view/547

71. Reznik N.P., Kotliarov V.O. Information Security: Challenges to the Global Information Society. ICEAF-2023. 15.12.2023. Estonia. URL: https://conf.scnchub.com/index.php/ICEAF/ICEAF-2023/paper/view/696. *Особистий внесок: класифіковано глобальні виклики інформаційній безпеці та формуванні аналітичної моделі оцінки їх впливу на міжнародні інститути.*

72. Reznik N.P., Kotliarov V.O. Особливості системи забезпечення стратегічної безпеки компанії. II International Scientific and Practical Conference «Modern Approaches to Problem Solving in Science and Technology». 15–17.11.2023. Варшава, Польща. URL: https://isu-conference.com/en/archive/modern-approaches-to-problem-solving-in-science-and-technology; PDF. *Особистий внесок: розроблено структурну модель корпоративної інформаційної безпеки з урахуванням репутаційних ризиків.*

73. Reznik N.P., Kotliarov V.O. Аспекти державної системи стратегічного планування національної безпеки України. III International Scientific and Practical Conference «Collective Thinking: Unifying Scientific Approaches in Multifaceted Research». 29.11–01.12.2023. Амстердам, Нідерланди. URL: https://isu-conference.com/en/archive/collective-thinking-unifying-scientific-approaches-in-multifaceted-research; PDF. *Особистий внесок: змодельовано інформаційний компонент державної системи стратегічного планування та обґрунтуванні його ролі в національній безпеці.*

НАЦІОНАЛЬНЕ АГЕНТСТВО КВАЛІФІКАЦІЙ
Юридична адреса: вул. Антоновича, 180, м. Київ, 03150
Адреса для листування: вул. Соломʼянська, 1, м. Київ, 03035
Код ЄДРПОУ 43344220; • Тел.: +38(068) 046 70 86
• nqa@nqa.gov.ua • https://nqa.gov.ua

22.01.2025 № 01/0101-06/1647

ДОВІДКА

про впровадження результатів докторської дисертації

Котлярова Валерія Олександровича

на тему : «Механізми інформаційної безпеки держави»

Національне агентство кваліфікацій (далі – Агентство) засвідчує, що результати наукового дослідження, викладені у докторській дисертації Котлярова Валерія Олександровича на тему «Механізми інформаційної безпеки держави», були впроваджені у діяльність Агентства в таких напрямах:

1. Оцінка ризиків у сфері кваліфікаційної безпеки:

Інтегровано методику класифікації інформаційних загроз та ризиків в регламенти роботи із даними Реєстру кваліфікацій.

2. Модернізація аналітичних систем:

Алгоритми прогнозування загроз, запропоновані в дисертації, стали основою вдосконалення цифрової інфраструктури аналітичних модулів.

3. Оновлення професійних стандартів:

Наукові положення використано при оновленні кваліфікаційних вимог для фахівців з кібербезпеки, зареєстрованих у Національному реєстрі кваліфікацій.

4. Аналітична підтримка державної політики:

Висновки дисертації включено до експертних матеріалів щодо гармонізації українських кваліфікаційних норм з європейськими рамками.

Голова **Юрій БАЛАНЮК**

ДОВІДКА

про впровадження результатів докторської дисертації

Котлярова Валерія Олександровича

на тему: «Інформаційна безпека держави: стратегічні цілі та механізми реалізації»

Результати докторської дисертації на тему «Інформаційна безпека держави: стратегічні цілі та механізми реалізації» були впроваджені у діяльність Департаменту кадрової політики Міністерства оборони України. Зокрема, розроблені у межах дослідження автора рекомендації використані для удосконалення механізмів захисту інформаційного простору департаменту та протидії інформаційним загрозам в умовах воєнного стану.

Департамент кадрової політики Міністерства оборони України може рекомендувати іншим структурним підрозділам, державним підприємствам, органам державної влади та місцевого самоврядування звертатися до положень зазначеного дослідження під час розробки стратегічних документів та реалізації заходів у сфері інформаційної безпеки. Практичне застосування результатів сприятиме підвищенню рівня захисту інформаційного середовища.

Забезпечення інформаційної безпеки в умовах воєнного стану потребує особливої уваги до норм законодавства, що регулюють відповідну сферу. Впровадження результатів дисертаційного дослідження Котлярова Валерія Олександровича узгоджується з положеннями Законів України «Про інформацію», «Про національну безпеку України» та «Про правовий режим воєнного стану», що визначають основи інформаційної безпеки, повноваження органів державної влади у сфері її забезпечення та особливості правового регулювання в умовах збройного конфлікту.

Директор Департаменту кадрової політики
Міністерства оборони України
полковник **Марк АНДРУСЯК**

ДОВІДКА

про впровадження результатів докторської дисертації

Котлярова Валерія Олександровича

на тему : «Інформаційна безпека держави: стратегічні цілі та механізми реалізації»

Результати докторської дисертації на тему «Інформаційна безпека держави: стратегічні цілі та механізми реалізації» були впроваджені у діяльність Національної акціонерної компанії «Надра України». Зокрема, розроблені у межах дослідження рекомендації використані для удосконалення механізмів захисту інформаційного простору національної акціонерної компанії, забезпечення кіберстійкості державних підприємств та протидії інформаційним загрозам в умовах воєнного стану.

Національної акціонерної компанії «Надра України рекомендує іншим державним підприємствам, органам державної влади та місцевого самоврядування звертатися до положень зазначеного дослідження під час розробки стратегічних документів та реалізації заходів у сфері інформаційної безпеки. Практичне застосування результатів сприятиме підвищенню рівня захисту інформаційного середовища.

Забезпечення інформаційної безпеки в умовах воєнного стану потребує особливої уваги до норм законодавства, що регулюють відповідну сферу. Впровадження результатів дисертаційного дослідження Котлярова Валерія Олександровимч узгоджується з положеннями Законів України «Про інформацію», «Про національну безпеку України» та «Про правовий режим воєнного стану», що визначають основи інформаційної безпеки, повноваження органів державної влади у сфері її забезпечення та особливості правового регулювання в умовах збройного конфлікту.

Голова Правління
НАК «Надра України» **Новіков В.В.**

МІНІСТЕРСТВО ОБОРОНИ УКРАЇНИ
ЦЕНТРАЛЬНИЙ
НАУКОВО-ДОСЛІДНИЙ ІНСТИТУТ
ЗБРОЙНИХ СИЛ УКРАЇНИ
проспект Повітряного флоту 28-б
м. Київ, 03049
Тел.: (044) 520-19-44
E-mail: crsi@post.mil.gov.ua
код згідно з ЄДРПОУ 08138347
від "07" 11 2025 р. № 172/2950

ДОВІДКА

про впровадження результатів докторської дисертації Котлярова Валерія Олександровича на тему: "Механізми інформаційної безпеки держави"

У межах науково-дослідної діяльності Центрального науково-дослідного інституту Збройних Сил України, спрямованої на вдосконалення системи інформаційної безпеки в умовах гібридних загроз, були використані результати докторської дисертації Котлярова Валерія Олександровича на тему "Механізми інформаційної безпеки держави".

Зокрема, дисертаційні положення були застосовані при:

- розробці методичних підходів до оцінки інформаційних ризиків у військовій сфері;
- моделюванні механізмів реагування на деструктивні інформаційні впливи в системах управління оборонного сектору;
- формуванні рекомендацій щодо підвищення кіберстійкості інформаційних систем Збройних Сил України;
- удосконаленні науково-методичних засад захисту критичних військових інформаційних ресурсів.

Результати дослідження були інтегровані в аналітичні матеріали, що використовуються при підготовці наукових висновків, оперативних завдань, експертних оцінок та рекомендацій для органів військового управління.

Практичне застосування дисертації сприяло:

- уточненню класифікації загроз у сфері військової інформаційної безпеки;
- посиленню міжвідомчої координації у питаннях кіберзахисту;
- формуванню стратегічних орієнтирів для розвитку інформаційної компоненти оборонної політики.

Таким чином, наукові результати дисертації Котлярова В.О. були впроваджені в науково-аналітичну діяльність ЦНДІ ЗС України, що підтверджує їхню актуальність, прикладну значущість та відповідність сучасним викликам у сфері національної безпеки.

Заступник начальника Центрального науково-дослідного інституту
Збройних Сил України з наукової роботи
доктор військових наук, професор
Заслужений працівник науки і техніки України
полковник Олег СЕМЕНЕНКО

Прим. № __

АДМІНІСТРАЦІЯ ДЕРЖСПЕЦЗВ'ЯЗКУ

Департамент захисту
критичної інфраструктури
ДКІ Адміністрації Держспецзв'язку

вул. Солом'янська, 13, м. Київ, 03110,
тел. (044) 281-67-65,
e-mail: dzki@cip.gov.ua,
web: cip.gov.ua
Код ЄДРПОУ 34620942

від 12.11 2025 р. № 1451
На № _____ від _____ 20__ р.

ДОВІДКА

про впровадження результатів докторської дисертації з державного управління
Котлярова Валерія Олександровича
на тему: «Механізми інформаційної безпеки держави»

У межах діяльності Департаменту захисту критичної інфраструктури Адміністрації Державної служби спеціального зв'язку та захисту інформації України, під час підготовки щорічної оцінки ризиків та загроз у сфері критичної інфраструктури, було здійснено аналіз наукових напрацювань, що стосуються стратегічного реагування на гібридні загрози, захисту інформаційного простору та забезпечення кіберстійкості державних і приватних суб'єктів.

Зокрема, результати докторської дисертації з державного управління Котлярова Валерія Олександровича на тему «Механізми інформаційної безпеки держави» були використані як аналітична та методологічна основа для формування окремих положень оцінки ризиків, зокрема:

- класифікації актуальних інформаційних загроз у контексті гібридної війни;
- моделювання механізмів реагування на деструктивні інформаційні впливи;
- формування рекомендацій щодо кіберзахисту об'єктів критичної інфраструктури;
- розробки пропозицій з інтеграції ризик-менеджменту в управлінські процеси підприємств.

Дисертаційні положення були враховані при оцінці загроз для об'єктів державного управління, телекомунікацій, транспорту, охорони здоров'я та інших секторів, що мають критичне значення для функціонування держави.

Практичне застосування результатів дисертації дозволило:

- підвищити точність і структурованість аналізу ризиків;

- посилити стратегічну частину оцінки загроз;
- сформувати дієві рекомендації для суб'єктів критичної інфраструктури щодо підвищення стійкості до інформаційних атак.

Таким чином, наукові результати дисертації Котлярова В.О. були впроваджені в аналітичну та стратегічну діяльність Адміністрації Держспецзв'язку, що підтверджує їхню актуальність, прикладну значущість та відповідність сучасним викликам у сфері національної безпеки.

Директор Департаменту Валерій НОВАК