МІНІСТЕРСТВО ОСВІТИ І НАУКИ УКРАЇНИ

ЗВО «ВІДКРИТИЙ МІЖНАРОДНИЙ УНІВЕРСИТЕТ РОЗВИТКУ ЛЮДИНИ «УКРАЇНА»

Кваліфікаційна наукова
праця на правах рукопису

ДРИГА ДМИТРО АНДРІЙОВИЧ

УДК 351:004.056

ДИСЕРТАЦІЯ

ДЕРЖАВНЕ РЕГУЛЮВАННЯ ІНФОРМАЦІЙНОЇ БЕЗПЕКИ В УМОВАХ СУЧАСНИХ ЦИВІЛІЗАЦІЙНИХ ВИКЛИКІВ

281 «Публічне управління та адміністрування»

Подається на здобуття наукового ступеня доктора філософії

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

Науковий керівник
ДАБІЖА Віра Василівна,
кандидат наук з державного управління,
доцент

Київ – 2026

АНОТАЦІЯ

Дрига Д.А. Державне регулювання інформаційної безпеки в умовах сучасних цивілізаційних викликів. – Кваліфікаційна наукова праця на правах рукопису.

Дисертація на здобуття наукового ступеня доктора філософії в галузі знань 28 «Публічне управління та адміністрування» за спеціальністю 281 «Публічне управління та адміністрування». ЗВО «Відкритий міжнародний університет розвитку людини «Україна». Київ, 2026.

Дисертаційне дослідження присвячено теоретико-методологічному обґрунтуванню та розробленню науково-практичних положень щодо вдосконалення державного регулювання інформаційної безпеки України в умовах сучасних цивілізаційних викликів. У роботі досліджено еволюцію інформаційного суспільства, визначено сутність інформаційно-цифрової цивілізаційної трансформації, розкрито місце інформаційної та цивілізаційної безпеки в системі національної безпеки, систематизовано сучасні цивілізаційні виклики та породжені ними інформаційні загрози. Проаналізовано нормативно-правове та інституційне забезпечення державного регулювання інформаційної безпеки, визначено структуру й функціональне призначення відповідних механізмів, узагальнено зарубіжний досвід та обґрунтовано напрями його адаптації до національних умов України. Розроблено концептуальні та практичні засади вдосконалення державного регулювання інформаційної безпеки на основі превентивності, адаптивності, міжсекторальної взаємодії та циклічності управлінського процесу.

На основі систематизації теоретичних підходів до еволюції інформаційного суспільства встановлено поступову трансформацію наукових уявлень про інформацію від її розуміння як засобу передачі відомостей та ресурсу економічної діяльності до визнання системоутворювальним чинником суспільного розвитку, функціонування держави та публічного управління. Досліджено еволюцію концепцій постіндустріального, інформаційного, мережевого суспільства, суспільства знань та інформаційної цивілізації.

Обґрунтовано, що цифровізація, платформізація, алгоритмізація суспільних процесів, розвиток штучного інтелекту, перетворення інформації та знань на стратегічні ресурси й посилення транскордонності інформаційних потоків зумовлюють якісні зміни економічних, політичних, соціальних та управлінських відносин.

Удосконалено понятійно-категоріальний апарат дослідження державного регулювання інформаційної безпеки шляхом обґрунтування авторського визначення поняття «інформаційно-цифрова цивілізаційна трансформація» як системного процесу якісних змін суспільних, економічних, політичних та управлінських відносин, що зумовлено перетворенням інформації і знань на стратегічні ресурси розвитку, глобальним поширенням цифрових технологій, мережевих форм взаємодії та алгоритмічних систем, унаслідок чого змінюються механізми функціонування держави, суспільства та взаємодії людини з інформаційним середовищем. Визначено дуалістичний характер зазначеної трансформації, яка, з одного боку, розширює можливості суспільного розвитку, удосконалення публічного управління та використання знань, а з іншого – формує нові системні вразливості, пов’язані з технологічною залежністю, цифровою нерівністю, алгоритмічним впливом і зростанням залежності держави та суспільства від інформаційно-цифрової інфраструктури.

Розкрито теоретичні засади інформаційної безпеки як складової національної безпеки, обґрунтовано її комплексний та міжсекторальний характер. Встановлено, що сучасний зміст інформаційної безпеки охоплює взаємопов’язані інформаційно-технологічний та інформаційно-комунікаційний виміри, які передбачають захист інформації, інформаційних ресурсів та інфраструктури, забезпечення інформаційних прав та інтересів людини, суспільства і держави, а також протидію деструктивним інформаційним та інформаційно-психологічним впливам.

Набули подальшого розвитку теоретико-методологічні положення щодо сутності цивілізаційної безпеки, яку запропоновано розглядати як стан захищеності та стійкості держави і суспільства, за якого забезпечується збереження їх ключових ціннісних, інституційних, інформаційних, культурних і

технологічних основ, здатність адаптуватися до системних трансформацій цивілізаційного масштабу, протидіяти породженим ними загрозам та забезпечувати безперервність і перспективи сталого розвитку. Обґрунтовано надгалузевий та міжсекторальний характер цивілізаційної безпеки, що дозволяє розглядати її як категорію вищого рівня узагальнення для оцінювання системних, довготривалих, взаємопов'язаних і транснаціональних трансформацій та загроз.

Запропоновано концептуальну модель взаємозв'язку цивілізаційної, національної та інформаційної безпеки, у межах якої національна безпека визначає базову систему захисту національних інтересів держави, суспільства і людини, інформаційна безпека характеризує специфічний вимір такої захищеності, а цивілізаційна безпека формує теоретичну рамку оцінювання трансформацій і загроз цивілізаційного масштабу. Визначено, що інформаційна безпека є одним із ключових функціональних вимірів забезпечення цивілізаційної стійкості держави та суспільства.

Систематизовано сучасні цивілізаційні виклики за критеріями масштабності, системності, довготривалості, міжсекторальності, транснаціональності та трансформаційного впливу. Визначено, що до основних цивілізаційних викликів належать трансформація міжнародного порядку, глобалізація інформаційного простору, цифровізація та платформізація суспільних відносин, розвиток штучного інтелекту, посилення технологічної взаємозалежності, суспільна поляризація, культурно-ціннісні, екологічні, демографічні та соціальні трансформації. Обґрунтовано їх вплив на виникнення інформаційних вразливостей, ризиків і загроз та формування міжсекторальних наслідків для національної безпеки.

Удосконалено теоретико-методологічний підхід до визначення впливу цивілізаційних викликів на інформаційну безпеку шляхом встановлення причинно-наслідкового взаємозв'язку між цивілізаційними трансформаціями, цивілізаційними викликами, інформаційними вразливостями, ризиками, загрозами та їх міжсекторальними наслідками для національної безпеки. Визначено динамічний і нелінійний характер зазначеного взаємозв'язку, за якого

один цивілізаційний виклик може спричиняти сукупність взаємопов'язаних інформаційних ризиків і загроз, реалізація яких зумовлює каскадні наслідки для різних сфер національної безпеки. Обґрунтовано необхідність трансформації державного регулювання інформаційної безпеки на засадах превентивності, адаптивності, ризик-орієнтованості та міжсекторальності.

Запропоновано превентивно-адаптивну модель державного регулювання інформаційної безпеки, яка ґрунтується на функціональній взаємодії трьох взаємопов'язаних контурів: превентивно-прогностичного, регуляторно-реактивного та оціночно-адаптаційного. Доведено, що їх поєднання забезпечує формування безперервного управлінського циклу, який охоплює моніторинг цивілізаційних трансформацій, прогнозування викликів, виявлення інформаційних вразливостей, оцінювання ризиків, превентивне регулювання, реагування на загрози, забезпечення стійкості та відновлення, оцінювання результативності здійснених заходів і подальшу адаптацію механізмів державного регулювання. Визначальною особливістю моделі є забезпечення зворотного зв'язку між результатами регуляторного впливу та вдосконаленням нормативно-правових, організаційно-інституційних, інформаційно-комунікаційних і технологічних механізмів державного регулювання інформаційної безпеки.

Проаналізовано нормативно-правове забезпечення державного регулювання інформаційної безпеки України, яке постає як багаторівнева, системна та динамічна конструкція, що визначає правові засади державного управління у сфері інформаційної безпеки, кіберзахисту, повноваження суб'єктів системи національної безпеки та механізми захисту інформаційного суверенітету держави. Обґрунтовано напрями вдосконалення структурної моделі нормативно-правового забезпечення інформаційної безпеки шляхом її інтеграції з інформаційно-правовими системами для автоматизованого відстеження, систематизації та оперативного оновлення нормативно-правових актів у відповідних функціональних блоках, що створює передумови для підвищення актуальності й адаптивності правового регулювання.

Досліджено інституційне забезпечення державного регулювання інформаційної безпеки України та визначено його багаторівневий характер. Систематизовано суб'єктів державного управління за стратегічним, оперативно-силовим, технологічно-інфраструктурним, зовнішнім, ресурсно-економічним та екологічним, соціально-демографічним, гуманітарно-освітнім і когнітивним рівнями. Обґрунтовано необхідність урахування регіонального рівня державного управління, територіальних органів і підрозділів, а також наукових та науково-дослідних установ, що забезпечують аналітичний та експертний супровід державної політики інформаційної безпеки.

Визначено структурні та функціональні особливості механізму державного регулювання інформаційної безпеки як складної, багаторівневої та динамічної системи, що охоплює політичний, нормативно-правовий, організаційний, інформаційно-цифровий (технологічний), економічний і мотиваційний компоненти. Розкрито їх функціональне призначення та визначено основні функції державного регулювання інформаційної безпеки: цільову, стимулюючу, нормативну, коригувальну, соціальну та контрольну. Обґрунтовано взаємозалежність зазначених компонентів та необхідність їх функціонального узгодження для забезпечення цілісності й результативності державного регуляторного впливу.

На основі узагальнення зарубіжного досвіду Європейського Союзу, США та НАТО удосконалено критеріально-адаптаційний підхід до використання міжнародних механізмів державного регулювання інформаційної безпеки в Україні. Запропонований підхід передбачає комплексне оцінювання зарубіжних регуляторних практик за критеріями нормативно-правової сумісності, інституційної спроможності, безпекової релевантності, ресурсної забезпеченості, превентивності та адаптивності, дотримання прав людини. Розроблено трьохетапний алгоритм визначення правової допустимості, управлінської доцільності та способу адаптації відповідних механізмів до національних умов України, що створює методичні передумови для обґрунтованого використання зарубіжного досвіду відповідно до національних безпекових пріоритетів та інституційних можливостей.

Обґрунтовано напрями вдосконалення механізмів державного регулювання інформаційної безпеки України в умовах сучасних цивілізаційних викликів та удосконалено комплексний підхід до їх узгодженої реалізації. Окреслений підхід ґрунтується на функціональній взаємодії політичного, нормативно-правового, організаційного, інформаційно-цифрового (технологічного), економічного та мотиваційного компонентів комплексного механізму. Розроблено практичні рекомендації щодо вдосконалення зазначених компонентів, визначено організаційні передумови їх реалізації та обґрунтовано поетапність впровадження управлінських заходів на оперативному, тактичному і стратегічному рівнях.

Запропоновано дворівневу систему оцінювання результативності державного регулювання інформаційної безпеки, що передбачає поєднання процесних показників виконання управлінських заходів із результативними показниками змін у стані інформаційної безпеки. Обґрунтовано доцільність узгодженого застосування механізмів державного регулювання в межах циклічного управлінського процесу, який забезпечує взаємозв'язок між оцінюванням інформаційних загроз, визначенням регуляторних пріоритетів, плануванням і реалізацією управлінських заходів, моніторингом їх результатів та подальшим коригуванням управлінських рішень.

Доведено, що запропоновані теоретико-методологічні положення, концептуальні моделі та науково-практичні рекомендації формують взаємопов'язане підґрунтя для вдосконалення державного регулювання інформаційної безпеки України. Поєднання превентивно-адаптивної моделі з комплексним підходом до реалізації механізмів державного регулювання спрямоване на підвищення системності, узгодженості, превентивності, адаптивності та результативності управлінського впливу, зміцнення інформаційної стійкості держави і суспільства та мінімізацію міжсекторальних наслідків інформаційних загроз для національної безпеки України.

Ключові слова: державне регулювання, інформаційна безпека, національна безпека, інформація, інформаційне суспільство, публічне

управління, інформаційні загрози, цивілізаційна безпека, правове регулювання, правовий механізм, кіберзагрози, кібербезкпека, інформаційні технології, штучний інтелект, гібридні загрози,

ABSTRACT

Dryha D. A. State Regulation of Information Security in the Context of Contemporary Civilizational Challenges. – Qualification scientific paper presented as a manuscript.

Dissertation for the degree of Doctor of Philosophy in the field of knowledge 28 “Public Management and Administration”, in the specialty 281 “Public Management and Administration”. HEI “Open International University of Human Development “Ukraine”. Kyiv, 2026.

The dissertation is devoted to the theoretical and methodological substantiation and development of scientific and practical provisions aimed at improving the state regulation of information security in Ukraine in the context of contemporary civilizational challenges. The research examines the evolution of the information society, defines the essence of information-digital civilizational transformation, reveals the place of information security and civilizational security within the national security system, and systematizes contemporary civilizational challenges and the information threats arising from them. The study analyzes the regulatory, legal, and institutional frameworks for state regulation of information security, identifies the structure and functional purposes of the relevant mechanisms, summarizes international experience, and substantiates approaches to its adaptation to Ukraine's national conditions. Conceptual and practical foundations for improving state regulation of information security are developed based on prevention, adaptability, cross-sectoral interaction, and the cyclical nature of the public administration process.

Based on the systematization of theoretical approaches to the evolution of the information society, the study identifies a gradual transformation of scientific perceptions of information, from its understanding as a means of transmitting knowledge and a resource for economic activity to its recognition as a system-forming factor in societal development, the functioning of the state, and public administration. The evolution of the concepts of post-industrial society, information society, network society, knowledge society, and information civilization is examined. It is substantiated that digitalization, platformization, the algorithmization of social processes, the

development of artificial intelligence, the transformation of information and knowledge into strategic resources, and the increasing transboundary nature of information flows bring about qualitative changes in economic, political, social, and administrative relations.

The conceptual and categorical framework for studying state regulation of information security has been improved by substantiating an original definition of "information-digital civilizational transformation" as a systemic process of qualitative changes in social, economic, political, and administrative relations driven by the transformation of information and knowledge into strategic development resources, the global proliferation of digital technologies, network-based forms of interaction, and algorithmic systems, resulting in changes in the mechanisms through which the state and society function and individuals interact with the information environment. The dual nature of this transformation is identified: on the one hand, it expands opportunities for societal development, improvement of public administration, and the use of knowledge; on the other hand, it generates new systemic vulnerabilities associated with technological dependence, digital inequality, algorithmic influence, and the growing dependence of the state and society on information and digital infrastructure.

The theoretical foundations of information security as a component of national security are examined, and its comprehensive and cross-sectoral nature is substantiated. It is established that the contemporary understanding of information security encompasses interconnected information-technological and information-communication dimensions, including the protection of information, information resources, and infrastructure; the safeguarding of the information rights and interests of individuals, society, and the state; and counteraction to destructive informational and information-psychological influences.

The theoretical and methodological provisions concerning the essence of civilizational security have been further developed. Civilizational security is proposed to be understood as a state of protection and resilience of the state and society in which the preservation of their fundamental value-based, institutional, informational, cultural, and technological foundations is ensured, together with their ability to adapt to

systemic transformations of a civilizational scale, counteract the threats arising from such transformations, and maintain continuity and prospects for sustainable development. The supra-sectoral and cross-sectoral nature of civilizational security is substantiated, allowing it to be considered a higher-order analytical category for assessing systemic, long-term, interconnected, and transnational transformations and threats.

A conceptual model of the interrelationship between civilizational, national, and information security is proposed. Within this model, national security defines the fundamental system for protecting the national interests of the state, society, and individuals; information security characterizes a specific dimension of such protection in the information sphere; and civilizational security provides a theoretical framework for assessing transformations and threats of a civilizational scale. Information security is identified as one of the key functional dimensions of ensuring the civilizational resilience of the state and society.

Contemporary civilizational challenges are systematized according to the criteria of scale, systemic nature, long-term duration, cross-sectoral impact, transnational character, and transformative influence. The principal civilizational challenges are identified as the transformation of the international order, globalization of the information space, digitalization and platformization of social relations, development of artificial intelligence, increasing technological interdependence, societal polarization, and cultural, value-based, environmental, demographic, and social transformations. Their influence on the emergence of information vulnerabilities, risks, and threats, as well as the formation of cross-sectoral consequences for national security, is substantiated.

The theoretical and methodological approach to determining the impact of civilizational challenges on information security has been improved by establishing causal relationships between civilizational transformations, civilizational challenges, information vulnerabilities, risks, threats, and their cross-sectoral consequences for national security. The dynamic and nonlinear nature of these relationships is identified, whereby a single civilizational challenge may generate a set of interconnected information risks and threats, the realization of which may cause cascading

consequences across various areas of national security. The necessity of transforming state regulation of information security based on the principles of prevention, adaptability, risk orientation, and cross-sectoral coordination is substantiated.

A preventive-adaptive model of state regulation of information security is proposed, based on the functional interaction of three interconnected components: the preventive-forecasting, regulatory-response, and evaluation-adaptation circuits. Their integration is substantiated as the basis for establishing a continuous public administration cycle encompassing the monitoring of civilizational transformations, forecasting of challenges, identification of information vulnerabilities, risk assessment, preventive regulation, responses to threats, ensuring resilience and recovery, evaluation of the effectiveness of implemented measures, and subsequent adaptation of state regulatory mechanisms. A defining feature of the model is the provision of feedback between the outcomes of regulatory intervention and the improvement of regulatory-legal, organizational-institutional, information-communication, and technological mechanisms of state regulation of information security.

The regulatory and legal framework for state regulation of information security in Ukraine is analyzed and characterized as a multilevel, systemic, and dynamic structure that establishes the legal foundations of public administration in the fields of information security and cyber protection, defines the powers of national security actors, and provides mechanisms for protecting the state's information sovereignty. Approaches to improving the structural model of the regulatory and legal framework for information security are substantiated through its integration with legal information systems to enable automated monitoring, systematization, and timely updating of regulatory legal acts within the relevant functional components. This creates prerequisites for enhancing the relevance and adaptability of legal regulation.

The institutional framework for state regulation of information security in Ukraine is examined, and its multilevel nature is identified. Public administration actors are systematized according to strategic, operational and security, technological and infrastructural, external, resource-economic and environmental, socio-demographic, humanitarian and educational, and cognitive levels. The necessity of taking into account the regional level of public administration, territorial authorities

and their subdivisions, as well as scientific and research institutions providing analytical and expert support for state information security policy, is substantiated.

The structural and functional characteristics of the mechanism of state regulation of information security are identified as those of a complex, multilevel, and dynamic system encompassing political, regulatory-legal, organizational, information-digital (technological), economic, and motivational components. Their functional purposes are revealed, and the principal functions of state regulation of information security are identified: goal-setting, incentive, regulatory, corrective, social, and control functions. The interdependence of these components and the necessity of their functional coordination to ensure the integrity and effectiveness of state regulatory intervention are substantiated.

Based on the generalization of international experience from the European Union, the United States, and NATO, a criteria-based adaptation approach to applying international mechanisms of state regulation of information security in Ukraine has been improved. The proposed approach involves a comprehensive assessment of foreign regulatory practices according to the criteria of regulatory and legal compatibility, institutional capacity, security relevance, resource availability, prevention and adaptability, and respect for human rights. A three-stage algorithm has been developed for determining the legal admissibility, administrative feasibility, and method of adapting the relevant mechanisms to Ukraine's national conditions. This creates methodological prerequisites for the informed application of international experience in accordance with national security priorities and institutional capacities.

Directions for improving the mechanisms of state regulation of information security in Ukraine in the context of contemporary civilizational challenges are substantiated, and a comprehensive approach to their coordinated implementation is further developed. The proposed approach is based on the functional interaction of the political, regulatory-legal, organizational, information-digital (technological), economic, and motivational components of the integrated mechanism. Practical recommendations for improving these components are developed, organizational prerequisites for their implementation are identified, and the phased implementation of

administrative measures at the operational, tactical, and strategic levels is substantiated.

A two-level system for evaluating the performance of state regulation of information security is proposed, combining process indicators reflecting the implementation of administrative measures with outcome indicators reflecting changes in the state of information security. The expediency of coordinated application of state regulatory mechanisms within a cyclical public administration process is substantiated. This process ensures interconnections between the assessment of information threats, identification of regulatory priorities, planning and implementation of administrative measures, monitoring of their outcomes, and subsequent adjustment of administrative decisions.

The study concludes that the proposed theoretical and methodological provisions, conceptual models, and scientific and practical recommendations provide an interconnected foundation for improving state regulation of information security in Ukraine. The integration of the preventive-adaptive model with a comprehensive approach to implementing state regulatory mechanisms is intended to enhance the systemic coherence, coordination, preventive capacity, adaptability, and effectiveness of public administration, strengthen the information resilience of the state and society, and minimize the cross-sectoral consequences of information threats to Ukraine's national security.

Keywords: government regulation, information security, national security, information, information society, public administration, information threats, civilizational security, legal regulation, legal mechanisms, cyber threats, cybersecurity, information technology, artificial intelligence, hybrid threats.

СПИСОК ОПУБЛІКОВАНИХ ПРАЦЬ ЗДОБУВАЧА ЗА ТЕМОЮ ДИСЕРТАЦІЇ

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

1. Дрига Д. А. Правовий механізм інформаційної безпеки як категорія публічного управління. *Публічне управління і адміністрування.* 2023. № 2 (80). С. 93-97. DOI: https://doi.org/10.32782/1813-3401.2023.2.17.

2. Дрига Д.А. Особливості розуміння феномену інформаційної безпеки у сфері публічного управління. *Актуальні проблеми у сфері публічного управління.* 2023. Вип. 34. С. 108-111. DOI: https://doi.org/10.32782/pma2663-5240-2023.34.21.

3. Дрига Д.А. Аналіз правових механізмів забезпечення інформаційної безпеки інформаційної інфраструктури Європейського союзу. *Herald of Khmelnytskyi National University. Economic Sciences.* 2024. Вип. 334(5). С.46-51. DOI: https://doi.org/10.31891/2307-5740-2024-334-7.

4. Дрига Д.А. Державне регулювання інформаційної безпеки в Україні. *Координати державного управління*. 2026. № 1(6). С. 214-228. DOI: https://doi.org/10.62664/cpa.2026.01.11.

5. Дрига Д.А. Європейські підходи до державного регулювання інформаційної безпеки: сучасні механізми та перспективи імплементації в Україні. *Herald of Khmelnytskyi National University. Economic Sciences.* 2026. Вип. 356(4). С.183-188. DOI: https://doi.org/10.31891/2307-5740-2026-356-25.

Статті в інших виданнях

6. Дрига Д. А. Механізм формування важелів регулювання правових норм в умовах цифровізації. *Сучасний науковий журнал.* 2024. Вип. 3(1). С. 101-107. DOI: https://doi.org/10.36994/2786-9008-2024-3-13.

7. Дрига Д. А. Інформаційна стійкість як опора національної безпеки: українська модель державного адміністрування. *Сучасний науковий журнал*. 2025. Вип. 10(4). С. 28-34. DOI: https://doi.org/10.36994/2786-9008-2025-10-3.

Тези наукових доповідей

8. Дрига Д. А. Деякі актуалізовані підходи до оцінки класифікації загроз у інформаційній безпеці у сфері державного управління. *Сучасні аспекти модернізації науки в Україні: стан, проблеми, тенденції розвитку* : V Міжнародна науково-практична онлайн-конференція, м. Венеція, Італія, 7 січня 2021 року : тези доповіді. Венеція, 2021. С. 32-35.

9. Дрига Д. А. Роль інформаційної безпеки у забезпеченні національної безпеки держави. *Актуальні питання сучасної стратегії розвитку України: виклики, пріоритети та прогнози* : VI Науково-практична онлайн-конференція студентів, аспірантів і молодих вчених, м. Київ, 14 травня 2026 року : тези доповіді. Київ, 2026. С. 71-73.

10. Дрига Д. А. Інформаційна безпека як складова національної безпеки в контексті досягнення цілей сталого розвитку. *Цифрове наукове суспільство: соціально-економічні, правові та міжнародні аспекти* : VII Міжнародна наукова конференція, м. Харків, 31 липня 2026 року : тези доповіді. Харків, 2026. С. 65-67.

11. Dryha D. Modern challenges to Ukraine’s national security: a comprehensive approach to strengthening state resilience. *Modern Science: Research, Economy and Innovation* : 6th International Scientific and Practical Conference, Zagreb, Croatia, September 2-4, 2026 : conference paper. Zagreb, 2026. P. 162-166.

ЗМІСТ

ПЕРЕЛІК УМОВНИХ СКОРОЧЕНЬ 19

ВСТУП 21

РОЗДІЛ І. ТЕОРЕТИКО-МЕТОДОЛОГІЧНІ ЗАСАДИ ДЕРЖАВНОГО РЕГУЛЮВАННЯ ІНФОРМАЦІЙНОЇ БЕЗПЕКИ В УМОВАХ ЦИВІЛІЗАЦІЙНИХ ТРАНСФОРМАЦІЙ 33

1.1. Теоретичні засади становлення інформаційного суспільства в контексті сучасних цивілізаційних трансформацій 33

1.2. Інформаційна та цивілізаційна безпека в системі національної безпеки 58

1.3. Сучасні цивілізаційні виклики та інформаційні загрози як чинники трансформації державного регулювання інформаційної безпеки 85

Висновки до розділу 1 106

РОЗДІЛ ІІ. АНАЛІЗ СУЧАСНОГО СТАНУ ДЕРЖАВНОГО РЕГУЛЮВАННЯ ІНФОРМАЦІЙНОЇ БЕЗПЕКИ УКРАЇНИ В УМОВАХ ЦИВІЛІЗАЦІЙНИХ ВИКЛИКІВ 110

2.1. Правове забезпечення державного регулювання інформаційної безпеки 110

2.2. Інституційне забезпечення державного регулювання інформаційної безпеки в системі національної безпеки України 130

2.3. Механізми державного регулювання інформаційної безпеки в умовах цифровізації, глобалізації та розвитку інформаційного суспільства 145

Висновки до розділу 2 159

РОЗДІЛ ІІІ. УДОСКОНАЛЕННЯ ДЕРЖАВНОГО РЕГУЛЮВАННЯ ІНФОРМАЦІЙНОЇ БЕЗПЕКИ В УМОВАХ СУЧАСНИХ ЦИВІЛІЗАЦІЙНИХ ВИКЛИКІВ 162

3.1. Зарубіжний досвід державного регулювання інформаційної безпеки та можливості його адаптації в Україні 162

3.2. Удосконалення механізмів державного регулювання інформаційної безпеки України в умовах сучасних цивілізаційних

викликів 179
Висновки до розділу 3 207
ВИСНОВКИ 210
СПИСОК ВИКОРИСТАНИХ ДЖЕРЕЛ 217
ДОДАТКИ 239

ПЕРЕЛІК УМОВНИХ СКОРОЧЕНЬ

CERT – Computer Emergency Response Team – команда реагування на комп'ютерні надзвичайні події;

CERT-UA – Урядова команда реагування на комп'ютерні надзвичайні події України;

CISO – Chief Information Security Officer – керівник з інформаційної безпеки;

CSIRT – Computer Security Incident Response Team – команда реагування на інциденти комп'ютерної безпеки;

EC3 – European Cybercrime Centre – Європейський центр боротьби з кіберзлочинністю;

EDR – Endpoint Detection and Response – технологія виявлення загроз на кінцевих пристроях та реагування на них;

ENISA – European Union Agency for Cybersecurity – Агентство Європейського Союзу з питань кібербезпеки;

FBI – Federal Bureau of Investigation – Федеральне бюро розслідувань США;

IEC – International Electrotechnical Commission – Міжнародна електротехнічна комісія;

IoT – Internet of Things – Інтернет речей;

ISO – International Organization for Standardization – Міжнародна організація зі стандартизації;

NATO CCDCOE – NATO Cooperative Cyber Defence Centre of Excellence – Об'єднаний центр передових технологій з кібероборони НАТО;

NIST – National Institute of Standards and Technology – Національний інститут стандартів і технологій США;

SIEM – Security Information and Event Management – система управління інформацією та подіями інформаційної безпеки;

SOC – Security Operations Center – центр оперативного моніторингу та реагування на інциденти кібербезпеки;

UNOCT – United Nations Office of Counter-Terrorism – Управління ООН з боротьби з тероризмом;

WSIS – World Summit on the Information Society – Всесвітній саміт з питань інформаційного суспільства;

ЄС – Європейський Союз;

ЄСВ – Єдиний внесок на загальнообов'язкове державне соціальне страхування;

ІКТ – інформаційно-комунікаційні технології;

ІТ – інформаційні технології;

КІІ – критична інформаційна інфраструктура;

КСЗІ – комплексна система захисту інформації;

НАДС – Національне агентство України з питань державної служби;

НАН України – Національна академія наук України;

НАТО – Організація Північноатлантичного договору;

ОБСЄ – Організація з безпеки та співробітництва в Європі;

ОЕСР – Організація економічного співробітництва та розвитку;

ООН – Організація Об'єднаних Націй;

ПДВ – податок на додану вартість;

РНБО – Рада національної безпеки і оборони України;

СБУ – Служба безпеки України;

США – Сполучені Штати Америки;

ШІ – штучний інтелект;

ЮНЕСКО – Організація Об'єднаних Націй з питань освіти, науки і культури.

ВСТУП

Актуальність теми. Сучасний етап суспільного розвитку характеризується глибокими трансформаціями інформаційного середовища, зумовленими глобалізацією, цифровізацією, стрімким розвитком інформаційно-комунікаційних технологій, штучного інтелекту, мережевих платформ та нових способів створення, поширення й використання інформації. Інформація перетворилася на один із ключових стратегічних ресурсів держави, а здатність забезпечувати її захист, достовірність, доступність і належне використання безпосередньо впливає на стійкість державних інституцій, реалізацію національних інтересів, функціонування демократичних механізмів та забезпечення прав і свобод людини. За таких умов інформаційна безпека виходить за межі суто технологічної проблематики та набуває комплексного суспільного й державно-управлінського значення.

Особливістю сучасного періоду є те, що трансформація інформаційної сфери відбувається під впливом широкого комплексу цивілізаційних викликів, які змінюють характер взаємодії держави, суспільства та людини. До них належать глобальна цифрова трансформація, формування транскордонного інформаційного простору, технологічна конкуренція, поширення штучного інтелекту та алгоритмічних систем, зростання масштабів кіберзагроз, інформаційно-психологічних впливів і дезінформації, посилення ролі глобальних цифрових платформ, виникнення нових ризиків для приватності та персональних даних, а також використання інформаційних технологій як інструменту політичного, економічного та воєнного протиборства. Сукупність зазначених процесів свідчить про формування якісно нового безпекового середовища, в якому інформаційна складова дедалі тісніше пов’язується з політичною, економічною, соціальною, воєнною та гуманітарною стійкістю держави.

У цьому контексті інформаційна безпека постає не лише як складова національної безпеки, але й як важливий елемент забезпечення цивілізаційної

стійкості держави і суспільства. Сучасні інформаційні загрози здатні впливати одночасно на декілька рівнів суспільної системи: на особистісному рівні – на свідомість, поведінку, приватність та реалізацію інформаційних прав людини; на суспільному – на громадську думку, соціальну згуртованість, довіру до державних інституцій та суспільні цінності; на державному – на функціонування органів публічної влади, критичної інформаційної інфраструктури, процеси прийняття управлінських рішень та реалізацію державної політики; на міжнародному – на інформаційний суверенітет, міжнародний імідж держави та її спроможність протидіяти зовнішнім інформаційним впливам.

Особливої актуальності зазначена проблематика набуває для України, яка функціонує в умовах тривалої збройної агресії та одночасно здійснює масштабну цифрову трансформацію держави та суспільства. Інформаційний простір перетворився на одне із ключових середовищ сучасного протиборства, у якому поряд із традиційними загрозами використовуються кібератаки, дезінформаційні кампанії, маніпулятивні технології, інформаційно-психологічні операції, втручання в інформаційні системи та інші інструменти впливу.

Водночас стрімкість технологічних і суспільних змін призводить до того, що традиційні механізми державного регулювання не завжди відповідають динаміці сучасних інформаційних загроз. Виникає необхідність перегляду підходів до визначення суб’єктів, об’єктів, принципів, функцій, методів та інструментів державного регулювання інформаційної безпеки, удосконалення координації між органами публічної влади, суб’єктами сектору безпеки і оборони, інститутами громадянського суспільства та приватним сектором. Важливого значення набуває також забезпечення балансу між безпековими інтересами держави та необхідністю дотримання демократичних принципів, свободи слова, права на інформацію, захисту персональних даних та інших фундаментальних прав людини.

Зазначене зумовлює потребу у формуванні комплексної моделі державного регулювання інформаційної безпеки, адаптованої до сучасних цивілізаційних викликів та орієнтованої на забезпечення стійкості держави, суспільства й особистості до інформаційних загроз. Така модель має

ґрунтуватися на системному поєднанні нормативно-правових, інституційних, організаційно-управлінських, інформаційно-аналітичних, технологічних та комунікаційних механізмів, а також передбачати перехід від переважно реактивного реагування на інформаційні загрози до превентивного та ризик-орієнтованого державного управління.

Теоретичну основу дисертаційної роботи сформовано на основі наукових положень, концепцій та результатів досліджень вітчизняних і зарубіжних учених у сфері публічного управління та адміністрування, державного регулювання, національної та інформаційної безпеки, інформаційної політики, стратегічних комунікацій, цифрової трансформації, кібербезпеки, а також дослідження сучасних цивілізаційних, глобалізаційних і технологічних викликів.

Зокрема, з'ясовуючи сутність категорії «інформація», було розглянуто роботи І. Арістової, О. Кохановської, О. Пархоменка, О. Сосніної, В. Цимбалюка та багато інших. Проблематика визначення сутності інформації, її правової природи, місця в системі суспільних відносин та значення для забезпечення інформаційної безпеки набула ґрунтовного висвітлення у працях вітчизняних науковців: І. Арістової, О. Власюка, В. Дабіжи, А. Дорошевича, В. Желіховського, А. Загородньої, О. Золотар, Е. Кадебської, Б. Кормича, О. Кохановської, В. Ліпкана, В. Лопохи, Ю. Максименко, А. Марущака, А. Некряч, Н. Орлової, О. Сороківської, Т. Ярового та інших учених. У їхніх дослідженнях інформація розглядається не лише як сукупність відомостей і даних, але й як специфічний об'єкт правовідносин, нематеріальне благо, суспільно значущий та стратегічний ресурс, а також важлива складова інформаційних процесів і забезпечення національної та інформаційної безпеки. Різноманітність наукових позицій вітчизняних дослідників підтверджує багатоаспектність категорії «інформація» та необхідність її комплексного дослідження з урахуванням правового, управлінського й безпекового вимірів.

Теоретичною основою дисертаційного дослідження стали також класичні праці зарубіжних науковців, у яких відбувається осмислення інформаційних процесів, концепцій інформації, інформаційного суспільства, цивілізації та цивілізаційних викликів. Зарубіжні науковці Р. Баєрс, Г. Бейтсон, Д. Белл,

Н. Віннер, А. Вольферс, В. Ліппманн, Ф. Махлуп, С. Полсен, М. Порат, К. Шеннон, Л. Флоріді та багато інших розглядають означену проблематику, а їхні праці стали основою для переосмислення сучасних цивілізаційних викликів інформаційного суспільства та формування концептуально-методологічного підґрунтя даного дисертаційного дослідження.

Окрему основу дослідження становлять наукові напрацювання щодо державного регулювання інформаційної безпеки. Так, проблему правового забезпечення розкривають, зокрема, українські науковці І. Боднар, В. Бойко, М. Василенко, В. Горбулін, М. Дмитренко, Є. Колосовський, Г. Красноступ, Е. Круць, С. Кухаренко, С. Лукашевич, М. Микитюк, Т. Мужанова, Г. Ситник, Л. Сопільник, О. Старостін, Н. Тарасенко, О. Тихомиров, Н. Філіпенко, В. Харченко, які у своїх роботах звертають увагу на закони, законодавчі акти України та світового співтовариства, які регулюють питання інформаційної безпеки. Ці дослідники звертають увагу на стандарти в інформаційно-правовому забезпеченні інформаційної безпеки, наголошуючи на тому, що безпекові питання стають провідною функцією держави та державного управління.

Українські науковці та практики, наприклад, Н. Воробець, В. Кононенко, П. Копицька, І. Кукін, О. Левченко, Є. Манокін, Л. Новікова, В. Пашковський, Н. Тарасенко, Н. Цибульник, В. Шемчук та інші, розглядають у своїх роботах інституційні особливості формування та функціонування інформаційної безпеки в Україні в різних галузях суспіль-політичної діяльності.

Проте, сучасна наукова думка приділяє недостатню увагу розгляду механізмів державного регулювання інформаційної безпеки в умовах цифровізації, глобалізації та розвитку інформаційного суспільства. А. Клочко, А. Кузьменко, В. Пашковський, Т. Перун, М. Присяжнюк, В. Приходько, О. Чечель, М. Шевчук, К. Юдкова та інші дослідники при розгляді механізмів забезпечення інформаційної безпеки зосереджують увагу або на нормативно-правовому аспекті регулювання інформаційної безпеки, або розглядають суто інституційне регулювання, не заглиблюючись у особливості та ознаки саме механізмів державного регулювання інформаційною безпекою.

Аналіз наукової літератури засвідчив, що залишається недостатньо

опрацьованою також проблематика державного регулювання інформаційної безпеки в умовах сучасних цивілізаційних викликів, що зумовлює потребу в її поглибленому дослідженні. Особливої актуальності та наукового інтересу набуває аналіз ролі публічного управління в системі державного регулювання інформаційної безпеки, уточнення відповідних механізмів, а також оцінка впливу цивілізаційних викликів на інформаційну безпеку як невід'ємну складову національної безпеки.

Зв'язок роботи з науковими програмами, планами, темами. Дисертаційне дослідження відповідає проблематиці науково-дослідної роботи кафедри міжнародних відносин та політичного консалтингу Інституту права та суспільних відносин ЗВО «Відкритий міжнародний університет розвитку людини «Україна» за темами «Охорона прав та законних інтересів людини і громадянина: національний та міжнародний досвід» (№ державної реєстрації 0121U110399); «Воєнно-стратегічний розвиток сучасної України: міжнародно-політичні виклики, державні інтереси, безпека» (№ державної реєстрації 0124U000322). (довідка від 29.04.2024 р. № 92), де автором проаналізовано та оцінено інституційне забезпечення державного регулювання інформаційної безпеки в системі національної безпеки України.

Мета і завдання дослідження. Мета дисертаційного дослідження полягає в теоретико-методологічному обґрунтуванні та розробленні науково-практичних засад удосконалення державного регулювання інформаційної безпеки України в умовах сучасних цивілізаційних викликів, формуванні концептуальної моделі його розвитку, спрямованої на забезпечення стійкості держави, суспільства та особистості до сучасних інформаційних загроз, а також обґрунтуванні механізмів, інструментів і пріоритетних напрямів її практичної реалізації.

Досягнення поставленої мети зумовило вирішення наступних завдань:

- проаналізувати особливості еволюції інформаційного суспільства та обґрунтувати сутність інформаційно-цифрової цивілізаційної трансформації як сучасного етапу суспільного розвитку;
- розкрити теоретичні засади інформаційної безпеки та визначити її взаємозв'язок з національною й цивілізаційною безпекою та запропонувати

концептуальну модель такого взаємозв'язку;

- систематизувати сучасні цивілізаційні виклики та інформаційні загрози, встановити причинно-наслідкові зв'язки між ними шляхом розробки моделі державного регулювання інформаційної безпеки;
- дослідити теоретико-правові засади державного регулювання інформаційної безпеки та на цій підставі вдосконалити модель нормативно-правового забезпечення інформаційної безпеки в Україні;
- проаналізувати інституційне забезпечення державного регулювання інформаційної безпеки в системі національної безпеки України;
- поглибити розуміння механізмів державного регулювання інформаційної безпеки України;
- дослідити міжнародно-правовий досвід регулювання та забезпечення інформаційної безпеки і визначити можливі шляхи його адаптації в Україні;
- обґрунтувати напрями вдосконалення механізмів державного регулювання інформаційної безпеки України в умовах сучасних цивілізаційних викликів на основі комплексного підходу до їх узгодженої реалізації.

Об'єкт дослідження – процес державного регулювання інформаційної безпеки в умовах сучасних цивілізаційних викликів.

Предмет дослідження – теоретико-методологічні засади, правове та інституційне забезпечення і механізми державного регулювання інформаційної безпеки.

Методи дослідження. Теоретичною та методологічною базою дослідження становлять фундаментальні положення сучасних теорій публічного управління, концепції інформаційного суспільства та національної безпеки, а також наукові розробки вітчизняних і зарубіжних учених щодо природи інформаційної безпеки, викликів і загроз, зумовлених швидким розвитком інформаційного суспільства, технічним прогресом

У процесі дослідження використано сукупність загально- і спеціально-наукових методів. Методи аналізу та синтезу застосовано під час опрацювання наукової літератури та нормативно-правової бази у сфері забезпечення інформаційної безпеки. Для дослідження еволюції понятійно-категоріального

апарату, а також для аналізу розвитку системи державного регулювання інформаційної безпеки в умовах динамічної зміни цивілізаційних викликів застосовано діалектичний метод. Системний підхід став основою для розгляду інформаційної безпеки як невід'ємного елемента загальної системи національної безпеки України, оцінки її структури та функціональної гармонійної взаємодії елементів. Системний підхід застосовано також для аналізу правового та інституційного забезпечення державного регулювання інформаційної безпеки. Як динамічна система взаємодій, що забезпечує трансформацію ресурсів й управлінського впливу в конкретний результат, розуміється також поняття «механізми» державного управління та регулювання. Для оцінки функціонування та взаємодії державних органів, відповідальних за формування та реалізацію державної політики інформаційної безпеки, використано інституційний метод. Порівняльно-правовий та порівняльно-управлінський методи застосовано під час аналізу міжнародного досвіду державного регулювання інформаційної безпеки (зокрема країн ЄС та НАТО) з метою визначення можливостей його адаптації та імплементації у вітчизняну практику. Методологічним підґрунтям досліджень безпекової проблематики є положення загальної теорії систем і теорії відтворення, теорії ризиків та катастроф, а також концептуальні положення теорії соціальних конфліктів.

Застосування зазначених методів та підходів забезпечило об'єктивність та комплексність дослідження, дозволило виокремити наукову новизну, вирішити поставлені завдання.

Інформаційну базу дослідження склали діючі нормативно-правові акти України та міжнародні правові документи у сфері інформаційної безпеки, офіційні матеріали та аналітичні дані Міжнародної організації зі стандартизації / Міжнародної електротехнічної комісії, Державного центру кіберзахисту Держспецзв'язку, Ukrainian Business Award тощо, наукові публікації, монографічні дослідження і матеріали періодичних видань провідних вітчизняних і зарубіжних учених та практиків у галузі національної та інформаційної безпеки, а також власні аналітичні напрацювання автора, інформаційні дані з відкритих Інтернет-ресурсів.

Наукова новизна одержаних результатів полягає в теоретико-методологічному обґрунтуванні та розробленні науково-практичних положень щодо вдосконалення державного регулювання інформаційної безпеки в умовах сучасних цивілізаційних викликів. У межах проведеного дослідження сформульовано такі положення наукової новизни:

вперше:

- розроблено концептуальну модель взаємозв'язку цивілізаційної, національної та інформаційної безпеки, яка відображає їх функціональну взаємодію задля забезпечення стійкості держави і суспільства в умовах інформаційно-цифрової цивілізаційної трансформації; при цьому цивілізаційна безпека постає ширшим рівнем осмислення системних трансформацій і загроз, здатних одночасно впливати на різні сфери безпекового середовища;
- розроблено превентивно-адаптивну модель державного регулювання, яка відображає циклічність управлінського впливу на систему інформаційної безпеки та містить в собі три функціональні контури: превентивно-прогностичний, регуляторно-реактивний та оціночно-адаптаційний, яка на підставі систематизації демонструє причинно-наслідкові взаємозв'язки між сучасними цивілізаційними викликами та інформаційними загрозами, що є результатом цивілізаційних трансформацій, передумовами реформування державного регулювання інформаційної безпеки.

удосконалено:

- поглиблено уявлення про механізм державного регулювання сфери інформаційної безпеки, як складну, багаторівневу та динамічну систему, що містить в собі політичний, нормативно-правовий, організаційний, інформаційно-цифровий (технологічний), економічний та мотиваційний компоненти, функціональним завданням яких є забезпечення захищеності національних інтересів, суверенітету та кіберстійкості в умовах сучасних цивілізаційних викликів;
- критеріально-адаптаційний підхід до використання зарубіжних механізмів державного регулювання інформаційної безпеки в Україні, де оцінювання міжнародних регуляторних практик відбувається за критеріями:

нормативно-правової сумісності, інституційної спроможності, безпекової релевантності, ресурсної забезпеченості, превентивності та адаптивності, дотримання прав людини, що дозволяє забезпечити обґрунтований вибір зарубіжних практик з урахуванням актуальних інформаційних загроз, інституційних можливостей і пріоритетів національної безпеки України на основі трьохетапного алгоритму визначення правової допустимості, управлінської доцільності та способу адаптації відповідних механізмів до національних умов;

- комплексний підхід до реалізації механізмів державного регулювання інформаційної безпеки України в умовах сучасних цивілізаційних викликів, який ґрунтується на функціональному узгодженні політичного, нормативно-правового, організаційного, інформаційно-цифрового (технологічного), економічного та мотиваційного компонентів та передбачає поетапну реалізацію управлінських заходів у межах оперативного, тактичного і стратегічного рівнів реалізації управлінських рішень, що створює передумови для підвищення превентивності, адаптивності та стійкості державного регулювання інформаційної безпеки на основі циклічності управлінського процесу та постійного зворотного зв'язку між результатами реалізації заходів і коригуванням регуляторних пріоритетів.

набули подальшого розвитку:

- уявлення про інформаційне суспільство як етап цивілізаційного розвитку, основні підходи до визначення сутності поняття «інформація», які трансформують сучасний інформаційний простір до мережевих, знаннєвих, цифрових та алгоритмізованих форм суспільної організації, що свідчить про поступове набуття інформаційними процесами цивілізаційного значення та спричиняє появу актуальних підходів до розуміння сутності поняття «інформаційно-цифрова цивілізаційна трансформація» як системного процесу якісних змін суспільних, економічних, політичних та управлінських відносин, зумовлений перетворенням інформації і знань на стратегічні ресурси розвитку, глобальним поширенням цифрових технологій, мережевих форм взаємодії та алгоритмічних систем, унаслідок чого змінюються механізми функціонування

держави, суспільства та взаємодії людини з інформаційним середовищем, що надає змогу уникнути технологічного детермінізму, і в якості чинників цивілізаційної динаміки. розглядати також політичні інститути, систему державного управління, суспільні цінності, правові механізми, культуру, освіту та здатність суспільства адаптуватися до нових форм інформаційної взаємодії;

- теоретико-правові засади нормативно-правового забезпечення державного регулювання інформаційної безпеки, що передбачає систематизацію нормативно-правових актів за основними сферами регуляторного впливу та формування структурованої моделі їх взаємозв'язку; виокремлено фундаментальні нормативно-правові блоки, здатні до змістового оновлення відповідно до змін законодавства та інформаційного середовища, а також обґрунтовано доцільність їх інтеграції з інформаційно-правовими системами для оперативного відстеження нормативних змін, що створює передумови для підвищення системності, актуальності та адаптивності правового забезпечення державного регулювання інформаційної безпеки;
- систематизація інституційного забезпечення державного регулювання інформаційної безпеки, що вирізняється своєю ієрархічною побудовою, включає в себе не лише уповноважені органи та установи, а й управлінські відносини, принципи, процедури, функції та механізми їх взаємодії. Виділено рівні функціонального призначення суб'єктів публічного управління за їх роллю в забезпеченні інформаційної стійкості держави, що дозволяє обґрунтувати необхідність міжвідомчої координації, функціональної узгодженості та залучення наукових установ, приватного сектору й інститутів громадянського суспільства до реалізації державної політики інформаційної безпеки.

Практичне значення отриманих результатів полягає у розробленні науково-методичного забезпечення щодо удосконалення механізмів державного регулювання інформаційної безпеки в умовах сучасних цивілізаційних викликів. Підтвердженням наукової та практичної цінності отриманих результатів дослідження є:

- результати дисертаційного дослідження були використані при

розробці робочих програм і викладанні навчальних дисциплін «Теорія державного управління» за програмою підготовки освітнього рівня «бакалавр» у ЗВО «Відкритий міжнародний університет розвитку людини «Україна» (довідка про впровадження № 13/23-268 від 30 вересня 2026 р.);

- науково-практичні результати та рекомендації дисертаційного дослідження були використані у науково-дослідній діяльності Закладу вищої освіти «Відкритий міжнародний університет розвитку людини «Україна», зокрема під час виконання науково-дослідної теми кафедри міжнародних відносин та політичного консалтингу «Воєнно-стратегічний розвиток сучасної України: міжнародно-політичні виклики, державні інтереси, безпека» (державний реєстраційний номер 0124U000322), що дозволило розробити науково-методичне забезпечення щодо удосконалення механізмів державного регулювання інформаційної безпеки в умовах сучасних цивілізаційних викликів (довідка про впровадження № 13/23/681д від 30.09.2026 р.);
- науково-практичні результати та рекомендації дисертаційного дослідження були використані у практичній діяльності Управління протидії кіберзлочинам в місті Києві Департаменту кіберполіції Національної поліції України, зокрема під час розробки аналітичних матеріалів, експертних рекомендацій та проведення прикладних досліджень з питань інформаційної безпеки й державного управління, що дозволило оптимізувати організаційно-управлінські процеси в діяльності підрозділу (довідка про впровадження № 132.5/38/100-2026 від 01.10.2026 р.);
- науково-практичні результати та рекомендації дисертаційного дослідження були використані у практичній діяльності Аналітичного центру «Український інститут політики», зокрема під час розробки аналітичних матеріалів, експертних рекомендацій та проведення прикладних досліджень з питань інформаційної безпеки та державного управління, що дозволило підвищити якість аналітичного забезпечення управлінських рішень та поглибити практичну складову навчально-методичних матеріалів у сфері державного регулювання інформаційної безпеки (довідка про впровадження № 519 від 01.10.2026 р.).

Особистий внесок здобувача. Дисертація є самостійно виконаною науковою працею, у якій автором особисто обґрунтовано теоретико-методологічні засади та розроблено науково-практичні рекомендації щодо вдосконалення державного регулювання інформаційної безпеки в умовах сучасних цивілізаційних викликів. Усі основні наукові положення, висновки та пропозиції, що становлять наукову новизну дисертаційного дослідження, сформульовано автором особисто.

Апробація матеріалів дисертації. Основні науково-теоретичні та практичні результати дисертаційного дослідження були оприлюднені на: V Міжнародній науково-практичній конференції «Сучасні аспекти модернізації науки в Україні: стан, проблеми, тенденції розвитку» (Венеція, 7 січня 2021 р.); VI Науково-практичній онлайн-конференції студентів, аспірантів і молодих вчених «Актуальні питання сучасної стратегії розвитку України: виклики, пріоритети та прогнози» (Київ, 14 травня 2026 р.); VII Міжнародній науковій конференції «Цифрове наукове суспільство: соціально-економічні, правові та міжнародні аспекти» (Харків, 31 липня 2026 р.); VI Міжнародній науково-практичній конференції «Modern Science: Research, Economy and Innovation» (Загреб, 2 вересня 2026 р.).

Публікації. Основні положення дисертаційного дослідження висвітлено у 11 наукових працях, з яких 5 статей у наукових фахових виданнях України, 2 публікації у інших виданнях та 4 тези наукових доповідей.

Структура та обсяг дисертації. Загальний обсяг дисертації складає 248 сторінок. Робота складається з анотації, вступу, трьох розділів, висновків, списку використаних джерел та додатків. Дисертація містить 16 таблиць, 13 рисунків та 4 додатки. Список використаних джерел містить 217 найменувань.

РОЗДІЛ І
ТЕОРЕТИКО-МЕТОДОЛОГІЧНІ ЗАСАДИ ДЕРЖАВНОГО РЕГУЛЮВАННЯ ІНФОРМАЦІЙНОЇ БЕЗПЕКИ В УМОВАХ ЦИВІЛІЗАЦІЙНИХ ТРАНСФОРМАЦІЙ

1.1. Теоретичні засади становлення інформаційного суспільства в контексті сучасних цивілізаційних трансформацій

Нині у світі інформація є ключовим ресурсом суспільного розвитку, економіки, державного управління та національної безпеки. Цифровізація, поширення інформаційно-комунікаційних технологій, глобальних мереж, штучного інтелекту, хмарних сервісів і цифрових платформ не лише збільшили обсяги створення та поширення інформації, а й посилили її роль у функціонуванні держави й суспільства. Якщо індустріальне суспільство спиралося переважно на матеріальні ресурси, енергію, капітал і виробничі потужності, то інформаційне – на здатність створювати, обробляти, передавати, захищати та використовувати інформацію.

Водночас поняття «інформація» не має єдиного загальновизнаного визначення. Його застосовують у філософії, інформатиці, кібернетиці, теорії комунікацій, економіці, соціології, праві, державному управлінні та сфері національної безпеки. Різні підходи акцентують її зміст, здатність зменшувати невизначеність, передаватися, бути ресурсом, впливати на рішення або мати певний правовий режим.

Термін «інформація» походить від латинського «informatio» – пояснення, повідомлення, відомості, формування уявлення про предмет чи явище [73]. У повсякденності нею називають дані або повідомлення, що дають змогу пізнати навколишній світ. У науці зміст цього поняття ширший і залежить від сфери використання.

Одним із найдавніших є розуміння інформації як знань або відомостей про об’єктивну дійсність. У цьому разі вона пов’язана з пізнанням: людина отримує, осмислює, зберігає та використовує дані про події, об’єкти й процеси для

формування знань. Такий підхід характерний передусім для гуманітарних наук, де інформація розглядається не просто як сигнал, а як зміст, наділений значенням для суб'єкта.

У XX ст. завдяки розвитку теорії комунікації, кібернетики та математичних методів інформація набула нового наукового змісту. Значний внесок у її сучасне розуміння зробив американський математик К. Шеннон. У праці «Математична теорія комунікації» він запропонував математичне визначення обсягу інформації та започаткував теорію інформації [205]. К. Шеннон розмежував кількісну характеристику інформації та її зміст, що дало змогу вимірювати її незалежно від смислу повідомлення.

Його дослідження стало важливим для розвитку телекомунікацій, комп'ютерних систем і цифрових технологій. К. Шеннон показав, що інформація пов'язана з невизначеністю: чим менш передбачуване повідомлення, тим вища його математична інформаційна цінність [205]. Так виникло поняття інформаційної ентропії, яке стало основою цифрового передавання й оброблення даних.

Водночас теорія К. Шеннона не досліджувала зміст повідомлень. Її кількісні показники визначають інформаційний обсяг, але не семантичну істинність чи суспільне значення. Тому два повідомлення можуть бути рівними за обсягом інформації, але мати різні наслідки. Для інформаційної безпеки важливі не лише обсяг, а й достовірність, актуальність, цілісність інформації та її вплив на поведінку людей.

Інший напрям сучасного розуміння інформації сформувала кібернетика. Н. Вінер у своїх працях розглядав інформацію через управління, комунікацію та зворотний зв'язок [214]. У кібернетичному підході вона є умовою функціонування складних систем, оскільки сигнали дають змогу отримувати дані про власний стан, довкілля та наслідки дій. За Н. Вінером, інформація є невід'ємною складовою управління. Система, неспроможна отримувати, обробляти й використовувати інформацію, поступово втрачає здатність адаптуватися до змін середовища, у тому числі це особливо важливо для державного управління, адже результативність рішень залежить від якості

інформації, на якій вони ґрунтуються.

Згодом інформацію почали трактувати як економічний ресурс, саме Ф. Махлуп дослідив створення й поширення знань в економіці США [182]. Він започаткував системне вивчення економіки знань і довів, що виробництво, оброблення та поширення знань є важливою частиною економічної діяльності. До виробництва знань він зарахував освіту, науку, ЗМІ, інформаційні технології та послуги.

Подальший розвиток цього напряму пов'язують із М. Поратом, який розробив методику оцінювання інформаційної діяльності та визначив її види, спрямовані на створення, оброблення й передавання економічно значущої інформації [198]. Так інформацію почали розглядати не лише як допоміжний ресурс, а й як самостійне джерело створення вартості.

Інформація може бути водночас ресурсом, продуктом і засобом управління. На відміну від матеріальних ресурсів, її можна багаторазово використовувати без втрати первинного змісту. Її цінність залежить від актуальності, достовірності, повноти, доступності та умов застосування.

У сучасному суспільстві ця властивість інформації виявляється особливо виразно. Ті самі відомості державний орган використовує для управлінських рішень, підприємство – для прогнозування ринку, науковець – у дослідженнях, громадянин – у повсякденному виборі, військове командування – для оцінки оперативної ситуації. Тому інформація є універсальним ресурсом майже всіх сфер суспільної діяльності.

В Україні правове розуміння інформації має свою специфіку. Вітчизняне законодавство, зокрема Закон України «Про інформацію», розглядає її крізь призму системи інформаційних відносин, що охоплюють створення, збирання, одержання, зберігання, використання, поширення та захист інформації. [92].

Окремого значення набуває інформація про фізичну особу. Закон України «Про інформацію» визначає персональні дані як відомості або сукупність відомостей про ідентифіковану чи таку, що може бути ідентифікована, особу [92]. Отже, правове розуміння інформації охоплює приватність, права людини, доступ до відомостей та їх захист. Закон також визначає види інформації й

особливості правового режиму. Цей Закон та станом на 2026 рік залишається основним нормативним актом в інформаційній сфері.

Що стосується вітчизняних науковців, то можемо виділити науковицю О. Кохановську, яка, досліджуючи інформацію з позицій цивільного права, акцентує увагу на її особливій нематеріальній природі та багатоаспектності як об'єкта цивільних прав. Дослідниця розглядає інформацію у декількох взаємопов'язаних аспектах: як особисте немайнове благо, що охороняється цивільним законодавством; як результат інтелектуальної, творчої діяльності; а також як інформаційний продукт, ресурс чи документ, який за певних умов може набувати ознак товару та виступати предметом цивільно-правових відносин [49]. Завдяки цьому дослідженню, можна характеризувати інформацію як специфічний нематеріальний об'єкт, правовий режим якого залежить від форми її існування, змісту та характеру використання.

Науковець В. Цимбалюк розглядає інформацію передусім крізь призму інформаційного права та суспільних інформаційних відносин. У межах його підходу, інформація – відомості, дані, знання та інші інформаційні прояви – становить основний предмет суспільних відносин в інформаційній сфері [132]. Відповідно, інформаційні відносини, що виникають у процесі створення, одержання, накопичення, зберігання, використання та поширення інформації, потребують комплексного правового регулювання. Дослідник обґрунтовує інформаційне право як комплексне правове утворення, у межах якого поєднуються публічно-правові та приватноправові механізми регулювання відносин щодо інформації.

В контексті становлення та розвитку інформаційного суспільства розглядає інформацію В. Бебик. На його думку, інформаційні ресурси, знання та комунікаційні процеси набувають визначального значення для функціонування суспільних і політичних інститутів [5]. В. Бебик пов'язує розвиток інформаційного суспільства з високим рівнем інформаційної культури, що передбачає створення, опрацювання, поширення та використання інформації. За такого підходу інформація постає не лише засобом комунікації, а й одним із ключових ресурсів суспільного розвитку та трансформації суспільно-політичних

відносин.

Як один із визначальних ресурсів розвитку сучасного інформаційного суспільства, значення якого посилюється в умовах глобалізації, інформатизації та поширення інформаційно-комунікаційних технологій, постає інформація в роботах О. Сосніна. У працях науковця інформаційний ресурс пов'язується з функціонуванням держави, суспільно-політичними процесами та необхідністю формування відповідної державної політики щодо його створення, використання, збереження і захисту. Відтак інформація в умовах інформаційного суспільства набуває не лише соціально-комунікаційного, а й стратегічного та державно-управлінського значення [117].

Отже, у сучасних наукових і нормативних джерелах можна виокремити кілька ключових підходів до розуміння інформації:

– гносеологічний, згідно з яким інформація постає як відомості та знання про об'єктивну реальність;

– математико-комунікаційний, насамперед репрезентований теорією К. Шеннона, у межах якої інформація кількісно визначається ступенем зменшення рівня невизначеності;

– кібернетичний, де інформація виступає основою комунікації, управління та зворотного зв'язку;

– економічний, відповідно до якого інформація і знання є самостійним виробничим фактором та джерелом економічної цінності;

– правовий, у якому інформація розглядається як об'єкт інформаційних правовідносин із визначеним режимом доступу, використання та захисту.

У сучасному науковому дискурсі поняття «інформація» характеризується багатогранністю та міждисциплінарністю, що зумовлює відсутність єдиного усталеного підходу до його трактування. Залежно від предметної сфери, інформація розглядається як сукупність відомостей і даних, засіб комунікації, форма представлення знань, стратегічний ресурс, об'єкт правового регулювання та важливий чинник управлінських процесів. Особливого значення розуміння сутності інформації набуває у сфері публічного управління та забезпечення

інформаційної безпеки, де вона одночасно виступає ресурсом державного управління та об'єктом захисту. З огляду на це доцільним є систематизувати основні наукові та нормативно-правові підходи до визначення сутності поняття «інформація» (табл. 1.1.).

Таблиця 1.1

Наукові та нормативно-правові підходи до визначення сутності поняття «інформація»

Джерело	Визначення	Підхід
Закон України «Про інформацію»	Інформація – це «будь-які відомості та/або дані, які можуть бути збережені на матеріальних носіях або відображені в електронному вигляді».	нормативно-правовий
Математична теорія комунікації (К. Шеннон)	Інформація розглядається через кількісне вимірювання та зменшення невизначеності під час передавання повідомлень; семантичний зміст повідомлення не є визначальним.	математико-комунікаційний
Кібернетична концепція (Н. Вінер)	Інформація – невід'ємна складова процесів управління, комунікації та зворотного зв'язку, що забезпечує функціонування й саморегуляцію складних систем.	кібернетичний
Підхід Г. Бейтсона	Інформація концептуалізується як відмінність, що здатна спричинити іншу відмінність, тобто як зміна або сигнал, який набуває значення для системи, що його сприймає.	системно-кібернетичний
Семантичний підхід (Л. Флоріді)	Інформація пов'язується з належним чином сформованими, змістовними та істинними даними, що дає змогу відмежувати її від простого масиву неструктурованих даних.	філософсько-семантичний
Концепція Ф. Махлупа	Інформація та знання – важливі економічні ресурси, виробництво, поширення та використання яких формують специфічну сферу суспільно-економічної діяльності.	інформаційно-економічний
Погляди М. Пората	Інформація – економічно значущий ресурс, а діяльність щодо її створення, оброблення, зберігання та поширення становить основу інформаційного сектору економіки.	економіко-інформаційний
Концепція мережевого суспільства (М. Кастельс)	Інформація набуває значення стратегічного ресурсу, а процеси її генерування, оброблення та передавання за допомогою інформаційних технологій істотно впливають на економічні, соціальні та владні відносини.	соціологічний / мережевий
І. Арістова	Інформація розглядається у взаємозв'язку з інформаційними відносинами, інформаційними потребами держави, суспільства та особи, а також із формуванням і реалізацією державної інформаційної політики.	державно-управлінський / інформаційно-правовий

Продовження табл.1.1

Джерело	Визначення	Підхід
О. Кохановська	Інформація досліджується як специфічний нематеріальний об'єкт цивільних правовідносин, якому притаманні особливості створення, одержання, використання, поширення та правової охорони.	цивільно-правовий
Б. Кормич	Інформація – об'єкт суспільних та інформаційно-правових відносин, функціонування якого пов'язане з необхідністю забезпечення балансу інформаційних прав і свобод та захисту інформаційної безпеки держави, суспільства й особи.	інформаційно-правовий / безпековий
Безпековий контекст (В. Ліпкан, Ю. Максименко, В. Желіховський)	Інформація набуває значення стратегічно важливого ресурсу, захист якого та забезпечення належного функціонування інформаційної сфери є складовими забезпечення інформаційної й національної безпеки держави.	інформаційно-безпековий

Джерело: складено автором на основі [2; 46; 47; 49; 50; 56; 92; 144; 150; 151; 169; 182; 198; 199; 205; 206; 213; 214]

Узагальнення наведених підходів у табл. 1.1. свідчить, що поняття «інформація» має міждисциплінарний характер і не може бути вичерпно розкрите в межах одного наукового підходу. Якщо в математико-комунікаційній парадигмі інформація характеризується насамперед через кількісні параметри та здатність зменшувати невизначеність, то філософсько-семантичний підхід акцентує увагу на її змістовності та істинності, соціологічний – на ролі інформації у трансформації суспільних відносин, а правовий – на її властивостях як специфічного об'єкта правового регулювання. Водночас у контексті публічного управління та забезпечення інформаційної безпеки інформація набуває значення стратегічного ресурсу держави, від належного формування, циркуляції, використання та захисту якого безпосередньо залежать якість управлінських рішень, стійкість державних інститутів та спроможність держави протидіяти сучасним інформаційним загрозам.

На нашу думку, в контексті державного регулювання інформаційної безпеки поняття «інформація» доцільно розглядати ширше за нормативно закріплену категорію відомостей та/або даних. Інформація – це стратегічно значущий нематеріальний ресурс, представлений сукупністю відомостей і даних,

що створюються, одержуються, обробляються, зберігаються, передаються та використовуються у процесах суспільної комунікації й публічного управління та здатні впливати на стан особи, суспільства, держави, функціонування її інститутів і прийняття управлінських рішень. Таке розуміння дає змогу розглядати інформацію значно ширше, і одночасно як об'єкт забезпечення інформаційної безпеки держави.

Зміна ролі та значення інформації в економіці та суспільстві сприяла формуванню концепції інформаційного суспільства. Поява цієї концепції стала результатом еволюційного розвитку телекомунікацій, комп'ютерної техніки, масових комунікацій, науки й освіти.

Водночас розвивалася теорія постіндустріального суспільства. У 1973 році Д. Белл у праці «Прийдешнє постіндустріальне суспільство» описав зміни в розвинених країнах, спричинені зростанням значення послуг, науки, освіти та професійної діяльності [145]. На його думку, головним ресурсом стають теоретичні знання, а університети й наукові установи набувають особливої ваги.

Подальший розвиток концепція інформаційного суспільства отримала у працях Й. Масуди. У 1980 році він написав книгу «Інформаційне суспільство як постіндустріальне суспільство», де розглядав комп'ютеризацію та інформаційні технології як чинники масштабної трансформації економічних, соціальних і політичних систем, що породжує нові види інтелектуальної праці та змінює суспільну структуру [183].

Тритомна праця «Інформаційна епоха: економіка, суспільство і культура» М. Кастельса стала вагомим внеском у розвиток концепції інформаційного суспільства. Перший том було опубліковано у 1996 році, у якому запропоновано концепцію мережевого суспільства [150]. М. Кастельс вважав, що цифрові технології створюють нові мережеві форми організації, де інформаційні потоки визначають упорядкування економічної та соціальної діяльності. Науковець наголошував, що інформаційні технології не обмежуються прискоренням передавання повідомлень. Вони трансформують організаційну будову суспільства, адже дають змогу узгоджувати діяльність людей і організацій незалежно від просторової віддаленості. Формуються глобальні мережі

виробництва, фінансової діяльності, комунікації, науки та управління. Саме мережевий принцип стає однією з визначальних рис сучасного інформаційного суспільства.

Водночас інформаційне суспільство не можна розглядати лише як результат масштабного поширення комп'ютерів та інтернету. Такий технологічно орієнтований підхід є недостатнім. Для інформаційного суспільства характерна всебічна трансформація соціальних зв'язків, економічних моделей, освітньої системи, державного управління, політичної комунікації та повсякденного побуту.

ЮНЕСКО трактує концепцію інформаційного суспільства у поєднанні з ідеями інформаційної доби, інформаційної революції та суспільства знань [210]. У документах організації підкреслюється, що поширення цифрових технологій істотно пришвидшило процеси створення, обміну й оброблення знань, сприяючи виникненню глобальних мереж взаємодії [212].

Визначальне значення для формування міжнародного підходу до інформаційного суспільства мав Всесвітній саміт з питань інформаційного суспільства (WSIS), організований під егідою ООН і Міжнародного союзу електрозв'язку. Першу частину саміту було проведено 10-12 грудня 2003 року у м. Женева, а другу 16-18 листопада 2005 року у м. Туніс [177]. Женевська декларація принципів охарактеризувала інформаційне суспільство як людиноорієнтовану й інклюзивну модель, у якій кожна людина може створювати, отримувати, використовувати та поширювати інформацію і знання [178].

Отже, міжнародне трактування інформаційного суспільства поступово відійшло від суто технологічного бачення. Цифрові технології стали сприйматися не як кінцева мета, а як інструмент розширення доступу до знань, розвитку комунікацій, освіти, економіки та громадянської активності. До його ключових ознак належать посилення ролі інформації та знань в усіх сферах суспільного життя, збільшення кількості інформаційних професій, цифрова трансформація державного управління, розбудова глобальних комунікаційних мереж і зростання значення цифрової грамотності. Водночас цифровізація

спричиняє появу нових ризиків, зокрема кіберзлочинності, витоків даних, інформаційних маніпуляцій, дезінформації та залежності від цифрової інфраструктури.

У міру посилення залежності держави, економіки й суспільства від інформаційних систем зростають і можливі наслідки порушення їхньої роботи. Отже, інформаційне суспільство одночасно відкриває нові перспективи розвитку та породжує нові типи загроз.

Формування інформаційного суспільства нерозривно пов'язане з історією інформаційних революцій. Інформаційну революцію доцільно визначати як масштабну зміну способів створення, фіксації, зберігання, передавання та використання інформації, що зумовлює трансформації у сфері комунікацій, економіки, державного управління й суспільного життя. На відміну від окремого технологічного нововведення, інформаційна революція змінює базові принципи функціонування інформаційного середовища.

У наукових працях представлено різні варіанти періодизації інформаційних революцій. Один із них ґрунтується на дослідженнях П. Друкера, який розглядав масштабні зміни інформаційної сфери крізь призму послідовного виникнення писемності, книги, друкарства та сучасної цифрової революції [163]. Інші науковці розширюють цю схему, додаючи розвиток телеграфу, телефону, радіо, телебачення, комп'ютерних технологій та інтернету.

Розвиток людської цивілізації нерозривно пов'язаний із трансформацією способів створення, накопичення, зберігання, опрацювання та поширення інформації. На різних історичних етапах поява принципово нових засобів інформаційної взаємодії не лише змінювала комунікаційні можливості суспільства, а й суттєво впливала на характер суспільних відносин, організацію державного управління, економічні процеси та механізми поширення знань.

Масштабність таких змін дає підстави розглядати їх як інформаційні революції, кожна з яких знаменувала перехід до якісно нового рівня функціонування інформаційного середовища [114].

Перші інформаційні революції були пов'язані насамперед із подоланням просторових і часових обмежень у передаванні суспільно значущих відомостей.

Виникнення писемності створило можливості для фіксації та тривалого збереження інформації, а поширення книгодрукування забезпечило її масове тиражування та значно розширило доступ до знань. Подальший розвиток засобів електричного зв'язку сприяв істотному прискоренню інформаційного обміну та поступовому формуванню глобального комунікаційного простору.

Якісно новий етап розпочався з поширення електронно-обчислювальної техніки та цифрових технологій. Інформація стала не лише об'єктом зберігання і передавання, а й предметом автоматизованого опрацювання. Розвиток комп'ютерних мереж та Інтернету перетворив інформаційні потоки на глобальні, транскордонні та практично безперервні. Унаслідок цього суттєво зросли обсяги інформації, швидкість її поширення та кількість суб'єктів, здатних одночасно виступати її виробниками, споживачами і поширювачами.

Сучасний етап розвитку інформаційних трансформацій характеризується активним розвитком штучного інтелекту, великих даних, хмарних технологій, Інтернету речей та алгоритмічних систем. Особливістю цього етапу є те, що технології дедалі частіше виконують не лише функцію передавання чи опрацювання інформації, а й здатні здійснювати її автоматизований аналіз, генерувати новий контент, прогнозувати процеси та використовуватися для підтримки управлінських рішень. Вищезазначене чітко вказує на поступовий перехід від суто цифрового інформаційного середовища до інтелектуалізованого та алгоритмізованого простору суспільної взаємодії.

Отже, інформаційні революції принесли численні переваги, але водночас створили безліч загроз для національної та міжнародної безпеки. Значна залежність держав від інформаційних ресурсів суттєво підвищує їхню вразливість перед загрозами інформаційній безпеці. Безумовно, інформаційні революції відкривають нові широкі можливості для економічного й політичного розвитку, а також для досягнення воєнно-стратегічних цілей [35].

Водночас кожне розширення інформаційних можливостей супроводжувалося виникненням нових ризиків і загроз. Якщо на ранніх етапах основними проблемами були фізичне збереження носіїв інформації, достовірність відомостей та обмеження доступу до них, то цифровізація

актуалізувала проблеми несанкціонованого доступу, порушення конфіденційності, модифікації та знищення даних, кібератак, дезінформації та інформаційно-психологічного впливу. Сучасні технології штучного інтелекту додатково посилюють проблему масштабування інформаційних впливів, створення синтетичного контенту та використання алгоритмічних інструментів для маніпулювання інформаційним середовищем [190].

Отже, інформаційні революції доцільно розглядати не лише як послідовність технологічних нововведень, а як складові більш широкої цивілізаційної трансформації. Зміна способів роботи з інформацією безпосередньо впливає на функціонування держави, суспільства та особи, одночасно формуючи нові об’єкти захисту, ризики й напрями державного регулювання. Узагальнення основних етапів інформаційних революцій та їх значення для формування сучасної проблематики інформаційної безпеки представлено в табл. 1.2.

Таблиця 1.2

Основні етапи інформаційних революцій та їх вплив на розвиток суспільства

Інформаційна революція	Орієнтовний період	Ключові технологічні зміни	Трансформація інформаційних процесів	Значення для інформаційної безпеки
Перша – виникнення писемності	IV–III тис. до н. е.	Формування систем письма та матеріальних носіїв інформації	З’явилася можливість фіксувати, накопичувати, зберігати та передавати знання незалежно від безпосереднього спілкування	Виникла потреба у збереженні документів, обмеженні доступу до окремих відомостей, забезпеченні достовірності повідомлень
Друга – винайдення книгодрукування	XV–XVI ст.	Поширення технології друку, масове тиражування книг і документів	Значно збільшилися масштаби поширення інформації та доступність знань; сформувалися передумови виникнення масової комунікації	Посилилося значення контролю інформаційних потоків, авторства, достовірності та регулювання поширення інформації

Продовження табл. 1.2

Інформаційна революція	Орієнтовний період	Ключові технологічні зміни	Трансформація інформаційних процесів	Значення для інформаційної безпеки
Третя – розвиток електричного зв'язку	XIX – перша половина XX ст.	Телеграф, телефон, радіо, фотографія, згодом – телебачення	Передавання інформації стало можливим на значні відстані з істотним скороченням часу комунікації	Актуалізувалися питання захисту каналів зв'язку, конфіденційності повідомлень, протидії перехопленню та інформаційному впливу
Четверта – комп'ютерна революція	Друга половина XX ст.	Електронно-обчислювальна техніка, мікропроцесори, автоматизовані інформаційні системи	Відбувся перехід до цифрового опрацювання, систематизації та зберігання великих обсягів даних	Сформувалися нові загрози несанкціонованого доступу, втрати чи модифікації даних; набули розвитку комп'ютерна та інформаційна безпека
П'ята – мережева (цифрова) революція	Кінець XX – початок XXI ст.	Інтернет, глобальні інформаційно-комунікаційні мережі, мобільний зв'язок, соціальні медіа	Інформаційний обмін набув глобального, транскордонного та практично безперервного характеру	Поширилися кіберзагрози, дезінформація, інформаційні операції, порушення приватності та загрози критичній інформаційній інфраструктурі
Шоста – інтелектуально-алгоритмічна революція	XXI ст., сучасний етап	Штучний інтелект, машинне навчання, великі дані, хмарні технології, IoT, генеративні системи	Інформаційні системи не лише зберігають і передають інформацію, а й автоматично аналізують її, генерують новий контент та підтримують прийняття рішень	Формуються нові ризики: алгоритмічні маніпуляції, deepfake, автоматизована дезінформація, витоки даних, кібератаки із застосуванням ШІ та проблеми контролю над алгоритмічними системами

Джерело: узагальнено автором на основі власних досліджень

Водночас інформаційні революції мають не лише позитивні наслідки.

Розширення комунікаційних можливостей породжує нові загрози: друк посилив вплив на громадську думку, телеграф і радіо – масове політичне та військове інформування, а цифрові мережі сприяли кібератакам, поширенню дезінформації, викраденню даних та інформаційним операціям.

Отже, історія інформаційних революцій підтверджує: зі зростанням ролі інформації в суспільстві посилюється потреба в її захисті, що закономірно зумовило формування поняття інформаційної безпеки, яке ми будемо досліджувати у ході нашої роботи.

Проведений аналіз еволюції інформаційних процесів дає підстави стверджувати, що сучасний етап суспільного розвитку вже не може бути вичерпно охарактеризований лише кількісним зростанням обсягів інформації, поширенням інформаційно-комунікаційних технологій або цифровізацією окремих сфер суспільного життя. Йдеться про значно глибші трансформації, які охоплюють економічні, політичні, соціальні, культурні та управлінські відносини, змінюють характер взаємодії між державою, суспільством і людиною та поступово набувають цивілізаційного масштабу. Через те дослідження інформаційного суспільства доцільно продовжити крізь призму цивілізаційного підходу та дозволить розглянути інформаційні зміни як складову більш широкої трансформації способу організації та функціонування сучасного суспільства.

Цивілізаційний підхід дозволяє вийти за межі суто технологічного трактування сучасних перетворень. Поява нової технології сама по собі ще не означає формування нового типу цивілізації. Визначальним є те, наскільки технологічні зміни трансформують базові принципи організації суспільного життя, систему цінностей, характер економічної діяльності, механізми політичної комунікації, способи накопичення й передавання знань, структуру управління та взаємодію між соціальними суб’єктами. За таких обставин можна стверджувати, що інформаційні технології виступають не кінцевою метою трансформації, а одним із її ключових чинників [126].

Передумови такого бачення простежуються в концепціях другої половини XX ст. Так, З. Бжезінський, характеризуючи перехід до технотронної ери, звертав увагу на те, що розвиток науки, електроніки та засобів комунікації

здатний спричинити зміни не лише у виробництві, а й у соціальній структурі, політичних відносинах та характері суспільної взаємодії [148]. Технологічний розвиток за такого підходу набуває суспільно-політичного значення, оскільки впливає на способи здійснення влади, характер управління та взаємозалежність держав і суспільств.

Подібну логіку цивілізаційної трансформації розвинув Е. Тоффлер у концепції «третьої хвилі» [208]. Науковець розглядав історичний розвиток людства через послідовну зміну великих хвиль суспільної трансформації: аграрної, індустріальної та нової постіндустріальної. Перехід до «третьої хвилі» пов'язувався не лише із впровадженням нових технологій, а з комплексною перебудовою виробництва, комунікацій, сімейних відносин, освіти, політики та суспільної організації. Вищезазначене є надзвичайно важливим для розуміння сучасних процесів, оскільки демонструє, що зміна способів створення, оброблення та поширення інформації здатна бути одним із чинників системної перебудови суспільства.

Отже, інформаційне суспільство доцільно розглядати не як ізольований результат технологічного прогресу, а як складову більш масштабного цивілізаційного переходу. Якщо поняття «інформаційне суспільство» акцентує насамперед на зростанні ролі інформації, знань та інформаційно-комунікаційних технологій у суспільних процесах, то цивілізаційний вимір дає змогу простежити, яким чином ці зміни трансформують фундаментальні засади суспільного розвитку.

У цьому контексті в науковому дискурсі використовується категорія «інформаційна цивілізація». Вона не має єдиного загальновизнаного трактування, однак застосовується для характеристики такого стану суспільного розвитку, за якого інформація, знання та інформаційні технології набувають системоутворювального значення для функціонування основних суспільних інститутів. Інформаційна цивілізація, таким чином, характеризує не тільки технологічний стан суспільства, а й якісні зміни способів комунікації, виробництва, управління, навчання, соціальної взаємодії та прийняття рішень.

Зокрема, С. Ченг розглядає інформаційну цивілізацію як особливу форму

цивілізаційного розвитку, яка не зводиться до простого продовження індустріальної цивілізації. На думку дослідниці, інформаційні технології змінюють способи сприйняття світу, мислення, навчання, прийняття рішень та суспільної взаємодії [153]. Важливим у підході дослідниці є перенесення акценту з технології як технічного засобу на її здатність трансформувати соціальні відносини та інституційні структури.

Інформаційна цивілізація може розглядатися як ширша категорія порівняно з інформаційним суспільством. Якщо останнє характеризує передусім конкретні особливості соціальної організації, пов'язані з домінуванням інформаційних процесів, то поняття інформаційної цивілізації дає змогу охопити довготривалі трансформації економіки, політики, культури, освіти, науки, системи державного управління та способу життя людини. Водночас ототожнювати ці категорії недоцільно, оскільки вони належать до різних рівнів наукового узагальнення.

Відповідно, поняття «інформаційне суспільство», «мережеве суспільство», «суспільство знань» та «інформаційна цивілізація» доцільно розглядати не як взаємовиключні концепції, а як різні теоретичні ракурси дослідження сучасних суспільних трансформацій. Концепція інформаційного суспільства акцентує на ролі інформації та інформаційно-комунікаційних технологій; концепція мережевого суспільства – на мережевій структурі соціальних, економічних і владних відносин; концепція суспільства знань – на здатності суспільства створювати, поширювати й використовувати знання; натомість концепція інформаційної цивілізації дозволяє узагальнити ці процеси на більш високому рівні та розглядати їх як складові масштабної трансформації цивілізаційного розвитку.

Особливе місце в цій системі займає концепція суспільств знань. У Всесвітній доповіді ЮНЕСКО «До суспільств знань» наголошується, що інформаційне суспільство значною мірою ґрунтується на технологічних досягненнях, тоді як поняття суспільств знань охоплює ширші соціальні, етичні, політичні та культурні виміри [212]. Інформація сама по собі ще не є знанням: вона набуває суспільної цінності внаслідок її осмислення, критичного

оцінювання, використання та перетворення на знання. Тому розвиток цифрової інфраструктури не є достатньою умовою формування якісно нового суспільства.

Усе сказане вище підкреслює та має принципове значення для публічного управління. Технологічна спроможність держави накопичувати значні масиви даних ще не гарантує ефективності державного управління. Визначальними стають спроможність перетворювати дані на релевантну інформацію, інформацію – на знання, а знання – на обґрунтовані управлінські рішення. У цьому контексті інформаційний розвиток держави безпосередньо пов'язаний із якістю інституцій, компетентністю суб'єктів публічного управління, відкритістю державних інформаційних ресурсів, розвитком електронної взаємодії та здатністю органів влади функціонувати в умовах швидких технологічних змін.

Сучасний етап цих трансформацій дедалі частіше характеризується також через поняття «цифрова цивілізація». Його використання пов'язане з тим, що цифрові технології перестали бути окремим інструментом здійснення певних видів діяльності та поступово перетворилися на середовище функціонування значної частини суспільних відносин. Економічні операції, публічні послуги, політична комунікація, освіта, наукова діяльність, соціальні зв'язки та значна частина повсякденної комунікації дедалі більше реалізуються через цифрові платформи, мережі та інформаційні системи.

У зв'язку з цим відбувається поступовий перехід від простої інформатизації до цифрової трансформації. Інформатизація передбачала переважно впровадження інформаційних технологій у вже існуючі процеси, тоді як цифрова трансформація змінює саму логіку їх організації, саме це особливо помітно у сфері публічного управління, де цифрові технології змінюють механізми взаємодії держави з громадянами, способи надання адміністративних послуг, організацію міжвідомчої взаємодії, використання державних реєстрів, механізми прийняття рішень та форми громадської участі [193].

Принципово новою ознакою сучасного етапу цивілізаційної трансформації є алгоритмізація суспільних процесів. Якщо попередні інформаційні революції переважно розширювали можливості людини щодо створення, зберігання та передавання інформації, то сучасні алгоритмічні системи здатні самостійно

здійснювати її сортування, аналіз, класифікацію, прогнозування та генерування [194]. Унаслідок цього алгоритми дедалі частіше опосередковують доступ людини до інформації, формують інформаційні потоки, визначають зміст рекомендацій та використовуються під час підготовки управлінських рішень.

Особливу роль у зазначених процесах відіграє штучний інтелект, його поширення вказує на поступовий перехід від цифровізації як переведення інформації та процесів у цифрову форму до інтелектуалізації інформаційного середовища. Штучний інтелект дозволяє опрацьовувати масиви даних, масштаби яких перевищують можливості традиційних методів аналізу, виявляти закономірності, прогнозувати розвиток процесів, автоматизувати окремі управлінські функції та генерувати інформаційний контент [191].

Унаслідок цього змінюється і характер взаємодії людини з інформаційним середовищем. Людина дедалі частіше отримує інформацію не безпосередньо, а через алгоритмічно сформовані інформаційні потоки. Пошукові системи, соціальні мережі, цифрові платформи та рекомендаційні алгоритми фактично здійснюють попередній відбір інформації, визначаючи, які відомості будуть доступні конкретному користувачеві, а технологічні системи починають виконувати функцію інформаційного посередництва між людиною та навколишнім світом [211].

Водночас цивілізаційний характер сучасних інформаційних трансформацій виявляється в їх глобальності. Інформаційні потоки дедалі менше залежать від державних кордонів, а цифрові платформи здатні одночасно охоплювати аудиторію багатьох держав. Виникає глобальний інформаційний простір, у межах якого національні інформаційні системи, засоби масової комунікації, державні інститути, приватні технологічні компанії та окремі користувачі включені у складну систему транскордонної взаємодії.

За таких умов змінюється роль держави в інформаційних процесах. У традиційних моделях суспільної комунікації держава володіла значними можливостями впливу на інформаційний простір у межах власної території. Глобальні цифрові мережі суттєво ускладнили таку модель, значна частина інформаційної інфраструктури, платформ, програмного забезпечення, хмарних

сервісів і технологічних рішень може перебувати поза безпосереднім контролем національних органів влади. Відповідно, публічне управління здійснюється в умовах дедалі більшої технологічної та інформаційної взаємозалежності.

Іншою визначальною рисою сучасних цивілізаційних трансформацій є перетворення даних на стратегічний ресурс. Якщо для індустріальної моделі визначальними ресурсами були сировина, енергія, виробничі потужності та капітал, то в цифровому середовищі дедалі більшого значення набувають масиви даних, технології їх оброблення та здатність перетворювати їх на знання. Володіння інформаційними ресурсами та технологічними можливостями їх аналізу впливає на конкурентоспроможність держав, ефективність економіки та спроможність публічних інституцій.

Водночас зазначені процеси не є однозначно позитивними. Поряд із розширенням доступу до інформації формується цифрова нерівність, яка виявляється не лише у відмінностях доступу до мережі та технологій, а й у нерівності цифрових компетентностей, можливостей використовувати інформаційні ресурси та отримувати переваги від технологічного розвитку. ЮНЕСКО у зв'язку з цим наголошує, що побудова суспільств знань передбачає не лише розвиток інформаційної інфраструктури, а й забезпечення доступу до знань, освіти, свободи вираження поглядів, культурного й мовного різноманіття [212].

Отже, інформаційна та цифрова трансформація має виражений соціальний вимір. Розвиток технологій може сприяти демократизації доступу до знань, підвищенню ефективності державного управління та розширенню можливостей суспільної участі, але водночас здатний посилювати існуючі нерівності, створювати нові форми залежності та змінювати традиційні механізми суспільного контролю.

Ще однією характерною рисою сучасної цивілізаційної трансформації є зміна співвідношення глобального та національного. Інформаційний простір дедалі більше набуває глобального характеру, тоді як відповідальність за забезпечення стабільного функціонування державних і суспільних інститутів значною мірою залишається на рівні національної держави. Виникає своєрідна

суперечність: інформаційні процеси є транскордонними, а механізми державного регулювання переважно обмежені національною юрисдикцією [26].

Зазначене ставить перед системою публічного управління принципово нові завдання. Держава має не лише адаптувати традиційні механізми регулювання до цифрового середовища, а й формувати нові інституційні спроможності, здатні функціонувати в умовах високої швидкості технологічних змін, глобальної взаємозалежності та постійного збільшення обсягів інформації. При цьому предметом державної політики стають не лише інформаційні ресурси як такі, але й цифрові платформи, алгоритмічні системи, дані, технологічна інфраструктура, механізми електронної комунікації та інші елементи сучасного інформаційного простору.

На нашу думку, зазначені зміни дають підстави розглядати сучасну трансформацію інформаційного суспільства як процес, що поступово набуває ознак цивілізаційного переходу. Його сутність полягає не просто в збільшенні кількості інформації чи поширенні цифрових технологій, а в системній зміні способів створення та використання знань, організації економічної діяльності, здійснення публічного управління, політичної комунікації та соціальної взаємодії.

Відтак поняття «інформаційна цивілізація» може бути використане як теоретична конструкція для позначення цивілізаційного стану, за якого інформація, знання та технології їх створення, опрацювання і поширення набувають системоутворювального значення для розвитку суспільства. Водночас категорія «цифрова цивілізація» акцентує увагу на сучасному етапі цього процесу, для якого характерні цифровізація, платформізація, алгоритмізація, розвиток штучного інтелекту та формування глобального цифрового середовища.

Узагальнення розглянутих теоретичних підходів свідчить про поступове розширення наукового розуміння суспільних трансформацій, зумовлених зростанням ролі інформації, знань та інформаційно-комунікаційних технологій. Якщо ранні концепції акцентували увагу переважно на структурних змінах економіки та переході від індустріального до постіндустріального типу розвитку,

то подальші дослідження зосередилися на інформаційних, мережевих, знаннєвих і цифрових характеристиках суспільства. Еволюцію основних концептуальних моделей такого розвитку узагальнено в табл. 1.3.

Таблиця 1.3

Еволюція концептуальних моделей суспільного розвитку в умовах зростання ролі інформації та цифрових технологій

Концептуальна модель	Представник	Основний зміст концепції	Визначальний ресурс	Значення для дослідження цивілізаційних трансформацій
Постіндустріальне суспільство	Д. Белл	Перехід від домінування промислового виробництва до сфери послуг, науки та інтелектуальної діяльності; зростання ролі професійних і технічних груп	Теоретичні знання, наука, освіта	Формує теоретичні передумови розуміння переходу від індустріальної моделі розвитку до суспільства, заснованого на знаннях
Технотронне суспільство	З. Бжезінський	Науково-технологічний розвиток, електроніка та засоби комунікації трансформують суспільні, політичні й управлінські відносини	Наука, технології, електронні комунікації	Демонструє здатність технологічних змін впливати на політичну організацію суспільства, механізми влади та міжнародну взаємозалежність
«Третя хвиля» цивілізаційного розвитку	Е. Тоффлер	Перехід від аграрної та індустріальної цивілізацій до нового типу суспільної організації, пов’язаного з демасифікацією, знаннями, інформацією та новими технологіями	Інформація, знання, технологічні інновації	Дає змогу розглядати інформаційно-технологічні зміни як складову масштабної цивілізаційної трансформації

Продовження табл. 1.3

Концептуальна модель	Представник	Основний зміст концепції	Визначальний ресурс	Значення для дослідження цивілізаційних трансформацій
Інформаційне суспільство	Й. Масуда	Інформація та її виробництво, опрацювання і використання стають одним із визначальних чинників суспільного та економічного розвитку	Інформація, інформаційні технології	Відображає перетворення інформації на один із ключових ресурсів розвитку суспільства
Мережеве суспільство	М. Кастельс	Економічні, політичні та соціальні процеси організовуються через глобальні мережі, а інформаційні потоки набувають визначального значення	Інформаційні потоки, мережі, ІКТ	Пояснює глобалізацію та мережевий характер сучасної суспільної взаємодії, зменшення значення просторових меж для інформаційних процесів
Суспільства знань	UNESCO	Розвиток суспільства пов’язується не лише з доступом до інформації й технологій, а зі створенням, поширенням і використанням знань, освітою, свободою вираження поглядів та культурним різноманіттям	Знання, освіта, людський потенціал	Розширює технологічне трактування інформаційного суспільства соціальним, гуманітарним, етичним і культурним вимірами

Продовження табл. 1.3

Концептуальна модель	Представник	Основний зміст концепції	Визначальний ресурс	Значення для дослідження цивілізаційних трансформацій
Інформаційна цивілізація	С. Ченг та ін.	Інформація, знання та інформаційні технології набувають системоутворювального значення й трансформують способи мислення, навчання, комунікації та прийняття рішень	Інформація, знання, інформаційні технології	Дає можливість перейти від аналізу окремих характеристик інформаційного суспільства до цивілізаційного рівня осмислення інформаційних трансформацій
Цифрова трансформація суспільства і держави	OECD та ін.	Цифрові технології та дані не лише модернізують окремі процеси, а змінюють способи економічної діяльності, суспільної взаємодії та функціонування публічного управління	Дані, цифрові технології, цифрові платформи	Відображає перехід від інформатизації окремих процесів до системної перебудови економічних, соціальних та управлінських відносин
Алгоритмізоване та ШІ-опосередковане інформаційне середовище	UNESCO, OECD та сучасні дослідження ШІ	Алгоритмічні системи та ШІ беруть участь в аналізі інформації, формуванні інформаційних потоків, прогнозуванні, генеруванні контенту та підтримці прийняття рішень	Дані, алгоритми, штучний інтелект	Формує новий рівень взаємозалежності людини, суспільства, держави та технологічних систем і породжує нові суспільні та управлінські виклики

Джерело: сформовано автором на основі проведеного аналізу

Як свідчать дані табл. 1.3., розвиток наукових уявлень про трансформацію сучасного суспільства характеризується поступовим розширенням предмета дослідження: від структурних змін економіки та зростання ролі теоретичних знань – до глобальної мережевої взаємодії, цифровізації, алгоритмізації та поширення штучного інтелекту. При цьому кожна наступна концепція не обов'язково заперечує попередню, а переважно акцентує увагу на новому вимірі суспільних змін, що набував визначального значення на відповідному етапі технологічного й соціального розвитку.

Простежується також поступова зміна ролі інформації: від ресурсу забезпечення економічної та професійної діяльності вона перетворюється на системоутворювальний чинник функціонування суспільства, держави та глобального комунікаційного простору. Водночас розвиток цифрових платформ, великих даних, алгоритмічних систем і штучного інтелекту свідчить про подальше ускладнення інформаційного середовища, в якому технології вже не тільки забезпечують передавання інформації, а дедалі активніше опосередковують її відбір, аналіз, створення та використання.

На нашу думку, зазначена еволюція надає підстави говорити про інформаційно-цифрову цивілізаційну трансформацію як більш широкий процес, що інтегрує інформаційний, технологічний, соціальний, політичний та управлінський виміри сучасних змін.

Узагальнення розглянутих наукових підходів у дисертаційному дослідженні надає підстави обгрунтувати поняття «інформаційно-цифрова цивілізаційна трансформація». На нашу думку, «інформаційно-цифрова цивілізаційна трансформація» – це системний процес якісних змін суспільних, економічних, політичних та управлінських відносин, зумовлений перетворенням інформації і знань на стратегічні ресурси розвитку, глобальним поширенням цифрових технологій, мережевих форм взаємодії та алгоритмічних систем, унаслідок чого змінюються механізми функціонування держави, суспільства та взаємодії людини з інформаційним середовищем.

Обгрунтоване визначення надає змогу уникнути технологічного детермінізму, оскільки інформаційно-цифрова трансформація розглядається не

лише як наслідок розвитку технологій, а як комплексний процес взаємопов'язаних змін. Технологічні нововведення у такому разі виступають важливим, але не єдиним чинником цивілізаційної динаміки. Не меншого значення набувають політичні інститути, система державного управління, суспільні цінності, правові механізми, культура, освіта та здатність суспільства адаптуватися до нових форм інформаційної взаємодії.

Відтак, еволюція від постіндустріального та інформаційного суспільства до мережевих, знаннєвих, цифрових та алгоритмізованих форм суспільної організації свідчить про поступове набуття інформаційними процесами цивілізаційного значення. Інформація із допоміжного ресурсу перетворилася на один із системоутворювальних чинників функціонування держави та суспільства, а інформаційне середовище – на простір реалізації економічних, політичних, управлінських, соціальних і культурних відносин.

Водночас чим глибшою стає залежність держави й суспільства від інформаційних ресурсів, цифрових технологій, глобальних мереж та алгоритмічних систем, тим більш відчутними можуть бути наслідки порушення їх стабільного функціонування, зовнішнього впливу або деструктивного використання. Технологічний прогрес, таким чином, не лише розширює можливості суспільного розвитку, а й формує якісно нове середовище викликів, які виходять за межі окремих сфер життєдіяльності та здатні набувати загальнодержавного і цивілізаційного масштабу.

Саме ця подвійність сучасної інформаційно-цифрової трансформації – одночасне розширення можливостей розвитку та виникнення нових системних вразливостей – зумовлює необхідність переходу від аналізу інформації й інформаційного суспільства до дослідження категорії безпеки. За умов, коли інформаційні процеси безпосередньо впливають на функціонування державних інститутів, суспільну стабільність, реалізацію прав людини, національні інтереси та спроможність держави реагувати на зовнішні й внутрішні виклики, виникає потреба у визначенні місця інформаційного виміру в системі національної безпеки та з'ясуванні характеру його взаємозв'язку із ширшими цивілізаційними процесами.

1.2. Інформаційна та цивілізаційна безпека в системі національної безпеки

Сучасний етап суспільного розвитку характеризується поглибленням інформаційно-цифрових трансформацій, які поступово виходять за межі суто технологічних змін та набувають системного і цивілізаційного характеру. Перетворення інформації, знань і даних на стратегічні ресурси, глобалізація інформаційних потоків, поширення цифрових платформ, алгоритмізація суспільних процесів та розвиток штучного інтелекту істотно змінюють умови функціонування держави, суспільства й системи публічного управління. Водночас поглиблення залежності державних і суспільних інститутів від інформаційно-комунікаційних технологій та цифрової інфраструктури супроводжується виникненням нових вразливостей, ризиків і загроз, здатних впливати на стійкість держави, реалізацію її національних інтересів та спроможність реагувати на внутрішні й зовнішні виклики. За таких умов категорія безпеки набуває особливого значення та потребує переосмислення з урахуванням сучасних цивілізаційних трансформацій.

Безпека як складне суспільне та державно-управлінське явище охоплює різні сфери життєдіяльності держави і суспільства та характеризує стан їх захищеності, стійкості й спроможності протидіяти загрозам.

Безпека належить до фундаментальних умов існування та розвитку як окремої особи, так і суспільства та держави загалом. Потреба у захищеності супроводжує функціонування соціальних інститутів, організацій, підприємств та інших суспільних систем, оскільки їх стабільність безпосередньо залежить від здатності своєчасно виявляти, попереджати та мінімізувати вплив потенційних загроз. Саме тому проблематика безпеки посідає важливе місце в сучасному науковому дискурсі та розглядається як одна з визначальних передумов сталого суспільного розвитку.

У науковому розумінні безпека є складною, багатоаспектною та міждисциплінарною категорією, зміст якої не обмежується лише станом

захищеності від певної небезпеки. Її дослідження передбачає врахування широкого спектра взаємопов'язаних чинників, процесів і явищ, що зумовлюють виникнення загроз та визначають спроможність відповідної системи протидіяти їм. Відповідно, теоретичне осмислення безпеки здійснюється із застосуванням різних наукових підходів. Методологічним підґрунтям таких досліджень виступають, зокрема, положення загальної теорії систем і теорії відтворення, теорії ризиків та катастроф, а також концептуальні положення теорії соціальних конфліктів.

Особливої актуальності проблематика безпеки набуває в умовах динамічних суспільних трансформацій, посилення невизначеності та виникнення нових видів ризиків і загроз. Сучасне середовище характеризується високою швидкістю змін, взаємозалежністю економічних, політичних, соціальних, технологічних та інформаційних процесів. За таких обставин забезпечення безпеки дедалі більше пов'язується не лише з реагуванням на вже наявні небезпеки, а й зі здатністю прогнозувати потенційні загрози, оцінювати ризики, своєчасно ухвалювати обґрунтовані управлінські рішення та формувати механізми адаптації до змін зовнішнього і внутрішнього середовища.

Водночас сама проблема забезпечення безпечного існування не є породженням сучасності. Вона супроводжує людство фактично протягом усієї історії його розвитку. Від найдавніших часів життєдіяльність людини відбувалася під впливом природних, соціальних, воєнних, економічних та інших небезпек, що зумовлювало необхідність пошуку засобів самозбереження, захисту життя, майна, території та усталеного способу існування. З розвитком суспільства змінювалися характер і масштаби загроз, а разом із ними трансформувалися уявлення про зміст, способи та механізми забезпечення безпеки.

Історична еволюція поняття «безпека» свідчить про поступове розширення його змістового наповнення. У ранніх трактуваннях воно переважно асоціювалося зі станом спокою та відсутністю безпосередньої небезпеки для людини. Згодом розуміння безпеки вийшло за межі суто індивідуального виміру та почало охоплювати питання стабільності суспільства, державного устрою,

захисту території, суспільних інститутів та інтересів держави.

Витоки теоретичного осмислення безпеки простежуються вже в античній політико-філософській думці. Зокрема, у працях Аристотеля питання безпечного існування розглядалися у взаємозв'язку із самозбереженням людини, належною організацією державного устрою та забезпеченням умов для повноцінного розвитку громадянина. У такому розумінні безпека поступово набуває не лише індивідуального, а й суспільно-політичного змісту: її забезпечення пов'язується з належним управлінням, стабільністю суспільних відносин та створенням умов для розвитку особистості [3].

Подальший розвиток уявлень про природу безпеки простежується у філософській спадщині Платона. У його поглядах безпечний стан пов'язувався насамперед із недопущенням заподіяння шкоди та створенням умов, за яких наявна або ймовірна небезпека може бути своєчасно усунута. Розкриваючи відповідну проблематику, мислитель звертався до категорій «допомоги» та «порятунку», які відображали різні способи протидії небезпеці. Допомогу в такому контексті можна інтерпретувати як сукупність превентивних дій, спрямованих на недопущення реалізації існуючої чи потенційної загрози, тоді як порятунок характеризує безпосередні дії із захисту людини від можливої або вже актуалізованої шкоди [79]. Отже, ще у античній філософській думці формувалися уявлення не лише про захисну, а й про превентивну природу безпеки.

Показовою є й етимологічна еволюція досліджуваного поняття. У давньогрецькій мовній традиції зміст категорії «безпека» пов'язувався з такими характеристиками, як непохитність, міцність, надійність і стійкість [34]. Безпечний стан сприймався не тільки як відсутність безпосередньої загрози, а й як здатність певного об'єкта зберігати свою цілісність та стабільність під впливом несприятливих чинників.

Подібне змістове навантаження простежується й в етимології англомовного терміна «security». Його походження пов'язують із латинським «securitas» («безпека», «відсутність турботи»), утвореним від «securus» – «вільний від турботи, занепокоєння», що етимологічно поєднує компоненти se-

(«без», «вільний від») та cura («турбота», «піклування»). У процесі історичного розвитку семантика поняття security істотно розширилася: поряд із позначенням стану захищеності від небезпеки воно набуло значень упевненості, гарантії, надійності, забезпечення виконання зобов'язань, а згодом почало використовуватися також у правовому та фінансово-економічному контекстах [196].

Отже, еволюція наукових уявлень про безпеку демонструє перехід від її сприйняття переважно як стану відсутності небезпеки до розуміння як складної системної характеристики, що відображає здатність особи, суспільства та держави зберігати стійкість, захищати життєво важливі інтереси, адаптуватися до змін та протидіяти внутрішнім і зовнішнім загрозам. Зазначене вище створює методологічне підґрунтя для подальшого дослідження окремих складових безпеки, зокрема національної та інформаційної безпеки, зміст яких істотно трансформується під впливом сучасних цивілізаційних викликів.

Водночас у державно-управлінському вимірі безпека не може розглядатися виключно як стан відсутності небезпеки, оскільки її забезпечення передбачає цілеспрямовану діяльність держави щодо виявлення, попередження та нейтралізації загроз, формування відповідних механізмів реагування, забезпечення стійкості державних інститутів і захисту національних інтересів. Саме тому центральне місце в системі безпекових категорій держави посідає національна безпека, яка інтегрує сукупність взаємопов'язаних напрямів забезпечення захищеності особи, суспільства і держави.

Подальший розвиток наукових уявлень про безпеку та поступове розширення її змістових меж зумовили формування окремої категорії – «національна безпека». На відміну від первинного розуміння безпеки переважно як стану захищеності людини від небезпеки, концепція національної безпеки переносить акцент на рівень держави й суспільства, охоплюючи питання захисту національних інтересів, суверенітету, територіальної цілісності, суспільної стабільності та здатності держави протидіяти внутрішнім і зовнішнім загрозам.

Історичне становлення поняття «національна безпека» як категорії державно-політичного дискурсу традиційно пов'язують із початком XX ст.

Зокрема, у науковій літературі зазначається, що одним із перших випадків його використання на державному рівні стало звернення Президента США Теодора Рузвельта до Конгресу США у 1904 р. У контексті обґрунтування американської політики щодо зони Панамського каналу відповідні дії держави пов'язувалися з необхідністю захисту її стратегічних і безпекових інтересів [47]. Надалі проблематика національної безпеки поступово набула самостійного значення у політичній теорії та практиці державного управління.

Упродовж XX ст. зміст категорії «національна безпека» істотно розширився. Якщо на початкових етапах її формування основна увага концентрувалася передусім на військовій могутності держави, захисті її території та протидії зовнішнім загрозам, то з ускладненням суспільних відносин безпекова проблематика почала охоплювати політичну, економічну, соціальну, екологічну, технологічну та інформаційну сфери. Відповідно, поняття національної безпеки поступово вийшло за межі суто політичної категорії та стало предметом міждисциплінарного дослідження, зокрема у сфері права та публічного управління.

У сучасній науковій літературі національна безпека найчастіше розглядається через категорію захищеності життєво важливих інтересів особи, суспільства та держави від внутрішніх і зовнішніх загроз [39]. Водночас таке розуміння не варто обмежувати виключно фактичним станом захищеності. Національна безпека має динамічний характер і передбачає здатність держави та її інституцій своєчасно ідентифікувати загрози, прогнозувати їх розвиток, попереджати негативні наслідки, забезпечувати стійкість суспільства та формувати ефективні механізми реагування на зміни безпекового середовища.

Відомий американський науковець В. Ліппман у 1943 р. трактував національну безпеку як здатність держави захищати власні легітимні інтереси та зберігати їх у разі війни [180]. Така позиція відповідала умовам першої половини XX ст., коли основними небезпеками для держав уважали передусім збройні конфлікти.

Вагомий внесок у переосмислення цього поняття зробив А. Вольферс, який наголосив на неоднозначності терміна «національна безпека» та зазначив, що

різні суб’єкти можуть розуміти його по-різному [215]. Саме ця риса стала істотною передумовою подальшого розвитку безпекової теорії.

У другій половині ХХ ст. поступово утвердилося розширене бачення безпеки. Дослідники стали враховувати не тільки військові загрози, а й економічні, політичні, соціальні, екологічні та технологічні чинники. Вагомий внесок у цей процес належить Б. Бузану, який у своїх працях аналізував безпеку крізь призму взаємодії державного, суспільного та індивідуального рівнів, виокремлюючи політичний, економічний, суспільний, військовий і екологічний виміри [149].

Сучасна концепція національної безпеки поступово віддалилася від виключно військового трактування. Держава може бути формально убезпечена від безпосереднього воєнного нападу, проте водночас залишатися вразливою перед економічними кризами, політичною нестабільністю, кіберзагрозами, пошкодженням критичної інфраструктури, інформаційними операціями чи суспільною поляризацією.

В українському законодавстві національна безпека тлумачиться комплексно, зокрема, Закон України «Про національну безпеку України» визначає її як захищеність державного суверенітету, територіальної цілісності, демократичного конституційного устрою та інших національних інтересів України від наявних і можливих загроз [93].

Закон України «Про національну безпеку України» має принципове значення для усвідомлення взаємозв’язку національної та інформаційної безпеки. Якщо національна безпека передбачає охорону національних інтересів, а інформаційна сфера безпосередньо позначається на функціонуванні держави, суспільства й людини, то інформаційна безпека закономірно виступає елементом загальної системи національної безпеки.

Нормативне визначення національної безпеки водночас підкреслює особливу роль національних інтересів. Вони включають життєво важливі потреби та інтереси людини, суспільства і держави, реалізація яких гарантує державний суверенітет, демократичний поступ, безпечні умови життя та добробут громадян.

Національну безпеку не слід зводити лише до захищеності державного механізму. Вона має людиноцентричну спрямованість і охоплює захист особи, суспільства та держави.

Стратегія національної безпеки України, затверджена Указом Президента України № 392/2020, безпосередньо визначає безпеку людини одним із ключових орієнтирів державної політики у сфері національної безпеки [100]. Тут відображений сучасний перехід від суто державоцентричної моделі безпеки до комплексного бачення, у якому безпека людини, суспільства й держави постає як взаємопов'язана сукупність компонентів.

У цьому контексті національні інтереси доцільно розглядати як сукупність об'єктивно зумовлених потреб і пріоритетів особи, суспільства та держави, реалізація і захист яких є необхідними для їх стабільного функціонування та подальшого розвитку. Саме співвідношення категорій «національні інтереси – загрози – механізми захисту – стійкість» значною мірою визначає зміст сучасного розуміння національної безпеки та дозволяє розглядати її не як статичний стан, а як безперервний процес забезпечення захищеності й спроможності держави реагувати на трансформацію внутрішнього та зовнішнього середовища.

В умовах сучасних цивілізаційних трансформацій, коли поряд із традиційними воєнними, політичними та економічними загрозами посилюється вплив загроз інформаційного, кібернетичного, технологічного й комунікаційного характеру, таке трактування набуває важливого значення. У цих умовах інформаційна сфера перетворюється на один із ключових просторів реалізації національних інтересів та одночасно на середовище виникнення принципово нових ризиків. Відтак інформаційна безпека набуває значення однієї з важливих складових системи національної безпеки, без належного забезпечення якої у сучасних умовах неможливо гарантувати стійкість держави, суспільства та її ключових інститутів [30].

Комплексний характер національної безпеки зумовлює необхідність її розгляду як системного утворення, що охоплює сукупність взаємопов'язаних сфер забезпечення життєво важливих інтересів людини, суспільства і держави.

Диференціація таких сфер обумовлена різноманітністю об’єктів захисту, характером потенційних і реальних загроз, а також специфікою механізмів державного реагування на них. Водночас виокремлення окремих видів безпеки має переважно аналітичний характер, оскільки в реальних умовах їх функціонування відбувається у тісній взаємозалежності, а загрози, що виникають в одній сфері, здатні поширюватися на інші та набувати комплексного характеру.

З огляду на це, національну безпеку доцільно розглядати як інтегровану систему, у межах якої взаємодіють воєнна, економічна, соціальна, інформаційна, кібернетична, технологічна, енергетична, екологічна, біологічна, гуманітарна та продовольча безпека. Зазначений перелік не є вичерпною нормативно закріпленою класифікацією, а відображає систематизацію основних безпекових сфер, виокремлених у законодавстві, стратегічних документах та науковому дискурсі.

Особливе місце серед зазначених складових посідає інформаційна безпека, оскільки інформаційні процеси на сучасному етапі пронизують практично всі сфери життєдіяльності держави та суспільства. Інформаційні ресурси, цифрові технології, канали комунікації та інформаційний простір забезпечують функціонування органів публічної влади, економіки, оборонного та енергетичного секторів, соціальної й гуманітарної сфер, а їх порушення або використання з деструктивною метою здатне спричиняти наслідки одночасно для декількох складових національної безпеки. Саме тому інформаційна безпека в сучасних умовах набуває міжсекторального значення та тісно взаємодіє з іншими елементами системи національної безпеки.

Систематизацію основних складових національної безпеки та місце інформаційної безпеки в їх структурі представлено на рис. 1.1.

Рис. 1.1. Основні складові національної безпеки та місце інформаційної безпеки в їх системі

Джерело: сформовано автором на основі власних досліджень

Як наочно демонструє рис. 1.1., інформаційна безпека є невід'ємною складовою системи національної безпеки та водночас характеризується вираженим міжсекторальним характером, оскільки інформаційні процеси супроводжують функціонування практично всіх сфер життєдіяльності держави і суспільства. Інформаційні ресурси та технології використовуються у публічному управлінні, обороні, економіці, енергетиці, соціальній і гуманітарній сферах, а порушення їх належного функціонування здатне спричиняти наслідки одночасно для декількох складових національної безпеки. З огляду на це, концептуальне визначення місця інформаційної безпеки в системі національної безпеки потребує дослідження еволюції наукових підходів до її розуміння та трансформації змісту цієї категорії під впливом розвитку інформаційно-комунікаційних і цифрових технологій.

Поняття інформаційної безпеки формувалося поступово, у міру розвитку способів створення, зберігання, передавання та використання інформації й усвідомлення необхідності її захисту від несанкціонованого доступу, зміни,

знищення або втрати. Потреба в захисті інформації виникла задовго до появи комп'ютерних технологій: упродовж історичного розвитку держави прагнули забезпечувати збереження державних таємниць, військових відомостей, дипломатичної кореспонденції, фінансової інформації та інших даних, розголошення або спотворення яких могло завдати шкоди державним інтересам.

Водночас як самостійний науково-технічний напрям інформаційна безпека почала особливо активно розвиватися з появою та поширенням комп'ютерних систем. За даними NIST, проблематика комп'ютерної безпеки набула системного характеру у 1970-х роках, хоча завдання захисту інформації були притаманні й попереднім інформаційним системам [164]. На ранньому етапі основна увага приділялася запобіганню несанкціонованому доступу до комп'ютерних систем і захисту даних від втрати або модифікації. Подальше поширення персональних комп'ютерів, локальних і глобальних мереж, інтернету, цифрових баз даних та електронних комунікацій сприяло істотному розширенню змісту інформаційної безпеки.

У сучасному трактуванні інформаційна безпека, однак, не обмежується виключно технічним захистом комп'ютерних систем. NIST визначає інформаційну безпеку через захист інформації та інформаційних систем від несанкціонованого доступу, використання, розкриття, порушення функціонування, модифікації чи знищення з метою забезпечення конфіденційності, цілісності та доступності.

Одним із базових підходів до визначення властивостей захищеної інформації стала так звана тріада CIA – confidentiality, integrity, availability, тобто конфіденційність, цілісність і доступність [197]. Конфіденційність передбачає забезпечення доступу до інформації виключно уповноваженим суб'єктам; цілісність – її захист від несанкціонованої модифікації або знищення; доступність – можливість своєчасного отримання та використання інформації уповноваженими користувачами. Зазначені властивості й сьогодні становлять фундаментальну основу інформаційної безпеки в її техніко-технологічному вимірі.

Український нормативно-правовий підхід характеризується ширшим

баченням цієї категорії. Відповідно до Стратегії інформаційної безпеки України, затвердженої Указом Президента України від 28 грудня 2021 р. № 685/2021, інформаційна безпека України розглядається як складова національної безпеки України та пов'язується із захищеністю державного суверенітету, територіальної цілісності, демократичного конституційного ладу, інших життєво важливих інтересів людини, суспільства і держави, за якої належним чином забезпечуються конституційні права і свободи людини на збирання, зберігання, використання та поширення інформації, доступ до достовірної та об'єктивної інформації, а також існує ефективна система захисту і протидії завданню шкоди через поширення негативних інформаційних впливів [100].

Порівняння наведених підходів свідчить про поступове розширення змісту категорії «інформаційна безпека». Якщо на ранніх етапах її формування основна увага приділялася захисту інформації та інформаційних систем від несанкціонованого доступу, модифікації, знищення або втрати, то сучасне розуміння охоплює значно ширший комплекс відносин. Йдеться не лише про технічну захищеність інформаційних ресурсів, а й про забезпечення інформаційних прав людини, захист інформаційного простору, протидію деструктивним інформаційним впливам та забезпечення інформаційної стійкості держави і суспільства.

У найбільш загальному розумінні інформаційну безпеку доцільно пов'язувати зі станом захищеності життєво важливих інтересів людини, суспільства і держави в інформаційній сфері від внутрішніх і зовнішніх, навмисних і ненавмисних впливів та інших загроз, здатних порушувати належне функціонування інформаційного середовища, інформаційних ресурсів і відповідної інфраструктури. При цьому її зміст не може бути обмежений виключно захистом інформації як сукупності даних, оскільки інформаційна безпека охоплює також суспільні відносини, що виникають у процесах створення, збирання, оброблення, зберігання, поширення та використання інформації, реалізації інформаційних прав і свобод людини, функціонування інформаційного простору та протидії деструктивним інформаційним впливам.

Одним із базових моментів, що стосуються забезпечення інформаційної

безпеки залишається збереження ключових властивостей інформації та інформаційних ресурсів – конфіденційності, цілісності й доступності. Водночас у контексті публічного управління важливого значення набувають також достовірність та своєчасність інформації. Порушення хоча б однієї із зазначених властивостей може мати різні за масштабом наслідки залежно від характеру інформації, сфери її використання та значення відповідного інформаційного ресурсу для функціонування держави або суспільства. Особливо небезпечними такі порушення є у системі публічного управління, оборонній сфері, функціонуванні критичної інфраструктури та інших стратегічно важливих секторах, де якість і своєчасність інформації безпосередньо впливають на обґрунтованість управлінських рішень.

Водночас сучасне розуміння інформаційної безпеки не може зводитися лише до забезпечення технічних характеристик інформації. Інформація може залишатися технічно цілісною та доступною, але при цьому бути недостовірною, маніпулятивною або цілеспрямовано використовуватися для впливу на суспільну свідомість, поведінку населення, процеси прийняття рішень та функціонування державних інститутів.

Проблематика визначення сутності інформаційної безпеки набула значного розвитку й у працях українських науковців. Її дослідження здійснюється в межах правового, державно-управлінського, безпекового, інформаційно-комунікаційного та людиноцентричного підходів. Відмінності між науковими позиціями значною мірою зумовлені тим, який саме об’єкт захисту перебуває в центрі уваги дослідника: інформація та інформаційні ресурси, інформаційні права людини, інформаційний простір, національні інтереси, державні інституції або суспільна свідомість. Основні підходи українських учених до розуміння сутності інформаційної безпеки систематизовано в табл. 1.4.

Таблиця 1.4

Наукові підходи до визначення сутності категорії «інформаційна безпека»

Науковці	Підхід до розуміння поняття	Основний акцент	Значення для проведеного дослідження
Б. Кормич	Інформаційна безпека – комплексне державно-правове явище, пов'язане із захистом інформаційних інтересів особи, суспільства і держави та формуванням відповідної державної політики.	Організаційно-правові засади; державна політика; захист інформаційних інтересів	Формування системного організаційно-правового підходу до політики інформаційної безпеки України
В. Ліпкан, Ю. Максименко, В. Желіховський	Інформаційна безпека – складова системи національної безпеки, пов'язана із забезпеченням національних інтересів в інформаційній сфері та протидією інформаційним загрозам	Національна безпека, системний підхід; поняття та зміст інформаційної безпеки	Обґрунтування системного місця інформаційної безпеки у структурі національної безпеки
А. Марущак	Інформаційна безпека досліджується крізь призму правового регулювання інформаційних відносин, доступу до інформації, реалізації та захисту інформаційних прав	Інформаційні права; доступ до інформації; правове регулювання	Посилення правового та людиноцентричного виміру інформаційної безпеки
О. Золотар	Інформаційна безпека розглядається не лише на рівні держави, а й на рівні людини як суб'єкта інформаційних відносин, що потребує захисту від інформаційних загроз	Інформаційна безпека людини; інформаційні права; загрози особистості	Розширення об'єктного виміру інформаційної безпеки від держави до особи

Джерело: сформовано автором на основі [37; 46; 56; 58]

Аналіз наведених наукових позицій свідчить про відсутність суто одновимірного підходу до трактування інформаційної безпеки. У працях українських учених простежується поступове розширення її змісту: від захисту інформації, інформаційних ресурсів та інформаційних систем – до забезпечення

національних інтересів в інформаційній сфері, захисту інформаційного простору, інформаційних прав людини та протидії деструктивним інформаційним і психологічним впливам.

Водночас можна виокремити декілька основних напрямів наукового осмислення інформаційної безпеки: техніко-захисний, орієнтований на захист інформації та відповідної інфраструктури; правовий, пов'язаний із регулюванням інформаційних відносин та захистом інформаційних прав; національно-безпековий, у межах якого інформаційна безпека розглядається як складова національної безпеки; інформаційно-комунікаційний, що акцентує увагу на інформаційних і психологічних впливах; та державно-управлінський, зосереджений на механізмах формування й реалізації державної політики у сфері інформаційної безпеки.

Отже, узагальнення наукових підходів дає підстави стверджувати, що інформаційна безпека має комплексний характер і не може бути зведена виключно до технічного захисту інформації. Її сучасний зміст формується на перетині технологічних, правових, суспільних, комунікаційних та державно-управлінських відносин.

З огляду на це, інформаційну безпеку доцільно розглядати у двох взаємопов'язаних вимірах. Перший – інформаційно-технологічний, що охоплює захист інформації, даних, інформаційних систем, мереж та відповідної інфраструктури і передбачає забезпечення їх конфіденційності, цілісності та доступності. Другий – інформаційно-комунікаційний, пов'язаний із захистом інформаційного простору, суспільної свідомості та процесів комунікації від дезінформації, маніпулятивних технологій, інформаційно-психологічних операцій та інших форм деструктивного інформаційного впливу.

Узагальнене вище дозволяє чіткіше визначити співвідношення інформаційної безпеки та кібербезпеки, які, незважаючи на значну сферу перетину, не є тотожними категоріями. Кібербезпека концентрується передусім на забезпеченні захищеності інтересів людини, суспільства і держави під час використання кіберпростору, забезпеченні стійкості інформаційних, електронних комунікаційних та інформаційно-комунікаційних систем і протидії

кіберзагрозам [28]. Натомість інформаційна безпека має ширший функціональний зміст, оскільки поряд із технологічною складовою охоплює інформаційно-комунікаційний, суспільний, гуманітарний, правовий та управлінський виміри інформаційних процесів [20].

Розширення змісту інформаційної безпеки закономірно супроводжується трансформацією характеру загроз у цій сфері. Стратегія інформаційної безпеки України визначає інформаційні загрози як потенційно або реально негативні явища, тенденції й чинники інформаційного впливу, спроможні перешкоджати реалізації національних інтересів України в інформаційній сфері та завдавати шкоди життєво важливим інтересам людини, суспільства і держави [101]. Відповідно, джерелом небезпеки в сучасному інформаційному середовищі може бути не лише технічне проникнення в інформаційну систему, а й цілеспрямоване викривлення інформації, маніпулювання нею або використання інформаційних ресурсів для деструктивного впливу.

Загрози інформаційній безпеці можуть виникати як унаслідок навмисної діяльності певних суб'єктів, так і через ненавмисні порушення функціонування інформаційних систем та процесів. До них доцільно віднести несанкціонований доступ до інформаційних ресурсів, порушення конфіденційності інформації, її знищення або модифікацію, спотворення чи приховування суспільно значущих відомостей, перешкоджання законному доступу до інформації, поширення дезінформації, здійснення маніпулятивного та інформаційно-психологічного впливу, порушення функціонування інформаційної інфраструктури та інші дії або явища, здатні завдати шкоди інтересам людини, суспільства чи держави.

Особливого значення інформаційно-комунікаційний вимір набуває в умовах сучасних конфліктів. У підходах НАТО до протидії інформаційним загрозам акцентується увага на навмисних, шкідливих, маніпулятивних і скоординованих діях державних та недержавних суб'єктів в інформаційному середовищі [188]. До відповідного інструментарію можуть належати інформаційні операції, маніпулювання інформацією, іноземне інформаційне втручання та поширення дезінформації. При цьому розвиток штучного інтелекту та технологій створення синтетичного контенту, зокрема deepfake, додатково

розширює можливості масштабування й персоналізації деструктивного інформаційного впливу.

Важливим чинником інформаційної безпеки залишається людський фактор, бо незважаючи на автоматизацію процесів збирання, оброблення, зберігання та передавання інформації, людина продовжує одночасно виступати суб'єктом інформаційних відносин, об'єктом інформаційного впливу та потенційним джерелом інформаційних ризиків. Поширення соціальних мереж, цифрових платформ, технологій генерування контенту та систем штучного інтелекту ще більше ускладнює цей взаємозв'язок, оскільки межі між виробником, поширювачем і споживачем інформації стають дедалі менш чіткими.

У цьому контексті інформаційна безпека безпосередньо пов'язується з інформаційною стійкістю держави та суспільства. Стійкість інформаційного середовища передбачає не лише спроможність запобігати порушенню функціонування інформаційних систем, а й здатність державних інститутів і суспільства зберігати належне функціонування в умовах інформаційного впливу, забезпечувати доступ до достовірної інформації, критично оцінювати інформаційні повідомлення, адаптуватися до нових загроз та відновлювати нормальне функціонування після кризових ситуацій [107].

Розвиток інформаційних технологій істотно змінив і безпекове середовище у воєнній сфері. Інформаційні та цифрові технології використовуються для отримання й аналізу розвідувальної інформації, прогнозування загроз, забезпечення зв'язку та управління, функціонування сучасних систем озброєння, а також здійснення інформаційних і кібероперацій [10]. Унаслідок цього межі між інформаційними, кібернетичними та воєнними загрозами стають дедалі більш рухомими, а інформаційне середовище перетворюється на важливу сферу сучасного стратегічного протиборства [111].

Поряд із трансформацією загроз принципово змінюються й умови забезпечення інформаційної безпеки. На відміну від окремих традиційних сфер національної безпеки, інформаційні ресурси та відповідна інфраструктура не перебувають виключно у розпорядженні держави. Значна їх частина належить

або використовується суб’єктами господарювання, засобами масової інформації, цифровими платформами, громадськими організаціями, науковими й освітніми установами, окремими громадянами, транснаціональними корпораціями та іншими суб’єктами [13]. Крім того, сучасні інформаційні потоки дедалі менше обмежуються територіальними кордонами, а інформаційне середовище набуває глобального і транскордонного характеру.

За таких умов держава об’єктивно не може здійснювати абсолютний контроль над усією сукупністю інформаційних ресурсів, технологій, платформ та інформаційних потоків, що функціонують у сучасному інформаційному просторі. Проте це не означає зменшення її ролі у забезпеченні інформаційної безпеки. Навпаки, ускладнення інформаційного середовища зумовлює трансформацію функцій держави – від переважно адміністративного контролю за інформаційними процесами до формування нормативно-правових засад їх функціонування, координації діяльності суб’єктів інформаційної безпеки, розвитку інституційної спроможності, забезпечення інформаційної стійкості, захисту критично важливих інформаційних ресурсів, міжнародного співробітництва та розвитку механізмів державно-приватної і суспільної взаємодії [68].

З позицій публічного управління зазначене дає підстави стверджувати, що сучасне забезпечення інформаційної безпеки потребує поступового переходу від переважно контрольно-обмежувальної до координаційно-регуляторної моделі державного впливу, заснованої на поєднанні нормативно-правових, організаційно-інституційних, технологічних, інформаційно-комунікаційних та міжнародних механізмів. За такого підходу держава виступає не єдиним суб’єктом забезпечення інформаційної безпеки, а системоутворювальним суб’єктом, який формує нормативні правила, координує взаємодію учасників, забезпечує захист національних інтересів та створює умови для стійкого функціонування інформаційного середовища [51].

Відповідно, ефективність державного регулювання інформаційної безпеки визначається не можливістю встановлення всеохопного контролю над інформаційними процесами, а спроможністю держави сформувати систему

правових, організаційних, інституційних, технологічних та комунікаційних механізмів, які забезпечуватимуть узгоджену взаємодію органів публічної влади, приватного сектору, громадянського суспільства, громадян та інших суб'єктів інформаційних відносин [70].

Особливого значення за таких умов набуває міжнародний вимір забезпечення інформаційної безпеки. Транскордонність інформаційних потоків, глобальний характер цифрових платформ, функціонування міжнародної цифрової інфраструктури та можливість здійснення інформаційного впливу незалежно від географічного місцезнаходження його джерела обмежують ефективність виключно національних механізмів реагування. Виникає важлива необхідність у міжнародному співробітництві, координації підходів, обміну інформацією та вироблення спільних механізмів реагування на інформаційні загрози [140].

Отже, сучасна інформаційна безпека не може розглядатися лише як стан технічної захищеності інформації або інформаційної інфраструктури. Вона являє собою комплексний напрям забезпечення національної безпеки, що охоплює технологічні, інформаційно-комунікаційні, правові, управлінські, суспільні та міжнародні відносини. Її специфічною характеристикою є міжсекторальність: інформаційні загрози здатні одночасно впливати на воєнну, економічну, політичну, соціальну, гуманітарну, технологічну та інші сфери національної безпеки.

Проведений аналіз водночас свідчить, що трансформація інформаційної безпеки відбувається паралельно зі зміною характеру самого інформаційного середовища. Його глобалізація, транскордонність інформаційних потоків, розвиток цифрових платформ, алгоритмічних систем та штучного інтелекту призводять до того, що джерела, суб'єкти та наслідки інформаційних загроз дедалі частіше виходять за межі юрисдикції окремої держави. При цьому інформаційні впливи здатні одночасно позначатися на політичних, економічних, воєнних, соціальних, технологічних і гуманітарних процесах, що ускладнює їх дослідження виключно в межах окремої складової національної безпеки.

Зазначені процеси особливо виразно проявляються в умовах

інформаційно-цифрової цивілізаційної трансформації, сутність якої було обґрунтовано у попередньому підрозділі. Якщо така трансформація змінює не окрему сферу суспільного життя, а способи функціонування держави, суспільства, економіки, комунікації та взаємодії людини з інформаційним середовищем, закономірно виникає питання щодо формування відповідного безпекового виміру зазначених процесів.

Зокрема, глобалізація інформаційного простору, прискорення технологічних змін, розвиток штучного інтелекту, алгоритмізація суспільних процесів, транскордонність інформаційних впливів та взаємопроникнення різних сфер безпеки свідчать про поступове ускладнення сучасного безпекового середовища. Загрози, породжені такими трансформаціями, вже не завжди можуть бути чітко локалізовані в межах інформаційної, кібернетичної, економічної, воєнної чи іншої окремої сфери, оскільки набувають комплексного та системного характеру [116].

У ході нашого дослідження постає актуальне питання про достатність традиційних галузевих категорій безпеки для характеристики захищеності держави і суспільства від системних загроз, що виникають унаслідок трансформацій цивілізаційного масштабу. Відтак подальшого теоретичного осмислення потребує цивілізаційний вимір безпеки, а також можливість використання категорії «цивілізаційна безпека» для позначення відповідного рівня безпекових відносин, визначення її сутності, характерних ознак та співвідношення з національною й інформаційною безпекою.

Звернення до категорії цивілізаційної безпеки зумовлене насамперед зміною характеру сучасного безпекового середовища, традиційне розуміння безпеки історично було значною мірою сконцентроване навколо держави, її території, суверенітету, політичних інститутів та здатності протистояти зовнішнім і внутрішнім загрозам. Однак глобалізація, цифровізація, технологічні революції, розвиток штучного інтелекту, трансформація міжнародного порядку, зміна характеру комунікації та формування глобального інформаційного простору створюють загрози, наслідки яких не завжди можуть бути локалізовані в межах території окремої держави або однієї сфери національної безпеки.

У цьому контексті важливим є розмежування понять «цивілізаційний вимір безпеки» та «цивілізаційна безпека». Перше доцільно використовувати як ширшу аналітичну характеристику безпекових процесів, що виникають під впливом довготривалих і масштабних трансформацій суспільного розвитку. Натомість цивілізаційна безпека може розглядатися як категорія, за допомогою якої характеризується здатність певної соціальної, державно-політичної або цивілізаційної системи зберігати стійкість, базові цінності, ідентичність, знання, інституційну спроможність та перспективи розвитку під впливом системних трансформацій і загроз.

Сам термін «цивілізаційна безпека» (civilizational security) не є абсолютно новим для наукового дискурсу. Водночас його концептуалізація залишається дискусійною, що значною мірою пов'язано з неоднозначністю вихідної категорії «цивілізація». Залежно від того, чи розглядається цивілізація як певний рівень розвитку людства, як культурно-історична спільнота або як масштабна соціальна система, змінюється й зміст поняття цивілізаційної безпеки. Одну з найбільш системних спроб осмислення цієї категорії здійснив Б. Боуден у своїй праці «Цивілізаційна безпека» [146] наголошує, що експліцитна концепція «civilizational security» є відносно новою та особливо актуалізувалася після завершення холодної війни й поширення дискусії навколо концепції «зіткнення цивілізацій» [176]. Дослідник виходить із того, що множинність підходів до розуміння самої цивілізації закономірно зумовлює існування різних способів концептуалізації цивілізаційної безпеки. При цьому цивілізаційний рівень безпекового аналізу виходить за межі традиційної державоцентричної моделі та дозволяє враховувати нові й масштабні загрози, здатні впливати на значно ширші соціальні системи.

Особливо важливим для цього дослідження є те, що Б. Боуден не зводить проблематику цивілізаційної безпеки виключно до протистояння окремих цивілізацій. Автор доходить висновку про необхідність мислення і стратегування в категоріях цивілізаційної безпеки з огляду на появу нових та емерджентних загроз і небезпек, які стосуються людства та середовища його існування [146; 147]. Отже, цивілізаційний рівень аналізу дає змогу вийти за межі

традиційного розуміння безпеки окремої держави та розглядати довготривалі системні процеси, здатні впливати на фундаментальні умови суспільного розвитку.

Подальший розвиток зазначеного підходу простежується у праці Г. Левіцького «Цивілізаційна безпека: чому російське вторгнення в Україну демонструє, що поняття «національна безпека» є недостатнім для розуміння геополітики» [179]. Дослідник безпосередньо ставить питання про те, чи достатньою є категорія національної безпеки для пояснення сучасних геополітичних процесів, та пропонує використовувати категорію «цивілізаційна безпека» як додаткову аналітичну категорію. У трактуванні Г. Левіцького цивілізаційна безпека держави пов'язується з безпекою, що випливає з її належності до певної культурної зони або цивілізації [179]. Дослідник доводить, що врахування параметра цивілізаційної безпеки дозволяє глибше аналізувати окремі геополітичні дилеми та цивілізаційні тенденції.

Порівняння зазначених підходів демонструє, що цивілізаційна безпека може розглядатися щонайменше у двох взаємопов'язаних значеннях. У першому – як безпека конкретної цивілізаційної спільноти, її культурної ідентичності, цінностей, соціальних інститутів та здатності до самозбереження і розвитку. У другому, ширшому значенні – як захищеність фундаментальних умов розвитку суспільства та людства від системних загроз цивілізаційного масштабу, які за своєю природою виходять за межі окремих держав і традиційних секторів безпеки. Така багатозначність категорії підтверджує необхідність уточнення її змісту залежно від предмета конкретного дослідження.

Український науковий дискурс також містить теоретичні передумови для розвитку категорії цивілізаційної безпеки, хоча безпосередньо цей термін поки не набув такого рівня концептуальної усталеності, як категорії національної та інформаційної безпеки. Значна частина відповідних досліджень здійснюється через категорії цивілізаційної суб'єктності, національної стійкості, цивілізаційної ідентичності, стратегічної безпеки та глобальних цивілізаційних викликів.

Особливе значення у цьому контексті мають праці С. Пирожкова та

Н. Хамітова, у яких проблематика безпеки України безпосередньо пов'язується з її цивілізаційною суб'єктністю. У монографії «Цивілізаційна суб'єктність України: від потенцій до нового світогляду і буття людини» автори розглядають цивілізаційну суб'єктність як важливу передумову стратегічного розвитку держави, приділяючи окрему увагу співвідношенню цивілізаційної суб'єктності та національної безпеки України [77]. У структурі монографії цьому питанню присвячено окремий підрозділ «Цивілізаційна суб'єктність та національна безпека України», а також розглянуто трансформацію загроз в умовах гібридного світового порядку.

Розвиваючи зазначений підхід, С. Пирожков та Н. Хамітов обґрунтовують взаємозалежність цивілізаційної суб'єктності, національної стійкості та національної безпеки. На думку дослідників, реальна незалежність держави не вичерпується формальним суверенітетом, а передбачає її здатність бути самостійним суб'єктом історичного та геополітичного розвитку. Відповідно, стійкість цивілізаційної суб'єктності держави розглядається ними як принципова передумова забезпечення її національної безпеки [76].

Важливою для нашого дослідження є запропонована українськими вченими концептуальна зв'язка «цивілізаційна суб'єктність – національна стійкість – національна безпека». Вона демонструє, що безпековий стан держави визначається не лише її здатністю нейтралізувати конкретні воєнні, економічні, інформаційні чи інші загрози, а й спроможністю зберігати власну суб'єктність, забезпечувати інноваційний розвиток, суспільну консолідацію та реалізовувати самостійний цивілізаційний проєкт. У національній доповіді НАН України концепція національної стійкості безпосередньо розкривається через стійкість цивілізаційної суб'єктності країни [63].

У цьому аспекті цивілізаційна суб'єктність може розглядатися як одна з теоретичних передумов формування ширшого поняття цивілізаційної безпеки. Водночас зазначені категорії не є тотожними. Цивілізаційна суб'єктність характеризує здатність держави і суспільства виступати самостійним суб'єктом цивілізаційного розвитку, тоді як цивілізаційна безпека, у запропонованому в цьому дослідженні розумінні, характеризує стан їх захищеності та стійкості до

системних трансформацій і загроз цивілізаційного масштабу.

Окремого значення набуває цивілізаційна ідентичність як ціннісно-культурна основа такої суб'єктності. У колективній монографії Інституту політичних і етнонаціональних досліджень ім. І. Кураса НАН України «Цивілізаційна ідентичність українства: історія і сучасність» цивілізаційна ідентичність розглядається як складний історико-політичний і соціокультурний феномен, пов'язаний із самоідентифікацією українства та його місцем у цивілізаційному просторі [129].

Сучасна російсько-українська війна додатково актуалізує цивілізаційний рівень безпекового аналізу. Так, В. Антонюк та І. Миценко характеризують війну в Україні як глобальний цивілізаційний конфлікт, пов'язуючи його виникнення, зокрема, з розбіжністю стратегічних векторів розвитку України та Росії [1]. Вчені стверджують, що окремі сучасні загрози за масштабом і наслідками виходять за межі традиційного галузевого розмежування безпеки та здатні впливати на фундаментальні засади розвитку держави і суспільства.

Отже, аналіз українського наукового дискурсу дозволяє виявити формування теоретичного поля, суміжного з поняттям цивілізаційної безпеки. Воно охоплює проблематику цивілізаційної суб'єктності, цивілізаційної ідентичності, національної стійкості, стратегічної безпеки та цивілізаційних конфліктів. Водночас зазначені дослідження переважно розкривають окремі аспекти цивілізаційного виміру безпеки, тоді як комплексне державно-управлінське трактування цивілізаційної безпеки в контексті інформаційно-цифрових трансформацій залишається недостатньо розробленим**.**

Вищевказане дає підстави не заперечувати наявні наукові підходи, а розвинути їх шляхом виокремлення цивілізаційної безпеки як аналітичної категорії, що характеризує стійкість держави і суспільства до системних трансформацій цивілізаційного масштабу та створює теоретичне підґрунтя для визначення напрямів трансформації державного регулювання інформаційної безпеки.

Для проблематики державного регулювання інформаційної безпеки особливе значення має саме друге, системне трактування. Сучасні цивілізаційні

трансформації дедалі більше визначаються розвитком інформаційних і цифрових технологій. Штучний інтелект, глобальні цифрові платформи, алгоритмічні системи, великі дані, транскордонні інформаційні потоки та цифровізація критично важливих суспільних процесів одночасно виступають чинниками розвитку та джерелами нових вразливостей. Унаслідок цього інформаційні загрози перестають бути ізольованою проблемою інформаційної сфери та набувають здатності трансформувати політичні інститути, суспільну комунікацію, економічні відносини, культурні процеси, механізми формування ідентичності та способи реалізації державної влади [130].

Саме ця обставина дозволяє встановити безпосередній взаємозв'язок між інформаційною та цивілізаційною безпекою, де інформаційна безпека залишається складовою національної безпеки та спрямовується на захист відповідних інтересів людини, суспільства і держави в інформаційній сфері. Цивілізаційний вимір натомість дозволяє оцінювати ті самі процеси з позицій їх довготривалого системного впливу на стійкість держави і суспільства, їх ціннісні засади, ідентичність, систему знань, інституційну спроможність та перспективи розвитку.

Водночас зіставлення розглянутих підходів надає підстави констатувати, що державно-управлінський вимір цивілізаційної безпеки залишається недостатньо концептуалізованим**.** У наявних трактуваннях увага зосереджується передусім на цивілізаційній ідентичності, належності до певної цивілізаційної або культурної спільноти, а також на масштабних загрозах цивілізаційному розвитку. Натомість недостатньо розкритим залишається питання про те, яким чином держава повинна адаптувати систему публічного управління та механізми регулювання до загроз, породжених трансформаціями цивілізаційного масштабу.

Інформаційно-цифрова цивілізаційна трансформація змінює не лише технологічне середовище функціонування держави, а й самі умови здійснення публічного управління. Держава одночасно має забезпечувати захист інформаційного простору, стійкість критичної інфраструктури, інформаційні права людини, функціонування демократичних інститутів, протидію

деструктивним інформаційним впливам, адаптацію до технологічних змін та збереження власної управлінської спроможності [135].

За таких умов цивілізаційну безпеку недоцільно розглядати як ще одну відокремлену галузеву складову національної безпеки поряд з інформаційною, економічною, воєнною, енергетичною чи іншими видами безпеки. Її методологічне значення полягає в іншому рівні узагальнення. Цивілізаційна безпека характеризує здатність держави і суспільства зберігати стійкість та спроможність до розвитку в умовах системних трансформацій, які одночасно пронизують різні сфери національної безпеки.

Саме тому в межах цього дослідження пропонується розглядати цивілізаційну безпеку як категорію, що має міжсекторальний та надгалузевий характер. Наприклад, розвиток штучного інтелекту одночасно породжує технологічні, інформаційні, економічні, воєнні, правові та гуманітарні наслідки; глобальні інформаційні платформи впливають на інформаційну безпеку, політичні процеси, економічну конкуренцію та суспільну комунікацію; трансформація міжнародного порядку одночасно позначається на воєнній, економічній, енергетичній та інформаційній безпеці держави. Отже, цивілізаційний характер загрози визначається не стільки сферою її виникнення, скільки масштабом, системністю, довготривалістю та здатністю спричиняти взаємопов’язані зміни у декількох сферах функціонування держави і суспільства**.**

З урахуванням проведеного теоретичного аналізу та обґрунтованої у попередньому підрозділі категорії інформаційно-цифрової цивілізаційної трансформації уточнюється поняття «цивілізаційна безпека»: «Цивілізаційна безпека – це стан захищеності та стійкості держави і суспільства, за якого забезпечується збереження їх ключових ціннісних, інституційних, інформаційних, культурних і технологічних основ, здатність адаптуватися до системних трансформацій цивілізаційного масштабу, протидіяти породженим ними загрозам та забезпечувати безперервність і перспективи сталого розвитку».

Уточнене визначення розвиває наявні в науковій літературі підходи до розуміння цивілізаційної безпеки, однак, на відміну від трактувань, орієнтованих переважно на цивілізаційну належність, ідентичність або захист певної

цивілізаційної спільноти, акцентує увагу на стійкості держави і суспільства до системних трансформацій цивілізаційного масштабу та державно-управлінських механізмах реагування на породжені ними загрози.

Водночас цивілізаційна безпека не підміняє категорію національної безпеки. Національна безпека залишається базовою категорією, що характеризує захищеність національних інтересів держави, суспільства і людини. Цивілізаційна безпека натомість доповнює цей підхід у частині оцінювання масштабних, довготривалих і міжсекторальних трансформацій, наслідки яких виходять за межі традиційного розмежування окремих сфер безпеки.

У цьому контексті інформаційна безпека набуває особливого значення, оскільки інформаційне середовище виступає одночасно об'єктом, ресурсом і каналом поширення цивілізаційних трансформацій та загроз. Саме через інформаційні процеси значною мірою реалізуються технологічні зміни, трансформуються суспільні комунікації, поширюються цінності й моделі поведінки, здійснюється інформаційний вплив та забезпечується функціонування сучасної системи публічного управління [19].

Цивілізаційну, національну та інформаційну безпеку доцільно розглядати не як конкуруючі або взаємозамінні категорії, а як взаємопов'язані рівні осмислення сучасного безпекового середовища. Національна безпека визначає базову систему захисту національних інтересів держави; інформаційна безпека відображає її специфічний вимір в інформаційній сфері; цивілізаційна безпека дозволяє охопити системні трансформації та загрози, що мають довготривалий, міжсекторальний і транснаціональний характер. Авторське бачення взаємозв'язку зазначених категорій представлено на рис. 1.2.

Рис.1.2. Концептуальна модель взаємозв’язку цивілізаційної, національної та інформаційної безпеки

Джерело: сформовано автором на основі власних досліджень

Як представлено на рис. 1.2, цивілізаційна безпека в запропонованій концептуальній моделі не ототожнюється з окремою складовою національної безпеки, а відображає ширший рівень осмислення системних трансформацій і загроз, здатних одночасно впливати на інформаційну, воєнну, економічну, політичну, соціальну, гуманітарну, технологічну, енергетичну та екологічну сфери. Центральне місце інформаційної безпеки в моделі обумовлене наскрізним характером інформаційних процесів, які забезпечують функціонування практично всіх сфер держави і суспільства та водночас виступають середовищем реалізації значної частини сучасних цивілізаційних загроз. Отже, запропонована модель дозволяє відобразити не ієрархічне підпорядкування трьох категорій, а їх функціональний взаємозв’язок у процесі забезпечення стійкості держави і суспільства в умовах інформаційно-цифрової цивілізаційної трансформації.

Водночас теоретичне обґрунтування цивілізаційної безпеки потребує подальшої конкретизації тих чинників, під впливом яких виникає необхідність її виокремлення в сучасному безпековому дискурсі. Йдеться насамперед про

масштабні та довготривалі процеси глобального розвитку, які здатні одночасно трансформувати політичну, економічну, технологічну, інформаційну, соціальну та гуманітарну сфери, змінювати характер суспільних відносин і створювати нові вразливості держави та суспільства. При цьому не кожен ризик або загроза можуть бути віднесені до цивілізаційного рівня. Цивілізаційного характеру вони набувають за умови масштабності, системності, довготривалості, міжсекторальності й транснаціональності їх прояву, а також здатності спричиняти фундаментальні зміни в умовах функціонування та розвитку держави і суспільства.

Особливого значення зазначені процеси набувають в інформаційній сфері, оскільки сучасні цивілізаційні виклики не лише породжують нові інформаційні загрози, а й значною мірою реалізуються та поширюються через інформаційне середовище. Глобалізація інформаційних потоків, розвиток штучного інтелекту й цифрових платформ, алгоритмізація комунікації, технологічна залежність, трансформація міжнародного безпекового середовища та поширення гібридних форм протиборства змінюють характер, масштаби і механізми виникнення інформаційних загроз. Відтак, це зумовлює необхідність переходу від їх розгляду як сукупності окремих загроз інформаційній сфері до дослідження сучасних цивілізаційних викликів та породжених ними інформаційних загроз як чинників трансформації державного регулювання інформаційної безпеки.

1.3. Сучасні цивілізаційні виклики та інформаційні загрози як чинники трансформації державного регулювання інформаційної безпеки

Сучасний етап цивілізаційного розвитку характеризується формуванням комплексу взаємопов’язаних викликів, масштаб і характер яких істотно змінюють безпекове середовище та традиційні механізми державного реагування. Якщо протягом тривалого періоду проблематика безпеки розглядалася переважно крізь призму захисту держави від чітко визначених внутрішніх і зовнішніх загроз, то поглиблення глобалізаційних процесів, інформаційно-технологічний розвиток, цифровізація суспільних відносин,

трансформація міжнародного порядку та зростання взаємозалежності держав поступово ускладнюють саму природу сучасних безпекових процесів.

Як було обґрунтовано у попередніх підрозділах, становлення інформаційного суспільства та подальше поглиблення інформаційно-цифрової цивілізаційної трансформації супроводжуються не лише розширенням можливостей суспільного розвитку, а й виникненням нових вразливостей держави та суспільства. Інформація, знання, дані, цифрові технології, глобальні інформаційні мережі та алгоритмічні системи дедалі більше визначають функціонування публічного управління, економіки, оборони, соціальної сфери, міжнародної взаємодії та суспільної комунікації. Унаслідок цього порушення стабільності інформаційного середовища або його використання з деструктивною метою здатне спричиняти наслідки, що виходять далеко за межі безпосередньо інформаційної сфери.

Підкреслене у дослідженні узгоджується з тенденціями трансформації безпекового середовища, сформованими під впливом глобалізації. Зокрема, глобалізаційні процеси сприяли зростанню ролі економічних, фінансових, інтелектуальних та інформаційних ресурсів у забезпеченні впливу держав, посиленню міжнародної взаємозалежності та формуванню глобального інформаційного середовища. Відповідно, національна безпека дедалі тісніше пов’язується з процесами, які виникають поза межами окремої держави та не можуть бути ефективно врегульовані виключно на національному рівні.

Водночас сучасний етап характеризується не просто збільшенням кількості загроз, а зміною характеру їх виникнення, поширення та взаємодії. Окремі процеси глобального розвитку здатні одночасно впливати на декілька сфер життєдіяльності держави, породжувати вторинні ризики та формувати каскадні наслідки. У такому разі економічний, технологічний, політичний або екологічний виклик може трансформуватися в інформаційний ризик, інформаційний ризик – у конкретну інформаційну загрозу, а її реалізація може спричинити наслідки для політичної, економічної, воєнної, соціальної, гуманітарної чи іншої складової національної безпеки.

Подібна взаємозалежність дедалі виразніше простежується і в сучасних

міжнародних оцінках глобальних ризиків. У Global Risks Report 2026 року глобальне ризикове середовище характеризується одночасним посиленням геополітичних, геоекономічних, суспільних, технологічних та екологічних ризиків. Серед найбільш значущих ризиків найближчого періоду виокремлюються геоекономічне протистояння, міждержавні конфлікти, суспільна поляризація, дезінформація та кібернетична незахищеність, тоді як негативні наслідки розвитку штучного інтелекту істотно зростають за рівнем значущості у довгостроковій перспективі [170].

Зазначене вище підтверджує, що сучасні загрози дедалі складніше досліджувати ізольовано одна від одної. Вони формують взаємопов'язане середовище, у якому технологічні зміни можуть посилювати інформаційні ризики, інформаційні загрози – суспільну поляризацію, політичні конфлікти – економічну та інформаційну нестабільність, а порушення інформаційної стійкості – знижувати спроможність держави ефективно реагувати на інші види загроз. Нині в сучасних дослідженнях глобальних ризиків дедалі більшого значення набуває аналіз не тільки окремих ризиків, а й їх взаємозв'язків та потенційних каскадних наслідків.

Для визначення впливу сучасних цивілізаційних процесів на інформаційну безпеку принципового значення набуває розмежування понять «виклик», «ризик» та «загроза». Незважаючи на їх тісний взаємозв'язок, зазначені категорії не є тотожними, оскільки характеризують різні аспекти виникнення та розвитку потенційно небезпечних для держави і суспільства процесів.

У межах цього дослідження виклик доцільно розглядати як процес, явище або сукупність змін у зовнішньому чи внутрішньому середовищі, які змінюють умови функціонування держави і суспільства та потребують відповідної адаптації системи публічного управління. При цьому виклик не обов'язково має виключно негативний характер. Залежно від спроможності держави реагувати на нього, він може одночасно створювати як нові можливості, так і нові вразливості.

Особливо виразно така подвійність простежується на прикладі цифровізації та штучного інтелекту. Їх розвиток створює можливості для підвищення ефективності публічного управління, автоматизації процесів,

аналізу значних масивів даних, розвитку науки та економіки. Водночас ті самі технології можуть використовуватися для масштабування дезінформації, створення синтетичного контенту, посилення маніпулятивного впливу, автоматизації кібератак та інших форм деструктивної діяльності. Сучасні міжнародні оцінки також підкреслюють цю дуальність: технологічний розвиток створює значні суспільні можливості, проте водночас формує ризики для інформаційної цілісності, ринку праці, суспільної стабільності та безпеки [170].

Ризик, на відміну від виклику, характеризує можливість виникнення негативних наслідків у результаті розвитку певних процесів, подій або управлінських рішень. Отже, ризик відображає потенційний характер небезпеки та пов'язаний із невизначеністю щодо її реалізації, масштабу й наслідків [23].

Загроза характеризує більш конкретизовану форму небезпеки, за якої певні явища, процеси, дії або сукупність чинників здатні безпосередньо завдати шкоди визначеним об'єктам безпеки, порушити реалізацію національних інтересів, стабільність функціонування державних інститутів, суспільства або інформаційного середовища.

Співвідношення зазначених категорій можна представити за допомогою такої послідовності (рис.1.3.) :

Рис.1.3. Взаємозв'язок категорій «виклик – вразливість – ризик – загроза – наслідки» у контексті забезпечення інформаційної безпеки

Джерело: сформовано автором на основі власних досліджень

Водночас така послідовність не повинна сприйматися як виключно

лінійна. В умовах складних соціально-технологічних систем реалізація однієї загрози може породжувати нові ризики, посилювати інші виклики та створювати каскадні наслідки. Саме ця нелінійність є однією з характерних особливостей сучасного безпекового середовища.

З огляду на це запропоновано авторську логіко-структурну модель трансформації цивілізаційних викликів в інформаційні загрози та їх впливу на державне регулювання інформаційної безпеки (Додаток А). Запропонована модель відображає послідовність формування інформаційних загроз в умовах сучасних цивілізаційних трансформацій. Цивілізаційна трансформація формує нові умови функціонування держави і суспільства, у межах яких виникають цивілізаційні виклики. Останні, впливаючи на інформаційне, технологічне, політичне, економічне та соціальне середовище, формують нові або посилюють уже існуючі вразливості. За певних умов такі вразливості зумовлюють виникнення інформаційних ризиків, які в разі їх актуалізації можуть трансформуватися в конкретні інформаційні загрози.

Реалізація інформаційних загроз, своєю чергою, здатна спричиняти наслідки, що виходять за межі інформаційної сфери та поширюються на інші складові національної безпеки, набуваючи міжсекторального характеру. Відповідно, завершальною ланкою запропонованої моделі є трансформація державного регулювання інформаційної безпеки, необхідність якої виникає внаслідок невідповідності традиційних механізмів реагування характеру, швидкості, масштабу та взаємопов’язаності сучасних інформаційних загроз.

Водночас використання категорії «цивілізаційний виклик» потребує визначення ознак, за якими відповідні процеси можуть бути віднесені саме до цивілізаційного рівня. Не кожен виклик, ризик або загроза, що виникає у процесі функціонування держави і суспільства, має цивілізаційний характер. Надмірно широке використання цієї категорії призводило б до її фактичного ототожнення з будь-якими масштабними проблемами суспільного розвитку та, відповідно, до втрати її самостійного теоретико-методологічного змісту.

Як було встановлено у попередньому підрозділі, цивілізаційний вимір безпеки пов’язаний насамперед із системними трансформаціями, наслідки яких

виходять за межі окремої сфери національної безпеки та здатні впливати на базові умови функціонування держави і суспільства. Такий підхід набуває особливого значення в умовах глобалізації та інформаційно-цифрової цивілізаційної трансформації, оскільки взаємозалежність політичних, економічних, технологічних, інформаційних, соціальних і гуманітарних процесів істотно посилює можливість поширення наслідків окремого виклику на інші сфери суспільного розвитку.

У наукових підходах до аналізу сучасного безпекового середовища простежується поступовий перехід від переважно галузевого розуміння загроз до визнання їх комплексного та взаємопов'язаного характеру. Глобалізаційні процеси сприяли посиленню взаємозалежності національної та міжнародної безпеки, розширенню кола суб'єктів міжнародних відносин та зростанню значення економічних, технологічних, інформаційних та інших невійськових чинників безпеки [143].

Зазначена тенденція не лише зберігається, а й поглиблюється в сучасному безпековому середовищі. Так, у Global Risks Report 2026 року ризики розглядаються у геополітичному, економічному, суспільному, технологічному та екологічному вимірах, причому особлива увага приділяється їх взаємозв'язкам. Серед найбільш значущих ризиків коротко- та середньострокового періоду визначаються геоекономічне протистояння, дезінформація, суспільна поляризація та кібернетична незахищеність, тоді як негативні наслідки застосування штучного інтелекту суттєво підвищуються у довгостроковій перспективі [217].

Особливого значення набуває інформаційний вимір зазначеної взаємозалежності**.** Інтеграція ключових сфер життєдіяльності держави і суспільства в інформаційне середовище створює умови, за яких вплив на один сегмент системи безпеки здатний спричиняти зміни в інших її складових. Сучасні оцінки глобальних ризиків підтверджують цю закономірність: дезінформація тісно взаємопов'язана із суспільною поляризацією та інституційною недовірою, а розвиток штучного інтелекту здатний додатково посилювати такі процеси через поширення синтетичного контенту, ускладнення

розмежування достовірної і сфальсифікованої інформації та формування каскадних наслідків у різних сферах суспільного розвитку [173].

Важливо, що подібний комплексний підхід простежується й у національному нормативно-правовому регулюванні інформаційної безпеки. Стратегія інформаційної безпеки України визначає інформаційну безпеку складовою національної безпеки, а інформаційну загрозу – через потенційно або реально негативні явища, тенденції та чинники інформаційного впливу, здатні прямо чи опосередковано завдати шкоди інтересам держави, її національній безпеці та обороні. Стратегія також передбачає необхідність раннього виявлення, прогнозування та запобігання гібридним та інформаційним загрозам, що свідчить про необхідність не лише реагування на вже реалізовану загрозу, а й урахування передумов її виникнення [101].

З огляду на зазначене та спираючись на розвинуте у попередньому підрозділі розуміння цивілізаційної безпеки, у межах цього дослідження пропонується авторське трактування відповідної категорії. Під цивілізаційним викликом пропонується розуміти масштабний, системний і довготривалий процес, явище або трансформацію, що виходить за межі окремої сфери суспільних відносин та/або національних кордонів, істотно змінює базові умови функціонування і розвитку держави та суспільства, формує нові вразливості, ризики й загрози та обумовлює необхідність адаптації державної політики і механізмів публічного управління.

Запропоноване визначення дозволяє відмежувати цивілізаційний виклик від конкретної загрози. Якщо загроза характеризує потенційно або реально негативні явища, тенденції чи чинники, здатні завдати шкоди певному об’єкту безпеки, то цивілізаційний виклик має ширший трансформаційний характер: він змінює саме середовище, у якому формуються вразливості, виникають ризики та реалізуються конкретні загрози. Все це узгоджується з нормативним розумінням інформаційної загрози, закріпленим у Стратегії інформаційної безпеки України [101], однак розширює аналітичну перспективу дослідження шляхом встановлення передумов її формування.

Отже, один цивілізаційний виклик може породжувати сукупність

взаємопов’язаних ризиків і загроз, що одночасно або послідовно проявляються у різних сферах національної безпеки. Відповідно, ця властивість зумовлює необхідність визначення критеріїв, за якими певний виклик може бути віднесений до цивілізаційного рівня.

На основі узагальнення теоретичних положень щодо цивілізаційної безпеки, результатів попередніх етапів дослідження та аналізу характеру сучасних глобальних ризиків, запропоновано виокремити шість взаємопов’язаних критеріїв цивілізаційного характеру викликів: масштабність, системність, довготривалість, міжсекторальність, транснаціональність та трансформаційний вплив**.**

Таблиця 1.5

Критерії віднесення сучасних викликів до цивілізаційних

Критерій	Зміст критерію
Масштабність	поширення впливу виклику на значні соціальні системи, держави, регіони або глобальний простір та здатність спричиняти наслідки, що виходять за межі локальної проблеми;
Системність	здатність впливати не на окремий елемент, а на сукупність взаємопов’язаних суспільних, державних, економічних, інформаційних, технологічних та інших відносин;
Довготривалість	тривалий характер розвитку виклику та збереження його безпосередніх або опосередкованих наслідків у середньо- та довгостроковій перспективі;
Міжсекторальність	одночасний або послідовний вплив на декілька сфер національної безпеки та суспільного розвитку;
Транснаціональність	здатність виникати, поширюватися або спричиняти наслідки поза межами юрисдикції окремої держави;
Трансформаційний вплив	здатність змінювати усталені моделі функціонування держави, суспільства, економіки, інформаційного середовища та системи публічного управління.

Джерело: систематизовано та сформовано автором на основі власних досліджень

Запропонована у табл. 1.5. система критеріїв дозволяє уникнути необґрунтоване розширення змісту категорії «цивілізаційний виклик». Відповідно, цивілізаційного характеру виклик набуває тоді, коли його розвиток і наслідки характеризуються сукупністю ознак масштабності, системності, довготривалості, міжсекторальності, транснаціональності та здатності трансформувати фундаментальні умови функціонування й розвитку держави та

суспільства.

При цьому наявність окремої ознаки сама по собі не є достатньою підставою для віднесення певного явища до цивілізаційних викликів. Наприклад, масштабна кібератака може становити значну загрозу інформаційній або кібербезпеці держави, однак за своєю природою залишатися конкретною формою реалізації загрози. Натомість, глобальна цифровізація, поширення штучного інтелекту та алгоритмізація суспільних процесів змінюють саме середовище функціонування держави і суспільства, мають довготривалий та транскордонний характер, впливають одночасно на економічні, політичні, соціальні, інформаційні й управлінські відносини та породжують множинність нових ризиків і загроз. Сучасні глобальні оцінки підтверджують, що негативні наслідки ШІ пов'язані, зокрема, з дезінформацією, кібернетичною незахищеністю, інституційною недовірою та іншими взаємопов'язаними суспільними ризиками [170].

Таке розмежування має принципове значення для предмета цього дослідження. Цивілізаційний виклик не є інформаційною загрозою сам по собі; він формує або трансформує середовище, в якому виникають нові інформаційні вразливості, ризики та загрози. Відповідно, державне регулювання інформаційної безпеки не може обмежуватися реагуванням на вже реалізовані інформаційні загрози, а має охоплювати їх раннє виявлення і прогнозування, оцінювання нових вразливостей, формування превентивних механізмів та адаптацію системи державного регулювання до зміни безпекового середовища. Необхідність раннього виявлення, прогнозування та запобігання інформаційним і гібридним загрозам передбачена й Стратегією інформаційної безпеки України [101].

Визначення критеріїв цивілізаційності створює методологічне підґрунтя для подальшої систематизації сучасних цивілізаційних викликів, що безпосередньо або опосередковано впливають на інформаційну безпеку держави. При цьому їх класифікація має здійснюватися не шляхом механічного переліку глобальних проблем, а з урахуванням характеру трансформацій, які вони спричиняють, нових вразливостей, що формуються під їх впливом, та

інформаційних ризиків і загроз, які виникають унаслідок таких трансформацій.

Зазначений підхід обумовлений особливим місцем інформаційного середовища в сучасних цивілізаційних процесах. Інформаційна сфера дедалі більше виступає не лише самостійним об'єктом безпекового впливу, а й середовищем, через яке наслідки технологічних, геополітичних, соціальних, економічних та інших трансформацій поширюються на різні сфери життєдіяльності держави і суспільства. Ще в дослідженнях глобалізаційних процесів зверталася увага на посилення ролі інформаційних ресурсів і глобальних інформаційних потоків та їх здатність впливати на суспільну свідомість і стан національної безпеки [48]. У сучасних умовах цей процес істотно поглиблюється внаслідок розвитку цифрових платформ, алгоритмічних систем, генеративного штучного інтелекту та автоматизованих засобів створення і поширення інформації.

Показовим є те, що Global Risks Report 2026 року відносить дезінформацію та недостовірну інформацію до найбільш значущих ризиків дворічної перспективи, а кібернетичну незахищеність – до першої десятки глобальних ризиків. Водночас негативні наслідки застосування штучного інтелекту демонструють найбільше зростання значущості при переході від короткострокової до десятирічної перспективи [171]. Відбувається поступове перетворення інформаційно-технологічних чинників на один із системоутворювальних елементів сучасного глобального безпекового середовища.

При цьому особливу увагу необхідно звернути на взаємозалежність відповідних процесів. Маніпулювання інформацією здатне посилювати суспільну та політичну поляризацію, знижувати рівень інституційної довіри та ускладнювати реагування держави на кризові ситуації. Своєю чергою, розвиток штучного інтелекту створює додаткові можливості для генерування синтетичного контенту та ускладнює розмежування автентичної й штучно створеної інформації [173].

Отже, цивілізаційні виклики доцільно аналізувати не ізольовано, а через механізм формування під їх впливом нових інформаційних вразливостей,

ризиків і загроз. Відповідно до запропонованої у Додатку А логіко-структурної моделі, в межах дослідження систематизовано ключові цивілізаційні виклики, що мають безпосередній або опосередкований вплив на інформаційну безпеку держави (Додаток Б). Представлена систематизація демонструє, що цивілізаційні виклики та інформаційні загрози не перебувають у відношенні «один виклик – одна загроза». Навпаки, один і той самий цивілізаційний виклик може одночасно формувати декілька інформаційних вразливостей та породжувати комплекс взаємопов'язаних інформаційних ризиків і загроз. Водночас одна й та сама інформаційна загроза може виникати під впливом різних цивілізаційних процесів. Так, дезінформація може бути пов'язана з геополітичним протиборством, розвитком штучного інтелекту, суспільною поляризацією, кризовими явищами або культурно-ціннісними трансформаціями [181].

Саме тому інформаційні загрози набувають у сучасному безпековому середовищі мультиплікативного характеру. Вони не лише безпосередньо завдають шкоди інформаційній сфері, а й здатні посилювати негативні наслідки інших цивілізаційних викликів. Наприклад, дезінформація в умовах суспільної поляризації здатна поглиблювати соціальні суперечності; в умовах геополітичного протиборства – використовуватися для впливу на суспільну думку та державні рішення; під час екологічної або іншої масштабної кризи – ускладнювати кризове управління; а в умовах розвитку генеративного штучного інтелекту – масштабуватися зі швидкістю та обсягами, недоступними традиційним засобам створення інформаційного контенту. Взаємозв'язок дезінформації, суспільної поляризації, інституційної недовіри та технологічних ризиків простежується й у сучасних глобальних оцінках [174].

Зазначене дозволяє уточнити положення, закладене в логіко-структурній моделі (Додаток Б): цивілізаційні виклики формують середовище виникнення інформаційних загроз, тоді як інформаційні загрози виступають одним із механізмів, через які наслідки цивілізаційних трансформацій поширюються на різні сфери національної безпеки.

Особливе значення в цьому процесі має штучний інтелект. Його розвиток найбільш наочно демонструє відмінність між цивілізаційним викликом та

конкретною інформаційною загрозою. Штучний інтелект як технологічна трансформація сам по собі не є інформаційною загрозою. Він створює значні можливості для державного управління, економіки, науки, оборони та суспільного розвитку, але водночас формує нові вразливості, пов'язані з автоматизацією створення інформації, непрозорістю алгоритмічних рішень, складністю встановлення автентичності контенту та масштабуванням інформаційного впливу [124]. Натомість deepfake, автоматизоване генерування дезінформації або використання ШІ для персоналізованого маніпулятивного впливу є вже конкретними проявами інформаційних загроз. Global Risks Report 2026 також відзначає різке зростання довгострокового значення негативних наслідків ШІ та їх зв'язок із дезінформацією і кібернетичною незахищеністю [171].

Не менш важливою закономірністю є міжсекторальність наслідків інформаційних загроз. Інформаційна загроза, виникаючи та реалізуючись в інформаційному середовищі, може спричиняти політичні, економічні, соціальні, гуманітарні, воєнні або технологічні наслідки. Відповідно, інформаційна безпека дедалі менше може забезпечуватися ізольовано від інших напрямів державної політики. Такий висновок узгоджується і зі Стратегією інформаційної безпеки України, мета якої пов'язує забезпечення інформаційної безпеки не лише із захистом інформаційного простору, але й із соціальною та політичною стабільністю, обороною держави, захистом суверенітету, територіальної цілісності, конституційного ладу та прав і свобод громадян [101].

Водночас проведена систематизація дозволяє виявити ще одну принципову проблему. Швидкість виникнення та трансформації сучасних інформаційних загроз дедалі частіше перевищує швидкість адаптації традиційних механізмів державного регулювання. Особливо виразно це проявляється у сфері штучного інтелекту, алгоритмічного поширення інформації, цифрових платформ та транскордонних інформаційних процесів, для яких характерними є технологічна динамічність, відсутність чіткої територіальної прив'язки та участь значної кількості державних і недержавних суб'єктів.

Чинна Стратегія інформаційної безпеки України вже передбачає створення системи раннього виявлення, прогнозування та запобігання гібридним та інформаційним загрозам, а також необхідність швидкого реагування держави і суспільства на такі загрози. Разом із тим Стратегія була затверджена у 2021 році і розрахована на період до 2025 року, що саме по собі актуалізує питання подальшого розвитку стратегічних і регуляторних засад інформаційної безпеки з урахуванням суттєвих змін сучасного інформаційно-технологічного та безпекового середовища [101].

Отже, встановлена взаємозалежність між цивілізаційними викликами, інформаційними вразливостями, ризиками, загрозами та їх міжсекторальними наслідками свідчить про необхідність переходу від переважно реактивної моделі державного регулювання інформаційної безпеки, орієнтованої на реагування на вже сформовані загрози, до адаптивної та превентивної моделі**,** здатної забезпечувати прогнозування трансформацій безпекового середовища, раннє виявлення нових вразливостей і ризиків, міжсекторальну координацію та своєчасну адаптацію механізмів державного регулювання.

Встановлений характер сучасних цивілізаційних викликів та породжених ними інформаційних загроз надає підстави стверджувати, що трансформації потребує не лише сукупність інструментів протидії окремим загрозам, а сама логіка державного регулювання інформаційної безпеки. Традиційний підхід, за якого основна управлінська реакція формується після виявлення конкретної загрози або факту негативного інформаційного впливу, в умовах високої швидкості технологічних змін, транскордонності інформаційних потоків та взаємозалежності різних сфер національної безпеки виявляється недостатнім.

Необхідність превентивного реагування частково вже закладена у вітчизняному стратегічному регулюванні. Так, Стратегія інформаційної безпеки України передбачає створення системи раннього виявлення, прогнозування та запобігання гібридним загрозам, а також максимально швидке виявлення інформаційних загроз і реагування на них держави та суспільства. Водночас серед основних напрямів забезпечення інформаційної безпеки визначено стійкість і взаємодію, що підтверджує поступовий відхід від суто реактивного

розуміння забезпечення інформаційної безпеки [101].

Проте в умовах інформаційно-цифрової цивілізаційної трансформації превентивність має розглядатися ширше, ніж раннє виявлення вже сформованої інформаційної загрози. Як засвідчує запропонована у дослідженні логіко-структурна модель, формуванню конкретної інформаційної загрози передує виникнення цивілізаційного виклику, формування або посилення вразливостей та виникнення інформаційного ризику. Отже, об'єктом управлінської уваги держави мають ставати не лише самі загрози, а й динамічні зміни середовища, здатні сформувати нові вразливості та ризики ще до моменту їх трансформації у безпосередню загрозу інформаційній безпеці [29].

Саме тому перспективним напрямом розвитку державного регулювання інформаційної безпеки є перехід від переважно реактивної до превентивно-адаптивної моделі державного регулювання. Під такою моделлю в межах нашого дослідження пропонується розуміти систему цілеспрямованого державного впливу у сфері інформаційної безпеки, яка ґрунтується на постійному прогнозуванні змін інформаційного та безпекового середовища, ранньому виявленні нових вразливостей, оцінюванні інформаційних ризиків, попередженні формування та реалізації інформаційних загроз, міжсекторальній координації суб'єктів і своєчасній адаптації нормативно-правових, організаційних, інформаційно-комунікаційних та технологічних механізмів державного регулювання.

Ключовою відмінністю запропонованої превентивно-адаптивної моделі є перенесення управлінського акценту з реагування на наслідки реалізованої інформаційної загрози на виявлення та регулювання передумов її формування. Це не означає відмови від механізмів реагування, нейтралізації та відновлення. Навпаки, вони зберігають своє значення, але інтегруються у ширший управлінський цикл, який охоплює прогнозування, попередження, реагування, адаптацію та оцінювання результативності здійснених заходів.

Такий підхід відповідає сучасній тенденції до ризик-орієнтованого регулювання цифрового середовища**.** Зокрема, Регламент ЄС 2022/2065 про єдиний ринок цифрових послуг (Digital Services Act) передбачає для дуже

великих онлайн-платформ і пошукових систем систематичне оцінювання системних ризиків, що виникають унаслідок дизайну, функціонування та використання їхніх сервісів, а також запровадження пропорційних заходів їх мінімізації. Регламент окремо враховує ризики для суспільної дискусії, громадської безпеки та основоположних прав і передбачає спеціальний механізм реагування у кризових ситуаціях [202].

Аналогічний напрям простежується у рекомендаціях UNESCO щодо врядування цифрових платформ. Вони передбачають поєднання оцінювання ризиків, прозорості, підзвітності, захисту прав людини та багатосторонньої взаємодії держав, цифрових платформ, громадянського суспільства, медіа, академічного і технічного середовища. Особливо важливим є положення про необхідність оцінювання ризиків не лише після виникнення негативних наслідків, а й до суттєвих змін дизайну платформ, важливих управлінських рішень, а також у відповідь на кризу, конфлікт чи значні зміни середовища їх функціонування [175].

Отже, міжнародні підходи також демонструють поступове зміщення акценту від реагування на окремий негативний контент або вже реалізовану загрозу до оцінювання системних ризиків, управління ними та підвищення стійкості інформаційного середовища**.** При цьому важливим принципом такого регулювання залишається забезпечення балансу між безпекою та дотриманням прав людини, насамперед свободи вираження поглядів, доступу до інформації та права на приватність. UNESCO наголошує, що протидія дезінформації та іншому шкідливому контенту має здійснюватися із дотриманням міжнародних стандартів прав людини, а державні заходи не повинні бути свавільними чи непропорційними.

Вищезазначене дозволяє визначити основні напрями трансформації державного регулювання інформаційної безпеки (табл. 1.6).

Таблиця 1.6

Напрями трансформації державного регулювання інформаційної безпеки в умовах сучасних цивілізаційних викликів

Традиційний підхід	Необхідна трансформація	Зміст трансформації
Реактивність	Превентивність	перехід від реагування переважно на реалізовані загрози до прогнозування, раннього виявлення вразливостей і оцінювання інформаційних ризиків;
Статичність регулювання	Адаптивність	постійне оновлення механізмів державного регулювання відповідно до технологічних, інформаційних та суспільних змін;
Галузева фрагментарність	Міжсекторальність	координація інформаційної безпеки з політичною, воєнною, економічною, соціальною, гуманітарною, технологічною та іншими сферами національної безпеки;
Орієнтація на окремі загрози	Ризик-орієнтований підхід	системне виявлення вразливостей, оцінювання й ранжування ризиків та визначення пріоритетності державного реагування;
Переважно внутрішньодержавне регулювання	Транснаціональна координація	розвиток міжнародного співробітництва та механізмів взаємодії щодо транскордонних інформаційних і цифрових загроз;
Домінування державного суб'єкта	Багатосуб'єктна взаємодія	залучення органів влади, місцевого самоврядування, цифрових платформ, медіа, громадянського суспільства, наукових установ та інших суб'єктів;
Контроль інформаційних процесів	Забезпечення інформаційної стійкості	формування здатності держави і суспільства протидіяти деструктивному інформаційному впливу, адаптуватися та відновлювати нормальне функціонування;
Регулювання переважно контенту	Системне регулювання інформаційного середовища	врахування ролі алгоритмів, платформ, технологічної архітектури, механізмів поширення контенту та системних інформаційних ризиків;
Періодичне стратегічне планування	Безперервний моніторинг і прогнозування	постійне відстеження змін інформаційного середовища, технологічних трендів та нових цивілізаційних викликів;
Оцінювання результату після реалізації заходів	Циклічне оцінювання та коригування	регулярне оцінювання ефективності державного регулювання та оперативне коригування механізмів відповідно до зміни ризиків.

Джерело: систематизовано та сформовано автором на основі власних досліджень

Представлені у табл 1.6. напрями не означають повної заміни існуючих механізмів державного регулювання новими. Йдеться насамперед про зміну принципів їх побудови та функціонування. Реагування на інформаційні загрози залишається необхідною функцією держави, однак воно має доповнюватися прогнозуванням; нормативне регулювання – механізмами оперативної адаптації; державний контроль – координацією та партнерською взаємодією; захист інформаційного простору – формуванням його стійкості; національні механізми – міжнародною координацією.

При цьому превентивність та адаптивність є взаємопов'язаними, але не тотожними характеристиками запропонованої моделі. Превентивність характеризує здатність державного регулювання виявляти та мінімізувати вразливості й ризики до моменту реалізації загрози, тоді як адаптивність відображає спроможність системи державного регулювання змінювати власні механізми відповідно до трансформації інформаційного, технологічного та безпекового середовища. Їх поєднання дозволяє перейти від ситуативної відповіді на окремі інформаційні загрози до системного управління процесами їх виникнення.

Важливою характеристикою превентивно-адаптивної моделі має стати також ризик-орієнтованість. В умовах постійного розширення спектра інформаційних загроз держава об'єктивно не може забезпечити однаковий рівень регуляторного впливу щодо кожної потенційної небезпеки. Відповідно, необхідними є ідентифікація критичних вразливостей, оцінювання ймовірності та потенційних наслідків реалізації ризиків, визначення їх пріоритетності та концентрація державних ресурсів на тих напрямах, де реалізація інформаційної загрози здатна спричинити найбільш значні міжсекторальні наслідки. Подібна логіка оцінювання та мінімізації системних ризиків покладена, зокрема, в основу регуляторного підходу ЄС до дуже великих цифрових платформ [203].

Не менш суттєвим є перехід від галузевої фрагментарності до міжсекторальної координації. Запропонована раніше модель свідчить про те, що реалізація інформаційної загрози може одночасно впливати на декілька

складових національної безпеки. Відтак інформаційна безпека не може ефективно регулюватися як ізольований напрям державної політики [31]. Необхідною є інституційно закріплена взаємодія суб'єктів, відповідальних за інформаційну, кібернетичну, воєнну, економічну, соціальну, гуманітарну та технологічну безпеку, із забезпеченням обміну інформацією про ризики та координації управлінських рішень.

Водночас транскордонний характер сучасного інформаційного середовища обумовлює необхідність посилення міжнародної регуляторної координації. Національна юрисдикція держави не завжди збігається з фактичними межами функціонування цифрових платформ, інформаційних потоків, технологічних сервісів та алгоритмічних систем. Тому ефективність державного регулювання інформаційної безпеки дедалі більше залежить від міжнародного обміну інформацією, гармонізації підходів до оцінювання ризиків, співпраці регуляторів та взаємодії з глобальними цифровими платформами. UNESCO також розглядає врядування цифрових платформ як багатосторонній процес за участю держав, платформ, міжнародних організацій, громадянського суспільства, медіа, наукової та технічної спільноти [175].

При цьому посилення регуляторної спроможності держави не повинно ототожнюватися з необмеженим розширенням державного контролю над інформаційним середовищем. Ефективність державного регулювання інформаційної безпеки має поєднуватися із забезпеченням прав і свобод людини, принципами пропорційності, прозорості та підзвітності [141]. Такий баланс набуває особливого значення в умовах протидії дезінформації, регулювання цифрових платформ та застосування алгоритмічних технологій, оскільки надмірні або непропорційні обмеження самі можуть створювати ризики для свободи вираження поглядів та доступу до інформації. На необхідності саме такого правозахисного підходу наголошують рекомендації UNESCO щодо врядування цифрових платформ [175].

Отже, трансформація державного регулювання інформаційної безпеки в умовах сучасних цивілізаційних викликів полягає не лише в розширенні переліку регуляторних інструментів, а насамперед у переході до іншої логіки управління

інформаційними ризиками і загрозами**.** Така логіка передбачає випереджальне виявлення змін безпекового середовища, прогнозування нових вразливостей, ризик-орієнтоване визначення пріоритетів, міжсекторальну та міжнародну координацію, багатосуб'єктну взаємодію, постійне оцінювання ефективності регуляторних механізмів та їх адаптацію до динаміки інформаційно-цифрової цивілізаційної трансформації.

Враховуючи усе вищезазначене превентивно-адаптивну модель державного регулювання інформаційної безпеки доцільно представити як безперервний управлінський цикл (рис.1.4).

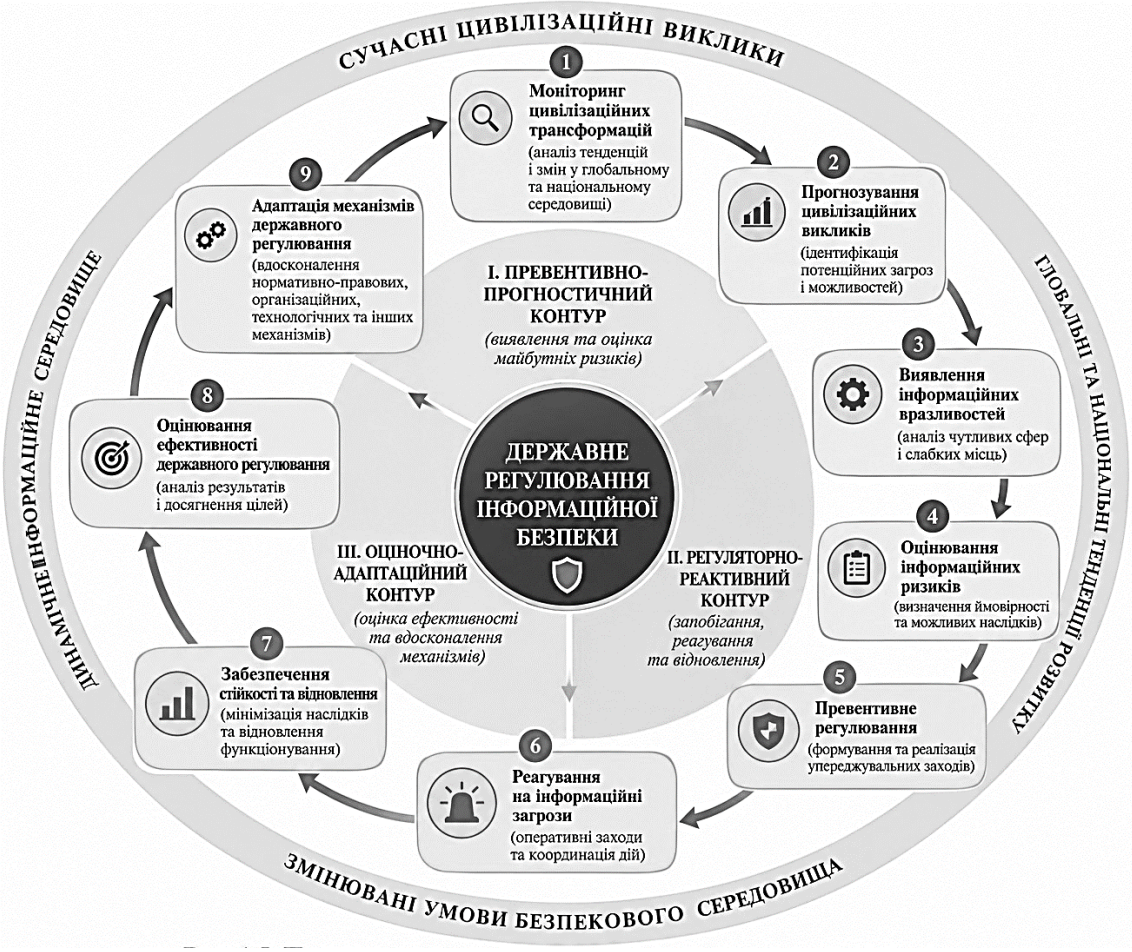

Рис. 1.4. Превентивно-адаптивна модель державного регулювання інформаційної безпеки в умовах сучасних цивілізаційних викликів

Джерело: власна розробка автора

Як представлено на рис. 1.4, запропонована превентивно-адаптивна модель державного регулювання інформаційної безпеки має циклічний характер та охоплює три взаємопов'язані функціональні контури: превентивно-

прогностичний, регуляторно-реактивний та оціночно-адаптаційний. На відміну від переважно реактивного підходу, за якого управлінський вплив активізується після виникнення або реалізації конкретної інформаційної загрози, запропонована модель передбачає перенесення частини державного регуляторного впливу на попередні стадії її формування: моніторинг цивілізаційних трансформацій, прогнозування викликів, виявлення вразливостей та оцінювання інформаційних ризиків.

Циклічність моделі забезпечується наявністю зворотного зв'язку між результатами державного регулювання та подальшою адаптацією його механізмів. Оцінювання ефективності здійснених заходів виступає підставою для коригування нормативно-правових, організаційно-інституційних, інформаційно-комунікаційних і технологічних механізмів, після чого оновлений управлінський цикл знову розпочинається з моніторингу цивілізаційних трансформацій. У такий спосіб державне регулювання набуває здатності не лише реагувати на наявні інформаційні загрози, а й адаптуватися до постійної зміни умов їх формування**.**

Отже, проведене дослідження засвідчує, що сучасні цивілізаційні виклики виступають не лише зовнішніми чинниками зміни безпекового середовища, а й визначальними передумовами трансформації державного регулювання інформаційної безпеки. Їх масштабність, системність, довготривалість, міжсекторальність, транснаціональність та здатність змінювати фундаментальні умови функціонування держави і суспільства обумовлюють формування нових інформаційних вразливостей, ризиків і загроз, наслідки реалізації яких можуть поширюватися на різні складові національної безпеки. За таких умов ефективність державного регулювання інформаційної безпеки дедалі більше залежить не лише від спроможності держави протидіяти конкретним інформаційним загрозам, а й від здатності своєчасно виявляти та прогнозувати зміни інформаційного середовища, оцінювати потенційні ризики й адаптувати відповідні механізми державного впливу.

На основі встановленого причинно-наслідкового взаємозв'язку між цивілізаційними трансформаціями, цивілізаційними викликами,

інформаційними вразливостями, ризиками, загрозами та їх міжсекторальними наслідками обґрунтовано необхідність переходу від переважно реактивного до превентивно-адаптивного підходу до державного регулювання інформаційної безпеки. Принципова відмінність такого підходу полягає у зміщенні акценту державного регуляторного впливу з реагування на вже сформовані або реалізовані інформаційні загрози на своєчасне виявлення передумов їх виникнення, прогнозування розвитку ризиків, формування превентивних заходів та забезпечення постійної адаптації регуляторних механізмів до змін цивілізаційного масштабу. При цьому превентивність, адаптивність, ризик-орієнтованість, міжсекторальна координація, багатосуб'єктна взаємодія та забезпечення інформаційної стійкості розглядаються як взаємопов'язані характеристики сучасного державного регулювання інформаційної безпеки.

Запропонована превентивно-адаптивна модель дозволяє розглядати державне регулювання інформаційної безпеки як безперервний, циклічний та динамічний управлінський процес, у межах якого моніторинг цивілізаційних трансформацій, прогнозування викликів, виявлення вразливостей, оцінювання інформаційних ризиків, превентивне регулювання, реагування на загрози, забезпечення стійкості, оцінювання результативності та адаптація регуляторних механізмів утворюють єдину функціонально взаємопов'язану систему. Її теоретико-методологічне значення полягає у формуванні цілісного підходу до державного регулювання інформаційної безпеки, який враховує не лише безпосередні прояви інформаційних загроз, а й цивілізаційні передумови їх виникнення, динаміку розвитку та можливі наслідки для інших сфер національної безпеки.

Отже, державне регулювання інформаційної безпеки в умовах сучасних цивілізаційних викликів має розглядатися як складова забезпечення не лише національної, а й цивілізаційної стійкості держави та суспільства. Представлені у дослідженні засади ґрунтуються на визнанні інформаційного середовища одночасно стратегічним ресурсом суспільного розвитку, об'єктом безпекового захисту та каналом поширення цивілізаційних трансформацій і породжених ними загроз. Відповідно, подальший розвиток системи державного регулювання

інформаційної безпеки потребує комплексного дослідження її нормативно-правового забезпечення, інституційної організації, функціональних механізмів та практичної спроможності держави забезпечувати інформаційну безпеку в умовах динамічного, транскордонного та технологічно складного безпекового середовища.

Висновки до розділу 1.

На основі узагальнення наукових підходів до сутності інформації, інформаційного суспільства та еволюції інформаційних революцій встановлено, що сучасний розвиток інформаційно-комунікаційних технологій супроводжується не лише зміною способів створення, оброблення, зберігання та поширення інформації, а й системною трансформацією економічних, політичних, соціальних та управлінських відносин. Набули подальшого розвитку теоретичні положення щодо сутності інформаційно-цифрової цивілізаційної трансформації, яку запропоновано розглядати як системний процес якісних змін суспільних, економічних, політичних та управлінських відносин, зумовлений перетворенням інформації і знань на стратегічні ресурси розвитку, глобальним поширенням цифрових технологій, мережевих форм взаємодії та алгоритмічних систем, унаслідок чого змінюються механізми функціонування держави, суспільства та взаємодії людини з інформаційним середовищем.

Встановлено, що сучасне розуміння національної безпеки характеризується переходом від вузького трактування захищеності держави від окремих видів загроз до системного підходу, який охоплює взаємопов’язані політичну, воєнну, економічну, інформаційну, соціальну, гуманітарну, технологічну, енергетичну, екологічну та інші сфери. Обґрунтовано особливе місце інформаційної безпеки в системі національної безпеки, що зумовлено наскрізним характером інформаційних процесів та їх впливом на функціонування державних інститутів, суспільну стабільність, реалізацію прав людини й захист національних інтересів. Доведено, що інформаційна безпека не може ототожнюватися виключно з кібербезпекою або технічним захистом

інформації, оскільки охоплює взаємопов’язані інформаційно-технологічний та інформаційно-комунікаційний виміри.

Розвинуто теоретико-методологічний підхід до розуміння цивілізаційної безпеки в державно-управлінському вимірі. Запропоновано визначати цивілізаційну безпеку як стан захищеності та стійкості держави і суспільства, за якого забезпечується збереження їх ключових ціннісних, інституційних, інформаційних, культурних і технологічних основ, здатність адаптуватися до системних трансформацій цивілізаційного масштабу, протидіяти породженим ними загрозам та забезпечувати безперервність і перспективи сталого розвитку. Обґрунтовано міжсекторальний та надгалузевий характер цивілізаційної безпеки, що дозволяє розглядати її не як окрему складову національної безпеки, а як ширшу теоретичну категорію, що характеризує здатність держави і суспільства зберігати стійкість в умовах масштабних, довготривалих і взаємопов’язаних цивілізаційних трансформацій.

Уточнено співвідношення цивілізаційної, національної та інформаційної безпеки. Визначено, що національна безпека формує базову систему захисту національних інтересів держави, суспільства та людини; інформаційна безпека характеризує специфічний вимір такої захищеності в інформаційній сфері; цивілізаційна безпека забезпечує ширшу теоретико-методологічну основу для оцінювання системних трансформацій і загроз, що мають міжсекторальний, довготривалий та транснаціональний характер. Запропоновано концептуальну модель взаємозв’язку зазначених категорій, у межах якої інформаційну безпеку визначено одним із ключових функціональних вимірів забезпечення цивілізаційної стійкості держави і суспільства.

Систематизовано сучасні цивілізаційні виклики, пов’язані з глобалізацією, цифровізацією, розвитком штучного інтелекту, трансформацією міжнародного порядку та посиленням технологічної й інформаційної взаємозалежності держав. Обґрунтовано, що їх визначальною особливістю є здатність формувати нові інформаційні вразливості, ризики та загрози, наслідки яких виходять за межі окремих сфер суспільного життя. Запропоновано шість критеріїв ідентифікації цивілізаційного характеру сучасних викликів: масштабність, системність,

довготривалість, міжсекторальність, транснаціональність і трансформаційний вплив. Застосування зазначених критеріїв дозволяє відмежовувати цивілізаційні виклики від локальних або галузевих проблем та визначати їх значення для державного регулювання інформаційної безпеки.

Удосконалено теоретико-методологічний підхід до визначення впливу цивілізаційних викликів на інформаційну безпеку шляхом встановлення причинно-наслідкового взаємозв'язку між цивілізаційними трансформаціями, цивілізаційними викликами, формуванням інформаційних вразливостей, виникненням ризиків, реалізацією інформаційних загроз та їх міжсекторальними наслідками для національної безпеки. Встановлено, що зазначений взаємозв'язок має динамічний і нелінійний характер, оскільки один цивілізаційний виклик здатний одночасно породжувати сукупність взаємопов'язаних інформаційних загроз, реалізація яких може спричиняти каскадні наслідки для різних складових національної безпеки. Це обґрунтовує необхідність переходу від ізольованого оцінювання окремих інформаційних загроз до комплексного дослідження передумов їх виникнення, розвитку та можливих наслідків.

Обґрунтовано необхідність трансформації державного регулювання інформаційної безпеки шляхом посилення його превентивної та адаптивної спрямованості, впровадження ризик-орієнтованого підходу, забезпечення міжсекторальної координації, багатосуб'єктної взаємодії та підвищення інформаційної стійкості держави і суспільства. Запропоновано превентивно-адаптивну модель державного регулювання інформаційної безпеки, яка охоплює три взаємопов'язані функціональні контури: превентивно-прогностичний, регуляторно-реактивний та оціночно-адаптаційний. Їх функціональна взаємодія формує безперервний управлінський цикл, спрямований на моніторинг цивілізаційних трансформацій, прогнозування викликів, виявлення інформаційних вразливостей, оцінювання ризиків, попередження та нейтралізацію загроз, забезпечення інформаційної стійкості, оцінювання результативності й адаптацію регуляторних механізмів відповідно до змін інформаційного та безпекового середовища.

Доведено, що забезпечення інформаційної безпеки в умовах сучасних

цивілізаційних викликів потребує вдосконалення не лише окремих інструментів державного впливу, а й концептуальних засад державного регулювання, орієнтованих на випереджальне виявлення ризиків, запобігання інформаційним загрозам, підвищення стійкості інформаційного середовища та систематичне коригування управлінських рішень. Запропоновані теоретико-методологічні положення формують наукове підґрунтя для подальшого дослідження нормативно-правового, інституційного та організаційного забезпечення державного регулювання інформаційної безпеки України в умовах сучасних цивілізаційних викликів.

РОЗДІЛ ІІ
АНАЛІЗ СУЧАСНОГО СТАНУ ДЕРЖАВНОГО РЕГУЛЮВАННЯ ІНФОРМАЦІЙНОЇ БЕЗПЕКИ УКРАЇНИ В УМОВАХ ЦИВІЛІЗАЦІЙНИХ ВИКЛИКІВ

2.1. Правове забезпечення державного регулювання інформаційної безпеки

Дослідження завдань регулювання інформаційної безпеки в умовах сучасного цифровізованого суспільства потребує застосування класифікаційного підходу. Такий методологічний інструментарій дозволить виокремити ключові об'єкти захисту, систематизувати актуальні загрози цифрового середовища та визначити пріоритетні напрями державної політики у цій сфері, а в подальшому – створити комплекс адекватних заходів «державного та недержавного характеру, спрямованих на підтримання оптимального інформаційного розвитку й інтеграції до світового інформаційного простору» [122].

Фахівець у галузі публічного управління, український дослідник Г. Ситник вважає, що основою державного регулювання інформаційної безпеки повинні стати результати поглибленого філософсько-політологічного та правового аналізу процесу забезпечення безпеки [113]. На його думку, «філософсько-політологічний аналіз дозволяє розглянути процес забезпечення безпеки як суспільне явище, яке спрямоване на захист і підтримку державної влади та пов'язане з інтересами життєдіяльності великих соціальних спільнот» [113]. А «правовий аналіз цінний з'ясуванням особливостей та меж можливого правового регулювання діяльності суб'єктів і об'єктів безпеки, які обумовлені існуючими правовими нормами» [113].

Отже, безпековий інструментарій розвивається за двома ключовими напрямами: нормативним та інституційним, кожен з яких має власну специфіку, функціональне призначення та логіку еволюції. Якщо нормативний напрям забезпечує кодифікацію правил і концептуалізацію стандартів відповідальної поведінки в цифровому середовищі, то інституційний – створює практичні

майданчики та механізми для їх реалізації на міжнародному й національному рівнях.

Україна – правова держава, а тому забезпечення інформаційної безпеки є однією із найважливіших її функцій, тобто офіційно визнаною діяльністю, регламентованою правовими актами [122], зокрема Конституцією (ст. 17) [44]. До нормативно-правових актів, що регулюють питання інформаційної безпеки в системі забезпечення національної безпеки України, належать Закони України «Про національну безпеку України» [93], «Про Основні засади розвитку інформаційного суспільства в Україні на 2007-2015 роки» [96], «Про Державну службу спеціального зв'язку та захисту інформації України» [83], «Про державну таємницю» [85], «Про доступ до публічної інформації» [86], «Про захист інформації в інформаційно-телекомунікаційних системах» [90], «Про основні засади забезпечення кібербезпеки України» [95], «Про інформацію» [92], Стратегія інформаційної безпеки [119] тощо. Зазначений правовий масив доповнюють інші ключові акти законодавства України: Цивільний [131] та Податковий [80] кодекси, Закони України «Про Національну програму інформатизації» [94], «Про електронні документи та електронний документообіг» [87], «Про стимулювання розвитку цифрової економіки в Україні» [104] та ін., які акцентують увагу на правовому регулюванні цифровізації як одного із головних трендів розвитку сучасного світу. Цифровізація формує новий вимір інформаційної безпеки, оскільки, по-перше, трансформує соціальні зв'язки та задає формат електронної взаємодії держави з підприємствами й населенням. По-друге, вона масштабує спектр потенційних кіберзагроз та вразливостей, що робить захист критичної інфраструктури оборонним пріоритетом держави. По-третє, вона створює ризики для безпеки персональних даних і державних реєстрів, що вимагає постійного оновлення технічного інструментарію їхнього захисту та відповідної нормативно-правової бази.

Зважаючи на масштаби глобальних інформаційних викликів, вирішити безпекові проблеми зусиллями однієї чи кількох держав неможливо. Це зумовлює необхідність поглиблення міждержавного співробітництва у сфері

забезпечення міжнародної інформаційної безпеки. Суб'єкти міжнародної взаємодії усвідомили, що лише узгоджені та взаємодоповнюючі дії на міждержавному, регіональному та світовому рівнях дозволять ефективно протидіяти актуальним викликам і загрозам. Одним із ключових напрямів такої взаємодії є підтримка створення міжнародної правової основи для співпраці та розробка єдиного термінологічного апарату в сфері забезпечення інформаційної безпеки.

Історичний аналіз актів міжнародного права дозволяє прослідкувати їх еволюцію та систематизувати етапи формування сучасних принципів відповідальної поведінки держав у цифровому середовищі. Ще у 1950 році було закладено міжнародно-правові стандарти інформаційної безпеки у положеннях Конвенції Ради Європи про захист прав людини і основних свобод [41]. У 1966 році стандарти інформаційної безпеки визначено у Міжнародній Хартії ООН про громадянські і політичні права [59]. Ідею забезпечення міжнародної інформаційної безпеки відображено в Резолюції Генеральної Асамблеї ООН A/RES/53/70 від 4 грудня 1998 року «Досягнення в галузі інформації та телекомунікацій у контексті міжнародної безпеки» [160]. Саме цей документ поклав початок глобальному діалогу про кібербезпеку та захист інформаційних систем, запустив багатосторонній переговорний процес щодо застосування норм міжнародного права в кіберпросторі, звернувши увагу світової спільноти на потенційні та реальні загрози використання інформаційних і телекомунікаційних технологій. Вперше перед державами було поставлено завдання розробити міжнародні принципи для протидії використанню мереж з метою інформаційного тероризму та злочинності.

Концептуальні засади формування глобального інформаційного суспільства та забезпечення безпеки цифрового простору дістали міжнародне закріплення в Окінавській хартії (2000 р.) [195]. Документ передбачає активізацію міждержавної взаємодії для захисту цілісності цифрових технологій, протидії правопорушенням у мережевому просторі, зміцнення економічної стабільності та забезпечення загального доступу до інформаційних ресурсів.

Ще у 2001 році Європейська Комісія презентувала документ «Мережева та

інформаційна безпека: Керівні принципи європейської політики» [156], що засвідчило становлення міжнародної інформаційної безпеки та її ключового елемента – кібербезпеки – як одного з пріоритетних напрямів діяльності ЄС. У документі мережеву та інформаційну безпеку визначено як здатність мереж чи інформаційних систем протистояти випадковим подіям або зловмисним діям, що можуть загрожувати доступності, автентичності, цілісності та конфіденційності даних, які зберігаються чи передаються, а також функціонуванню пов'язаних із ними цифрових послуг [156]. Саме таке розуміння інформаційної та мережевої безпеки лягло в основу всієї подальшої європейської термінології. Крім того, документ став одним із перших концептуальних актів, у якому систематизовано та класифіковано загрози мережевій та інформаційній безпеці (таблиця 2.1).

Таблиця 2.1

Інциденти безпеки [156]

Категорія інциденту	Механізм / Прояв загрози	Потенційні наслідки
1. Перехоплення комунікацій	Перехоплення електронних повідомлень, копіювання чи підробка даних під час передачі.	Порушення приватності, неправомірне використання чутливих даних.
2. Несанкціонований доступ	Прямий злом комп'ютерів та корпоративних/державних мереж із зловмисною метою.	Модифікація, несанкціоноване копіювання або повне знищення інформації.
3. Деструктивні мережеві атаки	Масовані атаки на веб-ресурси, зростання вразливості телекомунікаційних мереж.	Порушення доступності сервісів, дестабілізація мережевої інфраструктури.
4. Шкідливе ПЗ (Malware)	Поширення комп'ютерних вірусів, хробаків та інших деструктивних програм.	Виведення систем із ладу, незворотна втрата даних, високі фінансові збитки.
5. Фальсифікація та фішинг	Маскування під легітимні джерела, створення підроблених вебсайтів, обман користувачів.	Витік конфіденційних даних, розрив контрактів, завантаження шкідливого ПЗ.
6. Ненавмисні та форс-мажорні чинники	Стихійні лиха (повені, шторми), аварії обладнання, помилки програм чи операторів.	Апаратні збої, зупинка бізнес-процесів, системні аварії без зловмисного наміру.

Джерело: створено автором на основі [156]

Інциденти безпеки систематизовано за шістьма ключовими категоріями: 1) перехоплення комунікацій та компрометація даних, що призводить до

порушення приватності; 2) несанкціонований доступ до комп'ютерних систем із метою модифікації чи знищення інформації; 3) деструктивні мережеві атаки, спрямовані на дестабілізацію телекомунікаційної інфраструктури; 4) поширення шкідливого програмного забезпечення, яке спричиняє системні аварії та фінансові збитки; 5) соціальна інженерія та фальсифікація (фішинг, маскування під надійні джерела), що зумовлює витік конфіденційних даних; 6) ненавмисні та форс-мажорні чинники, зокрема стихійні лиха, апаратно-програмні збої та людські помилки. Такий засадничий підхід дозволив розмежувати навмисні кібератаки та техніко-антропогенні ризики, визначивши вектор подальшої гармонізації захисних механізмів на рівні Євросоюзу.

Безпекові питання посідають чільне місце й у Декларації «Побудова інформаційного суспільства – глобальне завдання у новому тисячолітті» (Declaration of Principles «Building the Information Society: a global challenge in the new Millennium»), затвердженої на Всесвітньому саміті в Женеві у 2003 році [14]. У цьому документі акцентується, що для розбудови інформаційного суспільства слід забезпечувати та зміцнювати довіру й захищеність при використанні технологій, що є одним із головних принципів створення суспільства, доступного для всіх. Декларація визначає інформаційно-комунікаційні структури як необхідну основу інформаційного суспільства та закладає принципи відкритості, прозорості, доступності, ефективності та інноваційності як підґрунтя для створення сприятливого нормативного середовища на національному рівні. Посиленню інформаційної безпеки сприяють й етичні аспекти інформаційного суспільства, зазначені в Декларації. Ними є повага до прав людини, запобігання використанню технологій з метою расизму чи дискримінації.

Важливим етапом концептуалізації безпекової політики стало затвердження Стратегії кібербезпеки Європейського Союзу (2013 р.), спрямованої на забезпечення функціонування відкритого, безпечного та стійкого кіберпростору [159].

До міжнародних правових документів, які регулюють співпрацю держав у безпековій сфері належать також Конвенція Ради Європи «Про

кіберзлочинність» 2001 року [42], Рамкове рішення Європейського Союзу щодо атак на інформаційні системи [157], «Угода про співробітництво у сфері міжнародної інформаційної безпеки» 2009 року [204] тощо.

Динамічний розвиток цифрових технологій зумовлює виникнення нових викликів інформаційній безпеці, що вимагає постійної адаптації та оновлення міжнародно-правового інструментарію. Показовою у цьому контексті є запропонована Європейською Комісією у березні 2021 року програма «Цифровий компас до 2030 року» [133]. Вона орієнтована на розбудову людиноцентричної та безпечної цифрової екосистеми, яка сприяє реалізації потенціалу громадян і розвитку бізнесу. Документ визначає чотири стратегічні вектори цієї трансформації: розвиток цифрових навичок, формування безпечної й ефективної цифрової інфраструктури, цифровізацію бізнес-процесів та цифрову трансформацію публічних послуг [115].

Логічним продовженням розбудови європейського безпекового простору стало ухвалення у 2022 році Європейським Парламентом, Радою ЄС та Європейською Комісією Декларації цифрових прав і принципів [168]. Документ виступає орієнтиром для компаній та урядів, закріплюючи фундаментальне правило, згідно з яким права людини підлягають рівноцінному захисту як в онлайн-середовищі, так і в офлайн-просторі. Декларація закладає нормативні підвалини формування безпечного цифрового середовища з високими стандартами кібербезпеки та захисту персональних даних від несанкціонованого відстеження. Важливою складовою документа є також акцент на екологічній сталості цифрових технологій і мінімізації їхнього негативного впливу на довкілля та клімат.

Отже, розпочавшись у 2000-х роках, процес становлення законодавства з інформаційної безпеки в країнах-членах ЄС та у світовому масштабі продовжується. Аналізу сучасного світового нормативно-правового регулювання цієї важливої сфери інформаційного суспільства присвячено низку наукових праць. Зокрема, трансформацію законодавства з урахуванням нових викликів та загроз досліджують такі науковці, як С. Лукашевич, Н. Філіпенко, В. Харченко [125], В. Бойко, М. Василенко, С. Кухаренко [7] та інші. Аналіз

наукової періодики в цілому дозволяє стверджувати, що український науковий дискурс (2022–2026) фокусує увагу переважно на протидії критичним інфраструктурним загрозам в умовах воєнного стану, захисті державних реєстрів, кібероборoні та адаптації національного законодавства до стандартів НАТО та ЄС. Європейський науковий дискурс (2022–2026) зосереджений на зміцненні колективної кіберстійкості (Cyber Resilience Act, NIS2), регулюванні безпеки штучного інтелекту (AI Act) та захисті критичних ланцюгів постачання.

Вітчизняна нормативно-правова база імплементувала основні міжнародні стандарти та базується на фундаментальних актах міжнародного права.

Програмним документом нормативного характеру, який стосується інформаційної безпеки є Стратегії інформаційної безпеки України [119]. Її було прийнято у 2021 році та затверджено Указом Президента України [101]. Але повномасштабне вторгнення росії 24 лютого 2022 року принципово змінило характер загроз та викликів, які не лише набули екзистенційного характеру, але й спрямовані на знищення української державності, української національної та громадянської ідентичності та єдності [52]. Виникла критична необхідність перегляду та оновлення Стратегії інформаційної безпеки як невідкладної правової відповіді на безпрецедентні виклики та загрози [52].

Тому варто погодитись з позицією провідного наукового співробітника наукової лабораторії інформаційного права та інформаційної безпеки Державної наукової установи «Інститут інформації, безпеки і права Національної академії правових наук України» Г. Красноступ, яка пропонує оновити зазначений документ та надає на розгляд наукової спільноти вісім стратегічних цілей нової Стратегії інформаційної безпеки. Дослідниця вважає, що саме реалізація таких завдань стане ефективною відповіддю на актуальні виклики сьогодення, спричинені російською агресією. Такими стратегічними цілями, на думку дослідниці, є: розвиток системи державних стратегічних комунікацій, що забезпечить проактивне поширення українських наративів та зміцнення національної ідентичності; створення ефективних механізмів реагування та співпрацю з цифровими платформами, що забезпечить протидію дезінформації та гібридним загрозам; визнання культури елементом національної безпеки;

підвищення медіаграмотності та критичного мислення громадян; удосконалення механізмів захисту прав людини в інформаційній сфері; забезпечення інформаційної реінтеграції тимчасово окупованих та деокупованих територій; посилення міжнародного співробітництва; забезпечення інформаційної єдності українців за кордоном. Досягнення цих цілей, вважає дослідниця, забезпечить не лише ефективний захист національного інформаційного простору, а й стане фундаментом для зміцнення національної безпеки України в цілому [52].

В окремий напрям національної безпеки держави виокремлено й питання забезпечення кібербезпеки. Вона постає як відносно самостійна, спеціалізована складова інформаційної безпеки, що сформувалася внаслідок стрімкого розвитку цифрових технологій та масового впровадження інформаційно-комунікаційних систем [121]. Така трансформація зумовлена необхідністю захисту інформаційного простору в специфічному цифровому середовищі – кіберпросторі, який активно розвивається. Це, у свою чергу, актуалізувало потребу в розробці комплексних техніко-технологічних та організаційних заходів захисту даних [121]. На сьогодні в Україні сформовано профільне нормативно-правове регулювання цієї сфери, базовими елементами якого є Закон України «Про основні засади забезпечення кібербезпеки України» [95], Стратегія кібербезпеки України [120] та інші.

У науковому середовищі звертають увагу на те, що інформаційна сфера є комплексним і складним об’єктом, захист якого потребує узгодженого комплексу нормативно-правових, організаційно-управлінських та техніко-технологічних заходів [18]. З огляду на це нормативно-правове забезпечення потребує розгалуженої законодавчої бази, яка наразі позбавлена необхідної системності; зокрема, у нормативно-правових актах досі відсутній єдиний понятійно-термінологічний апарат. Науковці також відмічають складність та обсяг правового регулювання, що потребує надмірних ресурсних, часових і кадрових витрат для адміністрування сфери інформаційної безпеки [18].

З іншого боку, аналіз нормативно-правової бази забезпечення інформаційної безпеки в Україні показав, що вона весь час модернізується, оскільки має відповідати сучасним викликам, бути гнучкою та адаптивною.

Зважаючи на це, варто погодитись з українською дослідницею Т. Мужановою, яка надає загальну схему нормативно-правового забезпечення інформаційної безпеки [62], систематизувавши в ній законодавчі акти, що існували в Україні станом на 2019 рік. Автор дисертаційного дослідження пропонує вдосконалити запропоновану модель та залишити в ній лише фундаментальні блоки, які можна змістовно наповнювати відповідно до динамічних трансформацій законодавства. Така модель допоможе здійснювати ефективне державне регулювання інформаційної безпеки, оскільки дозволить суб'єктам державного управління оперативно реагувати на правові трансформації, систематично актуалізуючи кожен елемент структури. Водночас в епоху цифровізації та технологічного розвитку подібну модель доцільно зробити інтерактивною, на кшталт Дії, інтегрувавши її з інформаційно-правовими системами (наприклад, «Ліга:Закон» або офіційним вебпорталом Верховної Ради України). Це забезпечить автоматизоване відстеження та оперативно-структуроване розміщення нових нормативно-правових актів у відповідних сегментах пропонованої моделі (рис. 2.1).

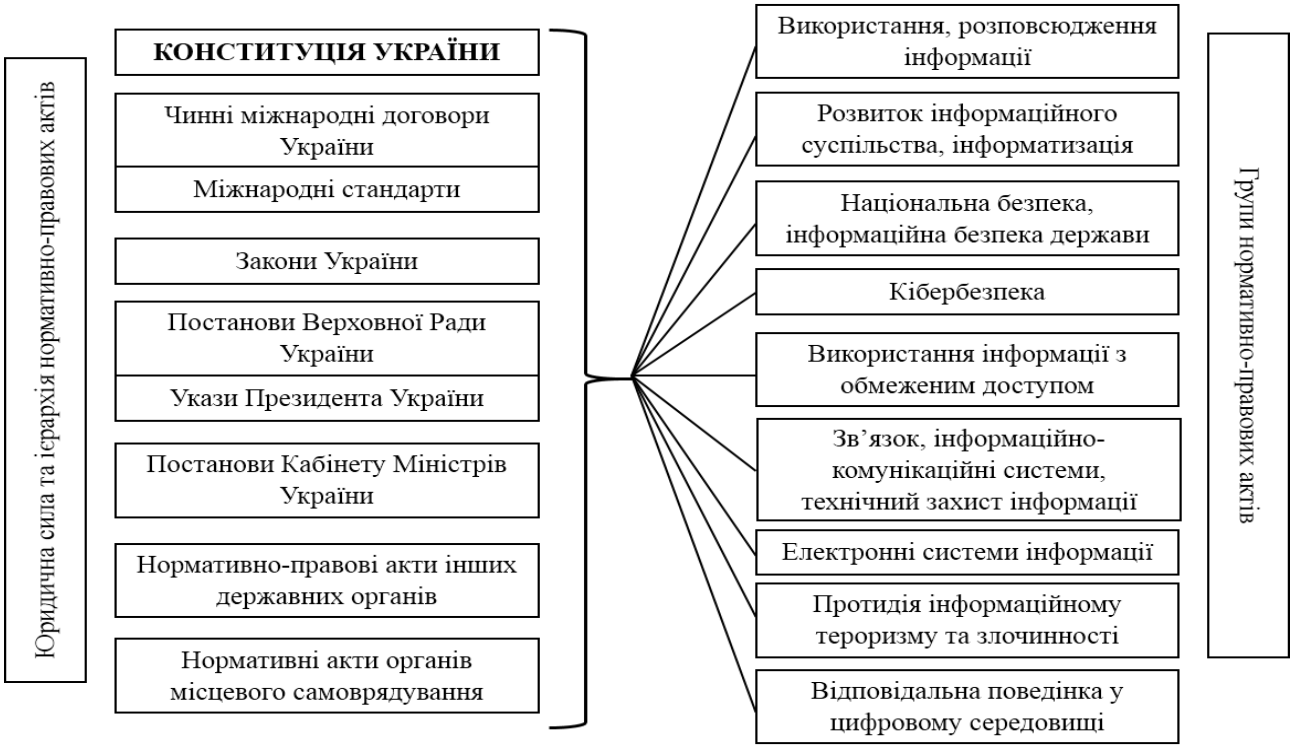

Рис. 2.1. Модель нормативно-правового забезпечення інформаційної безпеки в Україні

Джерело: створено автором на основі [62; 97]

Отже, державне регулювання інформаційної безпеки країни полягає у визначенні основних напрямків діяльності органів державної влади у цій сфері, які обумовлені змістом національних інтересів держави, суспільства та особистості і мають міждисциплінарний характер, оскільки питання забезпечення інформаційної безпеки не обмежується нормативно-правовим аспектом. Як зазначає М. Дмитренко, сучасні загрози інформаційній безпеці мають соціальний характер і зосереджені у внутрішньо-політичній, економічній, соціальній, екологічній, інформаційній та духовній сферах суспільства [18]. Тут задіяні фінансово-економічні чинники, адміністративно-організаційні заходи, науково-технічне підґрунтя, і навіть морально-етичні аспекти виховання [12]. Тому нормативно-правове регулювання інформаційної безпеки потрібно розглядати системно, враховуючи всі можливі чинники та фактори. Реалізація державної безпекової політики передбачає фокусування зусиль на системному розв'язанні низки критичних завдань. Ідеться про розробку та впровадження комплексних заходів з питань використання та поширення інформації, запобігання й нейтралізації, підвищення здатності суспільства до активної протидії негативним наслідкам інформаційно-психологічних впливів. Стратегічного значення набувають питання інтеграції національного інформаційного поля у світовий простір, модернізація системи масової комунікації, а також формування фахової підготовки особового складу сектору безпеки до інформаційного протиборства. У сучасних умовах інформаційну безпеку слід визнати основою інформаційної складової всіх сфер національної безпеки [18].

Отже, аналіз законодавства дозволив виокремити основні сфери застосування нормативно-правового забезпечення інформаційної безпеки (рис.2.2).

Рис. 2.2. Сфери застосування правових механізмів забезпечення інформаційної безпеки

Джерело: створено автором на основі [122]

Наприклад, забезпечення інформаційно-технічної (технологічної) безпеки передбачає створення можливостей для безпечного формування й розвитку інформаційних ресурсів та інформаційної політики. Складовою інформаційно-технічної (технологічної) безпеки є захист від несанкціонованого доступу, втручання, пошкодження чи знищення даних у комп'ютерах та їх системах, мережах або цифрових пристроях. Це захист від вірусів, хакерів, шкідливого програмного забезпечення тощо. У законодавстві передбачені заходи попередження та покарання за такі дії.

Окремої уваги потребує кібербезпека як самостійний і ключовий складник інформаційної безпеки. Актуальність цього напряму зумовлена цифровізацією суспільства, сплеском кіберзлочинності, застосуванням інструментів кібертероризму в гібридних конфліктах, а також потребою формування нових підходів до розбудови національної системи кіберзахисту з урахуванням викликів сучасного кіберпростору. Ефективний захист інформаційного простору є ключовим фактором забезпечення економічної стабільності та функціонування державних інституцій [40]. Успішне протистояння кіберзагрозам можливе виключно за умови комплексного застосування наявних правових інструментів та передбачає не лише розробку технологічних рішень, а й підготовку висококваліфікованих фахівців та управлінців, а також підвищення рівня загальної цифрової грамотності населення. Важливим аспектом у цьому контексті є розвиток культури кібергігієни – відповідального ставлення до

захисту персональних даних, критичного осмислення інформаційних потоків і системної протидії соціальній інженерії (зокрема фішингу), оскільки людський фактор залишається однією з найбільш уразливих ланок інформаційної безпеки [118].

Поширення соціальних мереж робить кіберпростір особливо вразливим. Так, О. Старостін зазначає [118], що для інформаційних маніпуляцій активно використовуються соціальні боти, здатні впливати на суспільну думку, поширювати дезінформацію та навіть сприяти вербуванню до терористичних угруповань. Ботоферми як мережі автоматизованих облікових записів можуть використовуватися не лише для легальних цілей (наприклад, індексування веб-сайтів пошуковими системами), а й для зловмисної діяльності, включаючи шахрайство з кліками (click fraud), організацію DDoS-атак та поширення фейкових новин. Завдяки сучасним ШІ-алгоритмам соціальні боти здатні генерувати персоналізовані відповіді, створювати переконливі повідомлення, взаємодіяти з користувачами та навіть імітувати реальну поведінку, що створює додаткові ризики для інформаційної безпеки. У цьому контексті соціальні мережі перетворюються на інструмент маніпулятивних технологій. Дезінформаційні кампанії, поширення конспірологічних теорій, кібербулінг та втручання у виборчі процеси стають частиною гібридних загроз. Тобто новітні технології, використовуючи складні алгоритми для завоювання довіри, синхронного видалення, зміни профілів, створення фальшивих облікових записів, відкривають нові можливості для кібершахрайства, поширення пропаганди та інших форм цифрової агресії. Причому, ідентифікація та нейтралізація таких продуктів вкрай складна, що зумовлює необхідність системного вдосконалення нормативно-правових механізмів регулювання кіберпростору.

Кібергігієна повинна стати провідним завданням кібербезпеки. У міжнародному дискурсі, зазначає, наприклад, О. Старостін [118], поняття «кібергігієна» розглядається як система заходів, спрямованих на мінімізацію ризиків, пов’язаних із використанням цифрових технологій. Кібергігієна включає в себе захист інформаційних ресурсів, а також заходи, спрямовані на запобігання негативному впливу цифрових технологій на здоров’я людини та

ефективні практики безпечної поведінки в інформаційному середовищі. Формування культури кібергігієни є особливо важливим для державного управління, оскільки від рівня цифрової безпеки залежить функціонування органів влади, збереження конфіденційної інформації та стійкість державних систем [118].

Отже, реформування системи державного контролю у сфері безпеки особистості та суспільства, у боротьбі з проявами корупції, а також контролю процесів, що відбуваються у кіберпросторі набуває особливого значення [27].

Актуальні виклики у сфері інформаційної та кібербезпеки вимагають від держави побудови цілісної, гнучкої та стійкої системи захисту. Навіть найдосконаліші технологічні рішення виявляються безсилими, якщо кадрова ланка не володіє базовою кібергігієною, або якщо відсутня чітка нормативно-правова та організаційна база для оперативної реакції на загрози. Саме тому дієва державна політика має базуватися не просто на механічному поєднанні окремих напрямів, а на глибокій синергії та міжкластерній взаємодії трьох основних кластерів: технологічного, організаційно-управлінського та освітнього.

Технологічний кластер відповідає за інфраструктурний базис безпеки. Він охоплює впровадження сучасних систем виявлення та реагування на загрози (SIEM/EDR), криптографічний захист інформації, захист об’єктів критичної інформаційної інфраструктури (КІІ), використання штучного інтелекту для моніторингу аномалій та системний відхід від уразливого програмного забезпечення.

Організаційно-управлінський кластер створює правову та процедурну рамку, у якій функціонує вся система. Він включає розробку нормативно-правової бази, чіткий розподіл ролей між державними органами (СБУ, Держспецзв’язку, Кіберполіція, Мінцифра), розробку регламентів та протоколів реагування для команд CERT/CSIRT, ризик-менеджмент та регуляторний контроль.

Освітній та кадровий кластер забезпечує людський капітал. Він спрямований на підготовку висококласних фахівців з кібербезпеки, регулярне підвищення кваліфікації держслужбовців, тренінги з протидії соціальній

інженерії, а також на загальне підвищення рівня кіберграмотності та безпекової культури всіх громадян.

Практична ефективність цієї політики досягається саме на перетині зазначених кластерів. Взаємодія технологій та освіти реалізується через безперервне тренування фахівців на технологічних кіберполігонах (Cyber Ranges) та формування навичок безпечної роботи з інформаційними системами. Поєднання управління та технологій забезпечує впровадження обов'язкових стандартів кібербезпеки (зокрема ISO/IEC 27001 чи моделей NIST) для державних структур і приватного сектору. Своєю чергою, союз управління та освіти закріплює нормативні вимоги щодо регулярного атестування знань з кібербезпеки для працівників критичної інфраструктури та державних органів.

Тільки такий всебічний підхід дозволяє державі ефективно нейтралізувати сучасні кіберзагрози, створити безпечне цифрове середовище та забезпечити захист інформаційних ресурсів як на рівні держави, так і для окремих користувачів [118]

Виходить, що інформаційною безпекою публічне управління повинно опікуватись на трьох рівнях, як мінімум. Первинним рівнем буде рівень особи, починаючи від інформаційної освіти, навичок інформаційної гігієни кожного члена суспільства – до підвищення рівня інформаційної гігієни на рівні чиновника, публічного управлінця. Причому, законодавство створює правові механізми забезпечення інформаційної безпеки на кожному рівні та деталізує особливості об'єктів безпеки.

Так, на рівні особи передбачається забезпечення прав і свобод людини на збирання, зберігання, використання та поширення інформації, права власності на неї; недопущення несанкціонованого втручання в зміст, процеси оброблення, передачі та використання персональних даних; неправомірного обмеження свободи слова та доступу громадян до публічної інформації та інших прав і свобод громадян, які належать до інформаційної сфери або реалізуються в ній. На рівні особи висувається також завдання захисту людини від негативного інформаційно-психологічного впливу, тобто мінімізація негативних інформаційних впливів на свідомість особистості (громадян, представників

влади, посадовців), обмеження різного роду маніпуляцій, поширення небезпечних ідей та наративів.

Інформаційна гігієна державних службовців є фундаментальним елементом загальної системи кібербезпеки та національної безпеки держави, оскільки посадовці залишаються першочерговою ціллю для ворожої розвідки, фішингових атак та інформаційно-психологічних операцій. Комплексна система навичок інформаційної гігієни чиновника охоплює чотири ключові взаємопов'язані напрями: цифрову безпеку робочого середовища, розпізнавання методів соціальної інженерії, критичне мислення для протидії дезінформації та суворе дотримання інформаційної стриманості.

Перший напрям стосується безпосереднього захисту цифрового робочого простору та дотримання технічної дисципліни. Чиновник повинен чітко розмежовувати приватне та службове життя, дотримуючись принципу використання окремих пристроїв, акаунтів та робочої пошти виключно для виконання посадових обов'язків. Обов'язковим стандартом є використання двофакторної автентифікації на основі додатків-генераторів кодів або апаратних ключів, створення складних унікальних паролів за допомогою парольних менеджерів та повна відмова від незахищених месенджерів чи сервісів, пов'язаних із країною-агресором, під час обговорення службових питань. Крім того, фізична безпека пристроїв вимагає суворої заборони на підключення неперевірених зовнішніх носіїв інформації, заблокування робочих станцій під час будь-якої відсутності, а також заборона демонстрації екрана у неперевіреному середовищі.

Тобто йдеться про два критично важливих правила фізичної та візуальної безпеки, спрямованих на запобігання витоку інформації з робочого пристрою посадовця. Зокрема, під час будь-якої відсутності чиновника, посадовця на робочому місці – вимагається обов'язкове блокування екрану комп'ютера чи смартфона. Навіть коротка відсутність створює можливість для несанкціонованого доступу сторонніх осіб, підключення шкідливих USB-пристроїв, зчитування конфіденційних даних або надсилання фейкових повідомлень від імені посадовця. Друге правило стосується утримання від

демонстрації екрана у неперевіреному середовищі. Таким середовищем можуть бути онлайн-наради у Zoom чи Teams, під час яких демонстрація екрана може спровокувати витік закритих даних, службової документації тощо. У фізичному вимірі це правило забороняє відкривати службові документи чи розгортати екран ноутбука у публічних місцях, де існує ризик візуального зчитування інформації сторонніми особами. Особливу увагу на ці вимоги слід звертати під час війни.

Така поведінка держслужбовця регулюється, зокрема, Законом України «Про захист інформації в інформаційно-комунікаційних системах» [90]. Режим поводження з документами та персональними даними формалізовано Законами України «Про державну таємницю» [85], «Про доступ до публічної інформації» [86], «Про захист персональних даних» [91] та Законом України «Про державну службу» [84], який безпосередньо покладає на посадових осіб обов'язок щодо збереження службової таємниці та дотримання безпекових норм. Деталізація цих вимог реалізується через підзаконні акти та нормативні документи уряду і профільних відомств. Зокрема, практичні аспекти кібергігієни – від заборони використання приватних поштових скриньок і незахищених месенджерів до регламенту проведення онлайн-нарад і правила стриманості при демонстрації екрана – деталізовані в Методичних рекомендаціях з кібергігієни Держспецзв'язку та Національного агентства України з питань державної служби (НАДС), рішеннях Ради національної безпеки і оборони України (РНБО), а також у внутрішніх інструкціях з діловодства та правилах внутрішнього трудового розпорядку кожної державної установи. Недотримання цих нормативно закріплених вимог тягне за собою дисциплінарну (догани чи звільнення), адміністративну (зокрема за ст. 212-2 КУпАП) або кримінальну відповідальність (у разі розголошення державної таємниці за ст. 328 КК України чи несанкціонованого втручання в роботу систем за ст. 361 КК України).

Другим критично важливим блоком є спроможність вчасно виявляти та нейтралізувати спроби соціальної інженерії й фішингу. Державному службовцю необхідно володіти навичками критичного аналізу будь-яких вхідних повідомлень, звертаючи увагу на адреси відправників, наявність підозрілих посилань та файлів із ризикованими розширеннями. Важливо зберігати

професійний скепсис щодо спроб емоційного маніпулювання, зокрема штучного створення відчуття терміновості чи тиску з посиланням на нібито вказівки керівництва. Будь-які нестандартні запити на передачу даних або виконання фінансових чи розпорядчих дій мають обов'язково верифікуватися через альтернативні та перевірені канали зв'язку.

Третій напрям передбачає розвинене критичне мислення для захисту від інформаційно-психологічних впливів та деструктивних наративів. Чиновник зобов'язаний споживати інформацію виключно з перевірених офіційних джерел та медіа з прозорою редакційною політикою, уникаючи використання анонімних Telegram-каналів чи сумнівних пабліків. Здатність ідентифікувати ознаки маніпуляцій, викривлення фактів та провокацій дозволяє запобігти поширенню фейків. Емоційна саморегуляція та правило часової паузи перед реакцією на шокуючі чи гучні новини допомагають оцінювати безпекову ситуацію раціонально та виважено.

Четвертим напрямом є контроль власного цифрового сліду та забезпечення захисту від збору даних методами розвідки на основі відкритих джерел (OSINT). Посадовець повинен усвідомлювати ризики надмірної публічності у соціальних мережах, утримуючись від розміщення геотегів з точним місцезнаходженням (позначки геопозиції), деталей робочого графіку, фотографій внутрішнього інтер'єру службових приміщень, перепусток чи службових документів. Суворе дотримання режиму таємності та вимог законодавства щодо роботи з інформацією з обмеженим доступом і персональними даними громадян виступає остаточною запорукою надійного функціонування всього державного апарату в сучасному інформаційному просторі.

Інформаційна безпека на рівні суспільства та держави – це саме ті нормативно-правові акти, про які йшлося вище, які забезпечують збереження і примноження духовних, культурних та моральних цінностей; формування і розвиток демократичних інститутів громадянського суспільства на рівні суспільства. На рівні держави – це недопущення інформаційної залежності, інформаційної блокади країни або експансії інших держав та міжнародних структур [122], захист інформаційного суверенітету тощо.

Правові аспекти інформаційної безпеки звертають також увагу на форми державного забезпечення. Закон регламентує сферу інформаційних відносин, зокрема, передбачено забезпечення якісного інформування суспільства (напр., Закон України «Про інформацію» [92]), впровадження процесів інформатизації (напр., Закон України «Про Основні засади розвитку інформаційного суспільства в Україні на 2007-2015 роки» [96]), визначено види правопорушень у інформаційній сфері та передбачено покарання за них. Зміст державного забезпечення інформаційної безпеки може інтерпретуватися як система державних гарантій в інформаційній сфері, прямо чи опосередковано визначених фундаментальними нормативно-правовими актами, що регламентують інформаційну сферу суспільних відносин.

Отже, головні завдання інформаційної безпеки полягають у мінімізації шкоди від неповноти, несвоєчасності чи недостовірності інформації, протидії негативному впливу інформаційних технологій та розголошенню даних, що вимагає визначення прав і обов'язків її суб'єктів згідно з міжнародним і вітчизняним законодавством та формування відповідних державних інститутів [6].

У такому контексті нормативно-правове регулювання інформаційної безпеки набуває особливого значення для розвитку суспільства й держави, а також визначає чіткий алгоритм залучення необхідних інструментів і ресурсів, окреслює юридичні межі діяльності суб'єктів та їхній правовий статус, створює регламент дій, виконуючи ряд важливих функцій, головними з яких є регулятивно-правова, нормативно-гарантувальна та організаційно-процедурна (рис.2.3).

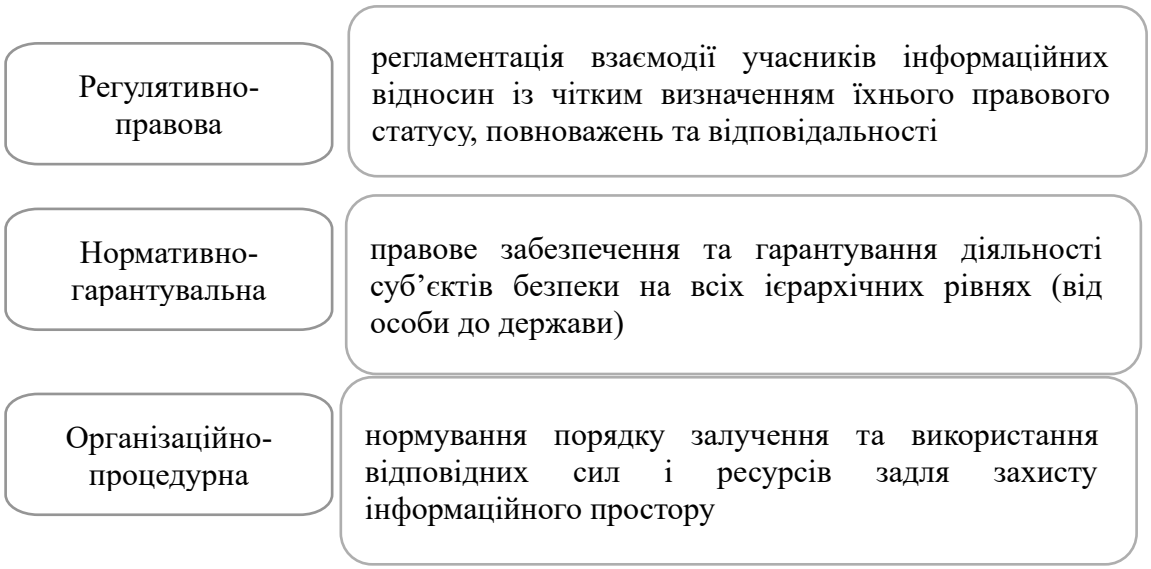

Рис. 2.3. Провідні функції нормативно-правового регулювання інформаційної безпеки

Джерело: створено автором на основі [62]

Регулятивно-правова функція нормативно-правового регулювання інформаційної безпеки забезпечує формування законодавчо обгрунтованого «каркасу» та нормативних правил поведінки для всіх суб'єктів інформаційних відносин. За допомогою цієї функції визначаються юридичні статуси інформації (відкрита, таємна, службова, персональні дані), об'єктів інфраструктури, зокрема, встановлюються критерії їх критичності, та суб'єктів національної системи безпеки. Саме у цьому сегменті регулювання інформаційної безпеки закріплюються права, обов'язки та межі дозволеної або забороненої поведінки для державних органів, приватного сектору, команд реагування на інциденти і громадян, а також забезпечується адаптація національного законодавства до міжнародних та європейських стандартів протидії сучасним інформаційним та цивілізаційним загрозам.

Нормативно-гарантувальна функція знаходить своє втілення у створенні юридичних гарантій захисту інформаційних прав, зокрема, конституційних прав громадян на доступ до інформації, захист приватності та конфіденційність персональних даних; визначенні підстав для настання адміністративної, цивільно-правової та кримінальної відповідальності за кіберзлочини та кримінальні правопорушення в інформаційній сфері, як-от: несанкціонований

доступ, витік даних чи перешкоджання роботі інформаційно-комунікаційних систем.

Організаційно-процедурна функція деталізує нормативні приписи до рівня практичних алгоритмів, протоколів та інституційних механізмів реалізації політики інформаційної безпеки. Саме вона встановлює чіткий юридичний порядок інформування про кібератаки, формалізує регламенти взаємодії між суб'єктами системи інформаційної безпеки, а також визначає порядок проведення аудиту та встановлює єдині стандарти захищеності об'єктів. Крім того, дана функція охоплює нормотворче забезпечення дій у надзвичайних ситуаціях чи під час особливих правових режимів, алгоритми швидкого відновлення функціонування критичних систем після збоїв або кібератак.

Ключова якість нормативно-правового регулювання інформаційної безпеки полягає в тому, що названі функції не діють ізольовано, а перебувають у стані постійної взаємодії. Синергія цих функцій дозволяє трансформувати абстрактні норми права у дієвий інструментарій забезпечення інформаційної безпеки перед цивілізаційними викликами та загрозами.

В цілому, нормативно-правове регулювання інформаційної безпеки варто розглядати як багаторівневу, системну та динамічну конструкцію, яка забезпечує правове закріплення засад державного управління у сфері інформаційної безпеки, кіберзахисту, визначає повноваження суб'єктів системи національної безпеки, створює надійну основу для захисту інформаційного суверенітету держави в умовах сучасних цивілізаційних викликів. Нормативно-правове регулювання інформаційної безпеки встановлює обов'язкові вимоги, стандарти та регламенти щодо ідентифікації загроз, моніторингу та реагування на кіберінциденти, гарантуючи безперервність функціонування об'єктів критичної інфраструктури та правовий захист суб'єктів інформаційних відносин, якими є людина, держава та суспільство. Потрібно зазначити, що правова база інформаційної безпеки у системі національної постійно трансформується під впливом появи нових кібер- та цивілізаційних загроз, технологічних рішень та спрямована на гармонізацію національного законодавства з міжнародними стандартами й нормами.

2.2. Інституційне забезпечення державного регулювання інформаційної безпеки в системі національної безпеки України

Задовго до початку XXI ст. світ зрозумів, що подальший розвиток суспільства вирішальною мірою буде залежати від інформаційної сфери, а інформація та інформаційні технології набуватимуть виняткового значення для забезпечення національної безпеки. Зважаючи на зростання кількості інформаційних злочинів та підвищення рівня інформаційної небезпеки, Генеральна Асамблея ООН у 2019 році прийняла резолюцію під назвою «Заохочення держав до відповідальних дій у кіберпросторі в контексті міжнародної безпеки» [142], акцентувавши на необхідності створення безпечного, відкритого, доступного та стабільного цифрового середовища.

Утім, ще на початку 2000-х безпековими питаннями в інформаційній сфері та спробами створення відповідного інституційного забезпечення активно опікувалися міжнародні організації, Європейський Союз і уряди національних держав.

Так, у листопаді 2003 року Генеральний секретар ООН Кофі Аннан створив Групу високого рівня із загроз, викликів і змін (High-level Panel on Threats, Challenges and Change), яка у підсумковій доповіді визнала інформаційну інфраструктуру критично вразливим елементом глобальної безпеки та запропонувала комплексні реформи ООН. У 2004 році під егідою ООН було створено першу Групу урядових експертів з питань інформаційної безпеки (GGE), покликану дослідити існуючі та потенційні загрози у цифровому середовищі. Важливим етапом також стало проведення Всесвітнього саміту з питань інформаційного суспільства (WSIS, 2003-2005 рр.), де на міждержавному рівні вперше було сформульовано базові принципи глобального управління Інтернетом та кібербезпекою. Наприкінці 2005 року ООН створила Комісію з розбудови миру (UN Peacebuilding Commission), до порядку денного якої згодом увійшли питання протидії дезінформації та інформаційним провокаціям у постконфліктних регіонах. А створення у червні 2017 року Управління ООН з

боротьби з тероризмом (UNOCT) заклало основу для координації міжнародних зусиль у сфері протидії використанню Інтернету та цифрових технологій у терористичних цілях (кібертероризм).

Серед міжнародних організацій, які приділяють увагу безпеці, політика інформаційної безпеки НАТО реформована найефективніше. Організація створила центри в державах-членах як багатонаціональні установи для розвитку доктрини цифрової безпеки; удосконалення міждержавного співробітництва; впровадження теоретичних розробок у практику боротьби з цифровими загрозами; обмін досвідом захисту інформації між країнами-учасницями та країнами-партнерами. Наприклад, Центр кібербезпеки НАТО, що діє в Естонії, не входить до структури збройних сил НАТО, фінансується державами-спонсорами та державами-членами НАТО [43].

Інституціоналізація безпекового напряму на рівні ЄС розпочалася зі створення у 2004 році Європейського агентства з мережевої та інформаційної безпеки (ENISA). Надалі, зважаючи на залежність кібербезпеки від ефективності міждержавної координованої протидії злочинності, у 2013 році в структурі Європолу було утворено Європейський центр боротьби з кіберзлочинністю (EC3). Важливу роль у зміцненні кібербезпеки, безпеки інформаційно-комунікаційних технологій відіграє ОБСЄ, працюючи над зниженням ризиків виникнення конфліктів між державами в результаті використання інформаційних технологій [43].

Реалізація політики інформаційної безпеки міжнародних організацій передбачає тісну співпрацю з регіональними інституціями, профільними відомствами та урядами держав на відповідних рівнях комунікації.

Відчуваючи появу нових загроз, пов’язаних із інформатизацією та цифровізацією суспільного життя, більшість країн світу почала створювати численні правоохоронні та військові підрозділи, призначені для боротьби з цифровими загрозами. У системі публічного управління розпочався процес розбудови інституційного забезпечення національної безпеки.

Про це свідчить, зокрема, зарубіжний досвід: держави, які ефективно забезпечують захист національних інтересів в інформаційній сфері, створили

розвинені системи національної інформаційної безпеки. У більшості провідних країн світу вони будуються виключно на засадах та принципах системного підходу, а відтак мають чітку структуру, елементи якої наділені конкретними функціональними обов'язками та гармонійно взаємодіють між собою. Сформовані системи інформаційної безпеки вирізняються низкою спільних ключових ознак: ієрархічною побудовою; здійсненням управління та координації на найвищому державному рівні, із створенням відповідного керівного органу; чіткою міжвідомчою взаємодією суб'єктів, а також залученням різноманітних засобів масової інформації для реалізації державної інформаційної політики [55]. Як правило, загальне керівництво системою здійснюється вищим керівництвом виконавчої влади через відповідний робочий орган, який розробляє державну інформаційну політику та координує діяльність її складових. Останні представлені підсистемами інформаційної безпеки у складі ключових державних структур (зокрема Міністерства оборони, Міністерства внутрішніх справ та інших відомств), що безпосередньо виконують функції виявлення, аналізу та протидії інформаційним загрозам. Центральному робочому органу в системі інформаційної безпеки надають повноваження вищого міжвідомчого органу управління з правом безпосереднього керівництва всіма її суб'єктами. Крім цього, на нього покладається виконання інших стратегічних завдань, зокрема: аналіз геополітичної та воєнно-політичної обстановки; підготовка пропозицій щодо врегулювання проблем у сфері інформаційної безпеки та розробка ключових керівних документів; визначення потреб у технічних засобах інформаційної боротьби та матеріальних ресурсах, а також забезпечення міжнародного співробітництва у цій галузі [55].

Однак організаційна архітектура – органи публічного управління та установи, які запобігають безпековим загрозам, – становить лише частину інституційного забезпечення інформаційної безпеки. Воно охоплює також комплекс відносин, принципів, процедур, цінностей і функцій, якими керуються ці суб'єкти у своїй діяльності.

Так, основними принципами інституційного забезпечення інформаційної безпеки є системність, розподіл і розмежування функцій, простота структури,

гнучкість, адаптивність, трансформаційність, стійкість, безперервність функціонування, превентивність [55]. До цього переліку варто додати також принцип легітимності, тобто визнання суспільством права даного інституту встановлювати обов'язкові правила гри, застосовувати санкції, контролювати і навіть карати.

Принцип системності передбачає врахування сукупності взаємопов'язаних, взаємодіючих і динамічних елементів, умов і чинників, необхідних для розуміння і розв'язання проблем забезпечення інформаційної безпеки. При цьому елементи системи мають постійно взаємодіяти між собою в межах єдиної системи відносин, яка може бути ієрархічною, централізованою або передбачати децентралізацію із делегуванням відповідних повноважень периферійним органам.

Принцип розподілу та розмежування функцій вимагає чіткого закріплення повноважень за кожним елементом системи відповідно до його призначення, що дозволяє уникнути дублювання функцій та однозначно визначити межі його відповідальності.

Принцип простоти структури вимагає наявності лише тих компонентів, які є необхідними для її ефективного функціонування з урахуванням вимог надійності та перспективного розвитку.

Принцип гнучкості за умови жорсткого централізованого управління силами і засобами щодо планування та протидії інформаційним загрозам передбачає делегування частини повноважень підпорядкованим та взаємодіючим структурам з окремих питань контролю інформаційного простору та моніторингу негативного інформаційного впливу. В окремих питаннях, наприклад, технічного захисту інформації, можливий перехід до повного децентралізованого управління. Тобто вибір моделі управління буде залежати від конкретних умов та інформаційних загроз національній безпеці [55]. Такий розподіл повноважень дозволяє суттєво спростити й прискорити діяльність суб'єктів, які не потребують тотального контролю з боку вищої інстанції. Водночас державне управління має неухильно спостерігати та контролювати різнопланові заходи забезпечення інформаційної безпеки, координувати

взаємодію між залученими державними та недержавними установами, узгоджувати напрями, зміст, тези та аргументи інформаційного впливу, залучати ресурси державних видавництв, друкарень, теле- та радіокомпаній тощо [55].

Адаптивність та трансформативність системи полягають у можливості її пристосування до змін зовнішніх і внутрішніх чинників, які впливають на безпеку інформаційного простору, до умов невизначеності сучасного світу, а також до новітніх викликів і загроз без порушення функціонування та зниження її ефективності. У відповідь на безпекові виклики система має володіти потенціалом структурно-функціональної перебудови, охоплюючи спроможність до інституційного новоутворення. Зокрема, інтенсивна цифровізація суспільних процесів та зростання кіберзагроз вимагають формування додаткових управлінських сегментів, яскравим прикладом чого є становлення інституту кіберзахисту. Водночас збереження базових характеристик та ефективності діяльності системи в умовах деструктивних впливів є безпосереднім проявом принципу її стійкості (резильєнтності).

Безперервність функціонування полягає в організації системою такого режиму роботи всіх складових і підсистем, за якого не допускаються перерви як суб'єктивного, так й об'єктивного характеру. При цьому має бути забезпечена постійна керованість процесами, які циркулюють у системі, організаційно-адміністративна і ресурсна підтримка роботи складових структур [55].

Принцип превентивності вимагає фокусування на ранньому виявленні й аналізі ознак безпекових загроз, а також на ухваленні упереджувальних управлінських рішень. Своєчасна ідентифікація загрози національній безпеці в інформаційній сфері забезпечує її нівелювання та мінімізує негативні наслідки для суспільства й держави.

Основними функціями системи інституційного забезпечення інформаційної безпеки є управлінська, аналітична, прогностична, контрольна та освітньо-наукова. Ця функціональна п'ятірка відображає сутність, засади та цільову спрямованість діяльності всієї системи. Управлінська функція полягає у безпосередньому виробленні, координації та реалізації державної інформаційної політики органами публічної влади, яка створює нормативно-правову базу,

визначає елементи системи, наділяє їх повноваженнями та координує їхню діяльність. Для реалізації аналітичної функції системи доцільно сформувати такі її інституційні елементи, які б здійснювали систематичне дослідження інформаційних загроз, оцінювали стан інформаційної безпеки, визначали рівень уразливості критичної інфраструктури й готували обґрунтовані рекомендації для органів публічної влади з метою ухвалення ними управлінських рішень. Аналітична функція тісно пов'язана з прогностичною, адже саме якісний стратегічний прогноз та вчасні превентивні заходи забезпечують високу ефективність інформаційної політики. Контрольна функція системи інституційного забезпечення інформаційної безпеки полягає в системному моніторингу діяльності її суб'єктів та оцінюванні результативності вжитих заходів. Вона передбачає здійснення постійного контролю за виконанням складовими елементами системи покладених на них завдань і функцій за призначенням, комплексне оцінювання ефективності заходів із захисту інформаційного простору й протидії загрозам, а також перевірку повноти та раціональності ресурсного (матеріально-технічного, фінансового й кадрового) забезпечення функціонування всіх її ланок. Освітньо-наукова функція системи спрямована на підготовку висококваліфікованих фахівців і забезпечення наукового підґрунтя для сфери інформаційної безпеки. Вона охоплює вдосконалення та розбудову сучасної системи фахової підготовки й підвищення кваліфікації кадрів, а також організацію та проведення фундаментальних і прикладних наукових досліджень із актуальних проблем протидії інформаційним загрозам.

Інституційний аспект регулювання інформаційної безпеки передбачає не лише формування її засад, забезпечення ефективності функціонування системи, але й створення дієвої системи взаємодії та співпраці між різними органами влади, структурами публічного управління, правоохоронними організаціями, представниками бізнес-середовища та інститутами громадянського суспільства. Такий підхід зумовлено тим, що держава фізично не здатна самостійно контролювати весь обсяг інформаційних потоків і потребує синергії з неурядовими акторами [22], тому тільки шляхом гармонійної співпраці всіх

сторін можна створити сильну та стійку систему інформаційної безпеки [11].

Питання виокремлення суб'єктів, уповноважених забезпечувати інформаційну безпеку, має як теоретичне, так і практичне значення [121]. Сучасна архітектура інституційного забезпечення державного регулювання інформаційної безпеки України охоплює низку уповноважених суб'єктів, на які покладено обов'язки формування інформаційної та безпекової політики, її реалізації та контролю. Науковці визначають їх, аналізуючи характер їх впливу на політику держави у зазначеній сфері [74]. До таких суб'єктів належать, по-перше, органи виконавчої влади, і, по-друге, система органів спеціального призначення, що забезпечують національну, інформаційну та кібербезпеку.

Потрібно зауважити, що в епоху гібридних цивілізаційних викликів питання національної та інформаційної безпеки виходять на перший план та стають пріоритетними напрямами діяльності кожного з міністерств сучасної системи державного управління. Жодне міністерство (орган виконавчої влади) не функціонує відірвано від безпекового контексту, оскільки гібридна агресія здійснюється одночасно у військовому, цифровому, когнітивному, економічному, енергетичному та соціальному вимірах.

Як було зазначено вище, система інформаційної безпеки вирізняється своєю ієрархічною побудовою, а отже на основі повного переліку Міністерств можна побудувати цілісну ієрархію суб'єктів забезпечення інформаційної безпеки, розташувавши органи виконавчої влади за рівнями значимості та функціональним призначенням. Причому, на основі функціонального аналізу було встановлено, що таких рівнів буде сім: стратегічний; оперативно-силовий; технологічно-інфраструктурний; зовнішній; рівень ресурсної, макроекономічної та екологічної безпеки; рівень соціально-демографічної стійкості; гуманітарно-освітній та когнітивний рівень (рис. 2.4).

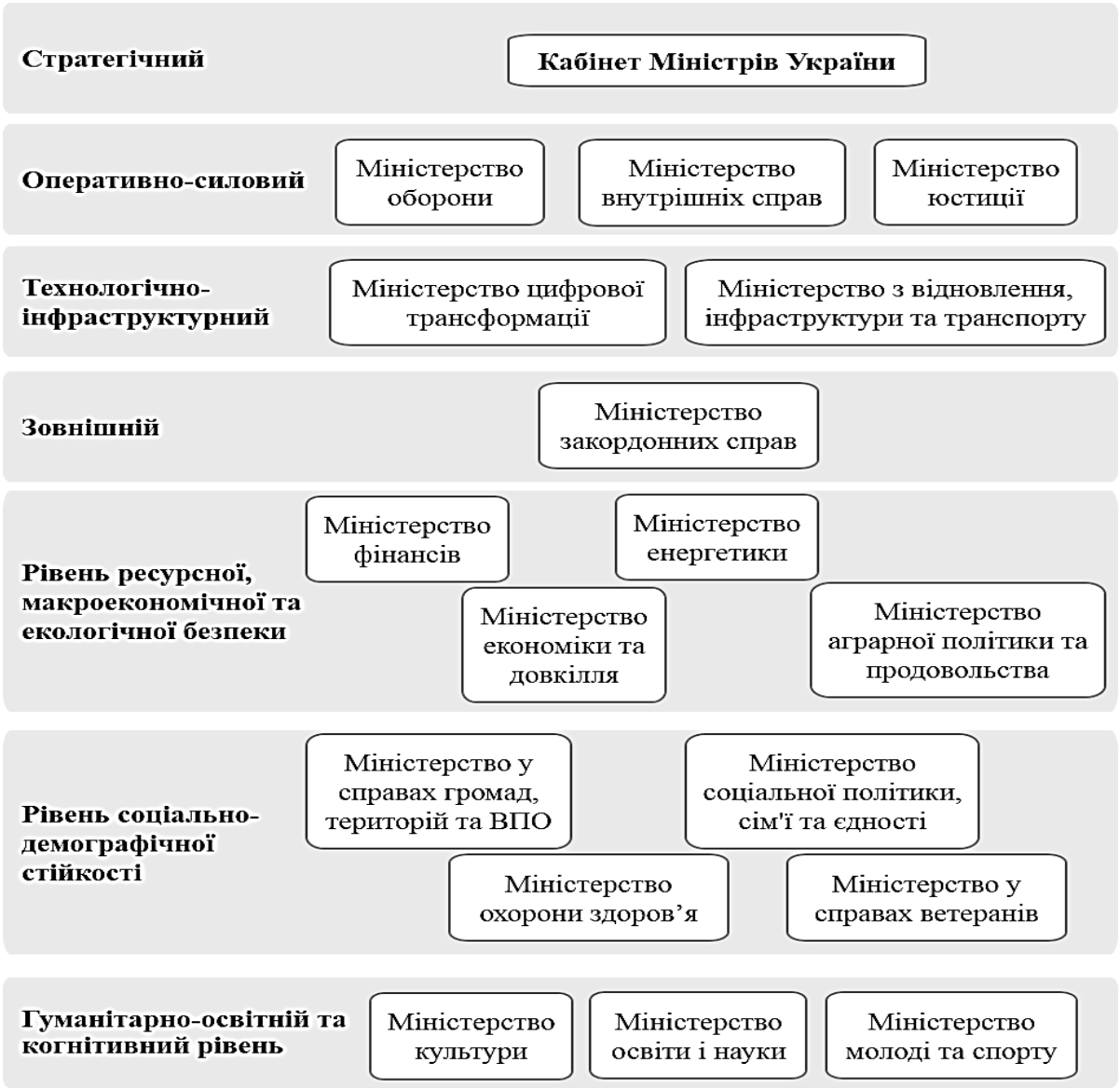

Рис. 2.4. Рівні ієрархії суб'єктів забезпечення інформаційної безпеки

Джерело: створено автором на основі [69]

Крім того, варто зазначити повноваження кожного з суб'єктів системи інституційного забезпечення інформаційної безпеки (Додаток В). Аналіз повноважень цивільних міністерств України дозволяє зробити висновок про те, що їхня роль охоплює не лише нормотворчість та адміністрування, а й забезпечення стійкості критичної інфраструктури, захист національних реєстрів, просування кібердипломатії та виховання цифрової культури громадян. Інституційна спроможність та кіберзрілість несилових міністерств є безпосередньою передумовою загальної суверенності та національної безпеки держави.

В умовах цивілізаційної нестійкості кожне міністерство відповідає за певний сектор інформаційної та національної безпеки. Це можна пояснити тим, що в інформаційному суспільстві кожний виконавчий орган має доступ до критичної інформації у сфері своєї компетенції. Ця інформація повинна бути захищеною та ефективно використовуватися для забезпечення системної резильєнтності держави, своєчасного виявлення деструктивних інформаційно-психологічних впливів і мінімізації загроз у відповідній галузі. У такому контексті цивільні (несилові) міністерства перетворюються з пасивних споживачів безпеки на активних суб'єктів захисту критичної інфраструктури, інформаційного суверенітету та функціональної стійкості держави. Особливу роль вони відіграють у питаннях кібербезпеки та кіберстійкості, оскільки транспонують загальнодержавні стандарти кібербезпеки в конкретні інструкції, регламенти та протоколи для підприємств, установ та організацій відповідного сектору економіки та суспільного життя, виступають галузевими регуляторами кіберстійкості.

Унікальне проміжне місце між цивільним регулюванням та стратегічним технологічним забезпеченням інформаційної безпеки займає Міністерство цифрової трансформації України [60]. Команда Міністерства відіграє ключову роль у протидії кібератакам та хакерським загрозам в умовах повномасштабної війни, реалізуючи низку стратегічних цифрових та інформаційно-безпекових ініціатив. Одним із важливих напрямів цієї діяльності стала цифрова блокада російської федерації, результатом якої стало припинення роботи на ринку агресора міжнародних технологічних компаній. Паралельно було сформовано ІТ-армію України, яка об'єднала понад 250 тисяч добровольців з усього світу та успішно здійснює системні атаки на цифрові ресурси ворога [33]. Ефективним інструментом цивільного сприяння безпеці виступає чат-бот «єВорог», через який передаються дані про пересування окупантів, воєнні злочини, колабораціонізм та мінну небезпеку, що сприяє успішному виконанню низки операцій Збройними Силами України. Крім того, використання алгоритмів штучного інтелекту для ідентифікації воєнних злочинців, а також застосування інструментів соціальної інженерії дозволяють ефективно знижувати морально-

психологічний потенціал ворога. Комплексна реалізація зазначених ініціатив забезпечує надійний захист вітчизняного інформаційного простору, виступаючи важливим чинником зміцнення національної безпеки України.

Масштабна цифрова трансформація, що реалізується в Україні з 2019 року за принципом digital first, виступає не лише драйвером економічної ефективності, а й критичним чинником зміцнення національної та інформаційної безпеки. Ліквідація корупційних ризиків з економічним ефектом у понад 16,3 млрд грн, автоматизація публічних послуг через застосунок «Дія» та цифровізація ключових державних реєстрів суттєво підвищують кіберстійкість та інституційну спроможність держави в умовах гібридної агресії. Водночас перехід від стандартної цифровізації сервісів до концепції TechChangers у трансформації оборонного сектору демонструє якісно новий рівень взаємодії суб'єктів безпекового сектору. Створення інноваційного кластеру оборонних технологій «Brave1» забезпечує горизонтальну інтеграцію між Збройними Силами України, органами публічної влади та приватними розробниками (Defense-Tech), що принципово прискорює процедури кодифікації розробок та їхню імплементацію на фронті. В інформаційній та військово-технічній сферах цей підхід реалізується шляхом впровадження мережецентричних цифрових рішень для автоматизації процесів комплектування, військової логістики та ухвалення оперативних управлінських рішень на основі штучного інтелекту, розбудови систем кібер- та радіоелектронної боротьби, засобів малого ППО й технологій deepstrike, спрямованих на нейтралізацію воєнного та критично-інфраструктурного потенціалу агресора, а також зміцнення стратегічних комунікацій і суб'єктності України у глобальному інформаційному просторі через цифрову фандрейзингову та медійну платформу United24 [60].

Розширюючи межі публічного управління поза контекст центральних органів влади, варто підкреслити критичну роль органів місцевого самоврядування як суб'єктів оперування критичними даними та комунальними активами. Механізм державного регулювання має забезпечити цілісність безпекового контуру на всіх рівнях публічного врядування, запобігаючи ризикам, коли вразливість локальної інфраструктури громади стає каналом

масштабної атаки на загальнодержавні реєстри [22].

До системи інституційного забезпечення інформаційної безпеки входять також органи спеціального призначення, які наділені виключними повноваженнями щодо виявлення, запобігання та нейтралізації зовнішніх і внутрішніх загроз в інформаційній та кіберсфері, а також забезпечення захисту державної таємниці й критичної інформаційної інфраструктури. Зокрема, такі суб'єкти, як Служба безпеки України, Державна служба спеціального зв'язку та захисту інформації України й підрозділи Кіберполіції, утворюють сильний силовий та технологічний каркас, який інтегрується з галузевими регламентами цивільних міністерств для створення цілісної системи національної кіберстійкості.

Головним координатором у безпековій сфері виступає Рада національної безпеки і оборони України (РНБО) [106]. Це постійно діючий конституційний колегіальний орган з питань координації та контролю діяльності органів виконавчої влади у сфері національної безпеки і оборони, створений Указом Президента України від 30 серпня 1996 р. №772 відповідно до статті 107 Конституції України.

Передумовою створення сучасного РНБО було існування протягом 1991-1996 років двох специфічних суб'єктів: Ради оборони України та Ради національної безпеки України. Згідно з Положенням про Раду оборони України, вона мала статус вищого державного колегіального органу керівництва безпековими та оборонними питаннями та була створена з метою захисту суверенітету, конституційного ладу, територіальної цілісності та недоторканності України, вироблення стратегії й постійного вдосконалення безпекової політики, всебічної наукової оцінки характеру воєнної загрози, а також забезпечення ефективного контролю за виконанням інститутами держави завдань із підтримання її обороноздатності. Натомість Рада національної безпеки України діяла як консультативно-дорадчий інститут при Президентові України з підготовки стратегічних рішень у сфері захисту національних інтересів і забезпечення національної безпеки [106].

У Конституції України зазначається, що «Рада національної безпеки і

оборони України є координаційним органом з питань національної безпеки і оборони при Президентові України. Рада національної безпеки і оборони України координує і контролює діяльність органів виконавчої влади у сфері національної безпеки і оборони. Головою Ради національної безпеки і оборони України є Президент України» [44, 106].

Президент України формує персональний склад Ради національної безпеки і оборони України, до якого за посадою входять Прем'єр-міністр, міністри оборони, закордонних і внутрішніх справ, а також Голова Служби безпеки України. Окрім них, участь у засіданнях Ради може брати Голова Верховної Ради.

Головні завдання та напрями роботи Ради національної безпеки і оборони України визначено на законодавчому рівні [98]. Пріоритетними серед них є формування стратегії національної та інформаційної безпеки, визначення орієнтирів протидії гібридним загрозам, координація виконання прийнятих рішень, здійснення поточного контролю діяльності органів виконавчої влади у сфері національної безпеки і оборони, зокрема в інформаційній сфері. Для забезпечення якісного аналізу інформації РНБО залучає посадових осіб і фахівців органів державної влади, державних установ, наукових закладів, а також підприємств та організацій усіх форм власності [98].

Робочим органом Ради національної безпеки та оборони України, утвореним відповідно до її рішення від 11 березня 2021 року «Про створення Центру протидії дезінформації» [103], є Центр протидії дезінформації [127]. До основних завдань цього спеціального органу віднесено: системний аналіз та моніторинг подій в інформаційному просторі, оцінку стану інформаційної безпеки та присутності України у світовому медіапросторі; ідентифікацію й вивчення поточних і прогнозованих інформаційних загроз та чинників, що впливають на їх формування; нейтралізацію дезінформаційних кампаній, деструктивних інформаційних впливів і пропаганди, а також запобігання спробам маніпулювання громадською думкою. Крім того, Центр бере участь у розбудові та координації національної системи стратегічних комунікацій і створенні інтегрованої системи оперативного реагування на інформаційні

виклики та загрози [78].

При Раді національної безпеки і оборони України створено також Національний координаційний центр кібербезпеки [64], який забезпечує комплексний аналіз стану національної системи кібербезпеки, готовності суб'єктів забезпечення кібербезпеки до виконання завдань з питань протидії кіберзагрозам, а також рівня виконання законодавчих вимог щодо кіберзахисту державних електронних інформаційних ресурсів та об'єктів критичної інформаційної інфраструктури. Центр здійснює систематичний моніторинг і виявлення потенційних та реальних кіберзагроз, здійснює прогнозування їхнього розвитку, узагальнює міжнародний досвід і забезпечує оперативне інформаційно-аналітичне інформування РНБО України. Він також бере участь в організації та проведенні міжнародних і міжвідомчих кібернавчань, розробляє методичні рекомендації та стандарти у сфері кіберзахисту [81].

Державним органом спеціального призначення з правоохоронними функціями, який забезпечує державну безпеку України, є Служба безпеки України (СБУ) [102]. У сфері інформаційної безпеки СБУ здійснює оперативно-розшукові та контррозвідувальні заходи, спрямовані на виявлення і нейтралізацію інформаційних диверсій, деструктивних пропагандистських впливів та кіберзлочинності, визначає та захищає державну таємницю, забезпечує контррозвідку в інформаційній сфері. Ця діяльність покликана захистити державний суверенітет, конституційний лад, територіальну цілісність, науково-технічний і оборонний потенціал України, а також права громадян від розвідувально-підривної діяльності іноземних спецслужб та забезпечити надійну охорону державної таємниці [102].

Забезпечення захисту інформаційних систем, кіберстійкості критичної інфраструктури, створення державних стандартів криптографічного та технічного захисту інформації покладено на Державну службу спеціального зв'язку та захисту інформації України (Держспецзв'язку) [83; 15]. Вона є центральним органом виконавчої влади зі спеціальним статусом, який забезпечує функціонування і розвиток державної системи урядового зв'язку, Національної системи конфіденційного зв'язку, формування та реалізацію

державної політики у сферах, визначених законом, і спрямовує свою діяльність на забезпечення національної безпеки України від зовнішніх і внутрішніх загроз та є складовою сектору безпеки і оборони України [83]. Інституційна структура Держспецзв'язку охоплює мережу спеціалізованих закладів, установ та підрозділів, які забезпечують виконання покладених на неї завдань. До їхнього складу, зокрема, входять Державний центр кіберзахисту, Національний центр оперативно-технічного управління мережами телекомунікацій України, Державний науково-дослідний інститут технологій кібербезпеки та захисту інформації, Інститут спеціального зв'язку та захисту інформації Національного технічного університету України «Київський політехнічний інститут імені Ігоря Сікорського», а також Галузевий державний архів, Департамент забезпечення, Управління охорони та Медичний центр Держспецзв'язку [15].

Керівним органом системи Держспецзв'язку є Адміністрація Державної служби спеціального зв'язку та захисту інформації України, до складу якої входять більше 20 департаментів, управлінь та відділів, які виконують завдання щодо регулювання інформаційної безпеки. Інституційне ядро Адміністрації сформоване навколо трьох ключових напрямів: захисту інформації та технічного захисту інформації [88]; кіберзахисту та оперативної протидії інцидентам [17]; а також нормативно-методичного регулювання. Сформована багаторівнева архітектура Адміністрації Держспецзв'язку забезпечує повноцінне регулювання, координацію та нормативно-методичний супровід усіх компонентів національної інформаційної безпеки.

До сфери управління Держспецзв'язку належить також Національний центр оперативно-технічного управління мережами телекомунікацій (НЦУ), утворений Урядом у 2019 році [105] для централізованого регулювання та забезпечення стійкості функціонування електронних комунікаційних мереж загального користування. Він організовує виконання рішень щодо блокування небезпечних інтернет-ресурсів, доменів, IP-адрес і підозрілих каналів на підставі звернень уповноважених державних органів, реалізуючи заходи протидії загрозам національній безпеці в інформаційному просторі та кіберпросторі. За офіційними даними, протягом трьох років повномасштабної війни росії проти

України заблоковано понад 50 тисяч інтернет-ресурсів, афілійованих із державою-агресором або спрямованих на підрив основ національної безпеки, 390 підсанкційних доменів, понад 40 тисяч онлайн-сервісів неліцензованих азартних ігор, а також майже 7,5 тисяч фішингових ресурсів, задіяних у кібератаках на українську інформаційну інфраструктуру [138].

Важливим елементом технологічного каркасу інституційного забезпечення інформаційної безпеки є Національний центр резервування державних інформаційних ресурсів (підпорядкований Держспецзв'язку). Його функціональне призначення полягає у забезпеченні надійності та безперебійності функціонування державних інформаційних систем, збереженні державних електронних ресурсів, а також проведенні резервного копіювання критичних даних державних органів, військових формувань і суб'єктів критичної інфраструктури [99]. Це спеціальна державна хмарна інфраструктура, створена для захисту, зберігання, адміністрування та створення резервних копій важливих електронних даних державних органів України [65].

Доцільно наголосити також, що функціонування системи інформаційної безпеки не обмежується центральним рівнем державного управління. На регіональному рівні її реалізацію гарантують територіальні органи (підрозділи) Держспецзв'язку, які забезпечують органи державної влади урядовим зв'язком, впроваджують сервіси кіберзахисту, а також реалізують державну політику у сферах криптографічного та технічного захисту інформації в областях.

Захист українського інформаційного простору від пропагандистської аудіовізуальної продукції держави-агресора, розповсюдження українського телерадіомовлення на тимчасово окупованих територіях України забезпечує Національна рада України з питань телебачення і радіомовлення – конституційний, постійний колегіальний, наглядовий та регуляційний державний орган [128].

Крім того, до інституційної системи забезпечення інформаційної безпеки держави можуть бути віднесені наукові та науково-дослідні установи під час забезпечення науково-аналітичного та експертного супроводження процесу формування та реалізації державної інформаційної політики [128].

Науково-технологічним ядром системи є Державний науково-дослідний інститут технологій кібербезпеки та захисту інформації, який перебуває під безпосереднім управлінням Адміністрації Держспецзв'язку [16]. Інститут здійснює фундаментальні та прикладні дослідження, розробку, виготовлення й упровадження засобів криптографічного та технічного захисту інформації, а також спеціального телекомунікаційного обладнання. Крім того, установа проводить сертифікаційні випробування, науково-технічні експертизи проєктів у сфері захисту даних та забезпечує фахову оцінку відповідних технологічних рішень.

Усі ці суб'єкти взаємодіють у межах єдиного безпекового простору, формуючи багаторівневу систему захисту інформації. У цілому система уповноважених суб'єктів складається з державних інституцій, які є регулятивною та безпековою основою розвитку інформаційного суспільства [121].

2.3. Механізми державного регулювання інформаційної безпеки в умовах цифровізації, глобалізації та розвитку інформаційного суспільства

Аналіз наукових праць у галузі публічного управління свідчить про відсутність єдиного підходу до розуміння сутності категорії «механізм державного регулювання» [54; 57; 72; 123; 136; 137].

У науці про публічне управління категорія «механізм» виступає універсальним інструментом для опису того, як державні рішення перетворюються на практичні суспільні результати, пояснює процесуальний характер реалізації державної політики та трансформації управлінських імпульсів у суспільні зміни. Це поняття дозволяє описати єдину функціональну систему, яка інтегрує норми, ресурси, процедури та взаємодію між суб'єктами й об'єктами владних повноважень.

Розрізняють поняття «механізми державного управління» та «механізми державного регулювання». Так, під механізмами державного управління у найширшому розумінні розуміють «способи розв'язання суперечностей явища

чи процесу в державному управлінні, послідовна реалізація дій, які базуються на основоположних принципах, цільовій орієнтації, функціональній діяльності з використанням відповідних їй форм і методів управління» [32]. Структурний склад і динаміка функціонування таких механізмів обумовлюються стратегічною метою, наявними ресурсами, специфікою ситуації та обраними інструментами впливу. До їхніх обов'язкових компонентів належать цілі, принципи, функції, методи, інформаційне забезпечення та управлінські технології, реалізовані через правові, організаційні, економічні, соціальні чи комплексні засоби. У цілому механізми управління можна охарактеризувати як «об'єкти, процеси, явища, які забезпечують процес управління» [32].

Державне регулювання, як стверджує В. Авер'янов, створює умови для діяльності суб'єктів та об'єктів управління в напрямі бажаному для держави [38]. Загалом, державне регулювання розуміють як функцію державного управління; як засіб керівного впливу; як цілеспрямовану діяльність уповноважених державних органів, їх посадових осіб та окремих недержавних утворень, що полягає у здійсненні комплексних заходів, спрямованих на практичну реалізацію державної політики [38].

Механізми регулювання – це способи координації та синхронізації процесів, які відбуваються у визначеній сфері суспільства з метою досягнення стратегічно окресленого результату. Під механізмом державного регулювання слід розуміти сукупність послідовних інструментів, функцій та процедур цілеспрямованого впливу на організаційну систему, ефективність якого визначається через порівняння досягнутих результатів із кількісними та якісними індикаторами виконання програмно-цільових завдань [82]. Складовими елементами системи державного регулювання є механізми взаємодії державних органів та відомств, підбір кадрового персоналу, адміністративні та політичні процеси органах публічної влади. Виступаючи частиною системи управління, механізм регулювання є сукупністю функцій, етапів і послідовних процедур регуляторного впливу на організаційну систему, результативність якого вимірюється показниками рівня досягнення управлінських цілей [82].

Державне регулювання сфери інформаційної безпеки виступає базовим елементом забезпечення загальної національної безпеки, державного суверенітету та кіберстійкості. Механізми державного регулювання формують нормативно-правову основу інформаційної безпеки, визначають технічні стандарти, встановлюють інституційні вимоги, у межах яких функціонують суб'єкти державних і приватних секторів.

Беручи за основу дослідження В. Приходька [82], комплексний механізм державного регулювання інформаційної безпеки в умовах цифровізації, глобалізації та розвитку інформаційного суспільства має системний характер та складається з взаємопов'язаних компонентів (рис. 2.5).

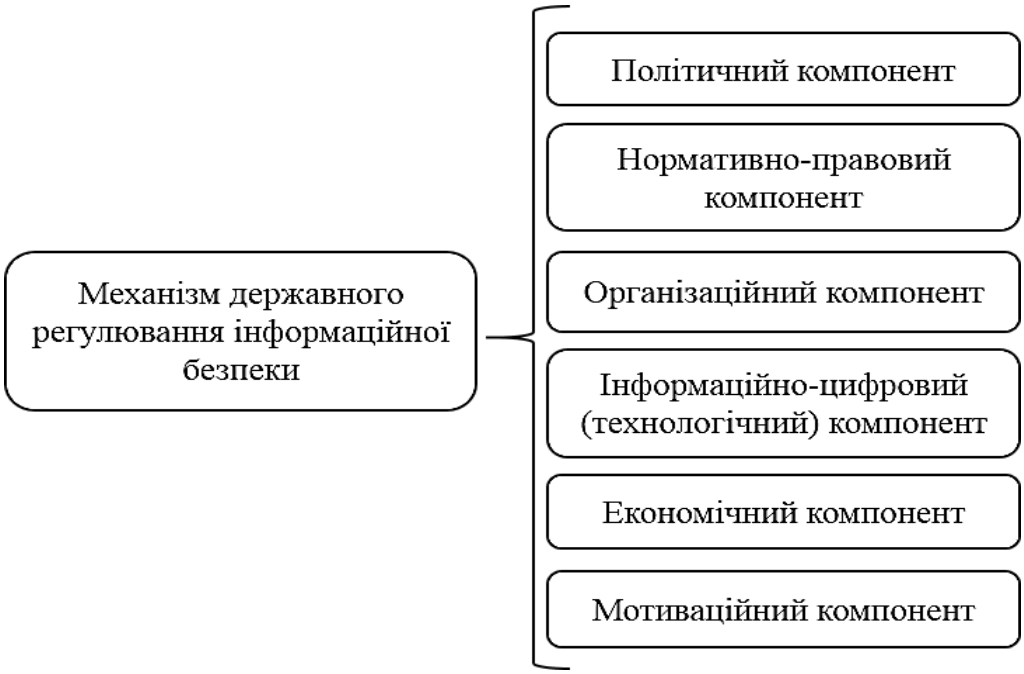

Рис. 2.5. Комплексний механізм державного регулювання інформаційної безпеки в умовах цифровізації, глобалізації та розвитку інформаційного суспільства

Джерело: створено автором на основі [82]

Політичний компонент механізму державного регулювання інформаційної безпеки виступає фундаментальною основою всієї системи державного управління у цій сфері, оскільки саме він задає стратегічні орієнтири, концептуальну та цільову спрямованість державної політики у цифровому просторі. Він виступає сполучною ланкою між вищими цінностями державного

суверенітету, національної безпеки та демократичного розвитку держави. Першочергове значення при цьому має механізм акумуляції та вираження політичної волі, який забезпечує підтримку системних реформ у сфері кіберзахисту, гарантує належне ресурсно-фінансове забезпечення та визначає пріоритетність цифрової безпеки в загальній системі національних інтересів. Практичне втілення цієї волі здійснюється через механізм стратегічного планування та цілепокладання, який полягає у розробці та регулярному оновленні засадничих документів, які формують нормативно-ідеологічний базис, встановлюють концептуальні пріоритети для всіх інших складових регуляторного механізму – нормативно-правової, організаційної та технічної. Політичний компонент механізму регулювання виявляє себе й у зовнішньополітичному вимірі, коли застосовуються механізми мережевої кібердипломатії та міжнародної інтеграції, спрямовані на поглиблення співпраці з ключовими геополітичними партнерами. Він передбачає імплементацію передових стандартів НАТО та ЄС, повноцінну участь держави у спільних системах колективної інформаційної та кібербезпеки, розбудову коаліцій протидії гібридним загрозам і транскордонній кіберзлочинності, а також активне відстоювання національних інтересів на глобальних міжнародних майданчиках.

Нарешті, демократичний вимір даного компонента забезпечується через механізм балансування та дотримання суспільних гарантій. Його функціональне призначення полягає у постійній узгодженості між вимогами суворого державного контролю та кіберзахисту критичних інституцій з одного боку, і збереженням фундаментальних прав і свобод громадян – з іншого. Зокрема, зберігаються гарантії на свободу слова, приватність, захист персональних даних та безперешкодний доступ до інформації.

Нормативно-правовий компонент механізму державного регулювання інформаційної безпеки полягає у встановленні законних правил, норм, регулятивно-правових актів, стандартів і гарантій, що визначають межі допустимої поведінки суб’єктів. Нормативно-правове забезпечення державного регулювання інформаційної безпеки докладно проаналізовано у Розділі 2.1 даного дисертаційного дослідження.

Організаційний компонент механізму регулювання інформаційної безпеки визначає суб'єктну архітектуру, систему вертикальних і горизонтальних зв'язків, розподіл повноважень, інституційну спроможність та управлінські регламенти, які забезпечують практичну реалізацію державної політики у сфері інформаційної безпеки. Про інституційне забезпечення державного регулювання інформаційної безпеки йшлося у Розділі 2.2 даного дисертаційного дослідження, де докладно висвітлено суб'єктну конфігурацію та систему органів державного управління у цій сфері.

Водночас слід підкреслити, що організаційний компонент механізму регулювання інформаційної безпеки охоплює безпосередньо операційно-управлінські процеси, встановлює чіткі регламенти взаємодії, процедури координації та розподіл відповідальності між суб'єктами забезпечення інформаційного та кіберзахисту на операційному та тактичному рівнях. Його функціональна архітектура систематизується через п'ять обов'язкових елементів.

Першим елементом виступає механізм розподілу функцій та субординації, що забезпечує чітке розмежування сфер відповідальності між відомствами задля усунення дублювання повноважень. В українській практиці цей механізм реалізується через розмежування завдань тих державних інститутів, про які йшлося у Розділі 2.2. Важливою складовою цього механізму є також організація та підтримка мережі спеціалізованих команд реагування на комп'ютерні надзвичайні події під загальною координацією державного центру CERT-UA. CERT-UA – це Урядова команда реагування на комп'ютерні надзвичайні події, яка функціонує у структурі Державного центру кіберзахисту Державної служби спеціального зв'язку та захисту інформації України (Держспецзв'язку) [152]. Поєднуючи функції технічної аналітики, координаційного хабу та оперативної допомоги у кіберпросторі, CERT-UA забезпечує повний цикл інцидент-менеджменту – від первинного виявлення компрометації та збору цифрових доказів до поширення індикаторів компрометації і розробки практичних рекомендацій щодо нейтралізації загроз. У системі публічного управління CERT-UA виступає сполучною ланкою між державним сектором, операторами

критичної інфраструктури та міжнародними партнерами, забезпечуючи перехід від статичного захисту до динамічного обміну даними про загрози у режимі реального часу.

Другим елементом є механізм міжвідомчої, мережевої та міжнародної взаємодії, який вирівнює вертикальні та горизонтальні зв'язки у секторі безпеки. На стратегічному та оперативному рівнях його горизонтальну координацію забезпечує Національний координаційний центр кібербезпеки як робочий орган РНБО України. На рівні взаємодії з недержавним сектором функціонує механізм державно-приватного партнерства, що забезпечує залучення IT-компаній, етичних хакерів та аудиторських фірм до обміну інформацією про загрози, а також проведення спільних хакатонів і навчань. На міжнародному рівні цей механізм реалізується через інституційну інтеграцію до європейських і євроатлантичних безпекових структур, зокрема взаємодію з ENISA (European Union Agency for Cybersecurity – Агентство Європейського Союзу з питань кібербезпеки), NATO CCDCOE (NATO Cooperative Cyber Defence Centre of Excellence – Об'єднаний центр передових технологій з кібероборони НАТО), Europol (European Union Agency for Law Enforcement Cooperation – Агентство Європейського Союзу з питань співробітництва у сфері правоохоронної діяльності) та FBI (Federal Bureau of Investigation – Федеральне бюро розслідувань США).

Третім є механізм регламентації та стандартизації управлінських процедур, що переводить нормативні вимоги у площину щоденної управлінської практики. Він охоплює затвердження стандартних операційних процедур інцидент-менеджменту, які визначають алгоритм дій у разі виявлення кібератаки чи витоку даних. У кадровому вимірі цей механізм регламентує обов'язкове введення посади керівника з інформаційної безпеки (CISO) або створення окремих підрозділів інформаційної безпеки на об'єктах критичної інфраструктури та в органах влади. Контрольно-аудиторна складова даного механізму забезпечує порядок проведення планових і позапланових перевірок стану захищеності та атестації систем захисту інформації.

Четвертим виступає механізм ситуаційного управління та забезпечення

оперативної стійкості, розрахований на роботу в умовах активних кіберінцидентів. Його базовим інструментом є побудова цілодобових ситуаційних центрів моніторингу та реагування у режимі 24/7. Практичну реалізацію стійкості забезпечує впровадження механізму управління безперервністю діяльності, що передбачає розробку та регулярне оновлення планів функціонування організацій у разі надзвичайних ситуацій, часткової втрати зв'язку або руйнування інфраструктури.

П'ятим елементом є механізм кадрово-компетентнісного забезпечення та оцінки готовності, який спрямований на розвиток людського чинника. Його основою є систематичне проведення національних та міжвідомчих кібернавчань у форматі командно-штабних і технічних тренувань для перевірки реальної готовності суб'єктів до відбиття масштабних атак. Доповнює його механізм сертифікації та акредитації фахівців, що встановлює організаційно-методичні вимоги до підготовки та підтвердження кваліфікації спеціалістів з інформаційної безпеки для державних установ.

Усі зазначені механізми в умовах цивілізаційних загроз трансформуються на засадах адаптивного врядування. Це передбачає застосування механізму децентралізації прийняття оперативних рішень, який надає локальним підрозділам інформаційної безпеки повноваження автономно застосовувати заходи захисту під час атаки без тривалого бюрократичного погодження з центральним регулятором. Одночасно відбувається перехід від статичного формального контролю до механізму постійного автоматизованого моніторингу захищеності у режимі реального часу, а також розгортання механізму гнучкої координації в умовах кризи через створення оперативних міжвідомчих штабів для миттєвого обміну індикаторами компрометації.

Отже, організаційний компонент механізму регулювання інформаційної безпеки виступає інституційною та процесуальною основою забезпечення кіберстійкості держави, що визначає суб'єктну структуру регулювання, розподіл повноважень, регламенти міжвідомчої та державно-приватної взаємодії, а також процедури ситуаційного управління та оперативної координації заходів із захисту критичної інформаційної інфраструктури.

Інформаційно-цифровий (технологічний) компонент механізму державного регулювання інформаційної безпеки розкриває прикладну, інструментальну та програмно-апаратну основу функціонування всієї системи безпеки. Його функціональне призначення полягає у забезпеченні технологічної спроможності, оперативності, прозорості та безперервності процесів публічного управління в кіберпросторі через імплементацію сучасних програмно-технічних рішень та інформаційно-комунікаційних платформ. Практичне застосування даного компонента реалізується через систему взаємопов'язаних інструментальних напрямів. Першочергову роль відіграє механізм цифровізації та автоматизації управлінських процесів (e-governance), що забезпечує перехід від паперового та дискретного контролю до електронного урядування та захищеного цифрового документообігу. Складовою цього напряму є захист державних реєстрів, хмарних інфраструктур та сервісів надання публічних послуг, що гарантує цілісність, конфіденційність та доступність критичних даних.

Оперативне реагування на кіберзагрози забезпечується через механізм технічного моніторингу та ситуаційного управління, який базується на розгортанні мережі ситуаційних центрів, автоматизованому зборі телеметрії, аналізі системних подій у режимі реального часу та застосуванні інтелектуальних алгоритмів виявлення аномалій. Застосування прогресивних алгоритмів аналізу даних та автоматизованих скриптів прийняття рішень дозволяє мінімізувати час виявлення та ліквідації інцидентів, суттєво послаблюючи негативний вплив людського чинника під час гострих фаз кібератак.

Прозорість та демократичний контроль регуляторної діяльності реалізуються через механізм відкритих даних та публічного аудит-моніторингу, що передбачає публікацію машинно-зчитуваних даних про стан захищеності, регулярне оприлюднення результатів автоматизованого сканування вразливостей державних ресурсів, а також функціонування відкритих реєстрів об'єктів критичної інфраструктури.

Нарешті, базову стійкість технологічного контуру формує механізм

криптографічного, апаратно-програмного та периметрового захисту. Він охоплює використання надійних засобів криптографічного захисту інформації, побудову Комплексних систем захисту інформації та Систем управління інформаційною безпекою, впровадження технічних стандартів суворої автентифікації, а також розгортання сучасних програмно-технічних засобів захисту мереж, пристроїв та інформаційних потоків на всіх об'єктах критичної інфраструктури.

Економічний компонент державного регулювання інформаційної безпеки включає в себе механізми фінансово-бюджетного забезпечення та державного інвестування інформаційної сфери. Держава визначає відсоток бюджету, який має спрямовуватися виключно на заходи з інформаційної безпеки та кіберзахисту, фінансує об'єкти критичної інформаційної інфраструктури, надає цільові субсидії, дотації для модернізації захисту стратегічних об'єктів. Іншим механізмом державного регулювання інформаційної безпеки можна вважати економічну підтримку вітчизняних розробників засобів захисту інформації (криптографія, SOC, рішення на базі AI) через прозорі державні закупівлі, грантові програми та стартап-інкубатори. До механізмів економічного спрямування належать також запровадження пільгових ставок ПДВ, податку на прибуток або ЄСВ для підприємств, що розробляють вітчизняні засоби технічного захисту інформації або криптозахисту, забезпечують кібербезпеку критичної інфраструктури. Суб'єктам господарювання надається дозвіл списувати витрати на нові засоби захисту інформації (файрволи, системи SIEM/EDR) за прискореною процедурою. Також держава надає гарантії або часткову компенсацію відсоткових ставок за кредитами для підприємств, що працюють у сферах інформаційної безпеки та кіберзахисту. Органами державного управління створюються ринкові стимули до захисту таких підприємств. Крім сприяння розвитку та підтримки застосовуються також механізми санкціювання та встановлюється відповідальність за незабезпечення інформаційної безпеки. До таких санкцій належать штрафи за витік даних та недбалість за аналогією з європейським регламентом GDPR, де штрафи сягають до 20 млн євро або 4% від річного обороту.

Економічний компонент механізму регулювання інформаційної безпеки являє собою систему фінансово-кредитних, податкових, тарифних та ринкових важелів, за допомогою яких держава забезпечує акумуляцію ресурсів для захисту критичних інформаційних активів, формує економічну мотивацію суб'єктів господарювання до дотримання стандартів кібербезпеки та мінімізує потенційні матеріальні збитки від деструктивних інформаційно-технічних впливів.

Мотиваційний компонент механізму державного регулювання інформаційної безпеки визначає сукупність стимулів, важелів, цінностей та умов, які спонукають суб'єктів свідомо, систематично та ініціативно дотримуватися вимог кібербезпеки та формувати стійку культуру кібер- та інформаційної гігієни. Мотиваційний регуляторний вплив реалізується на трьох взаємопов'язаних рівнях: мікро-, мезо- та макро-. Мікро рівень – це рівень індивіда, окремого працівника, громадянина. Мезорівень охоплює окремі підприємства та організації сфери інформаційної безпеки. Макрорівень – це рівень суспільства та держави, охоплює питання інформаційної та кіберстійкості, національного суверенітету, цифрової та інформаційної культури, що неможливо без довіри до органів публічного управління.

Мотиваційні механізми можна поділити на стимулюючі (позитивні) та стримуючі (запобіжні). До позитивних механізмів належать надання сертифікатів безпеки, наприклад, ISO/IEC 27001, або атестату відповідності КСЗІ (Комплексна система захисту інформації). Це створює репутаційний капітал або бренд довіри компанії, бізнесу, операторів, стає маркером надійності та залучає клієнтів, партнерів та інвесторів.

ISO/IEC 27001 – міжнародний стандарт з інформаційної безпеки, що був створений Міжнародною організацією зі стандартизації (International Organization for Standardization (ISO)) та Міжнародною електротехнічною комісією (International Electrotechnical Commission (IEC)). Стандарт містить вимоги щодо інформаційної безпеки, описи найкращих світових практик у галузі управління нею. Основою цього стандарту безпеки є принципи конфіденційності, цілісності інформації та доступності даних. Цей стандарт в умовах зростання кіберзлочинності та постійної появи нових загроз допомагає

організаціям усвідомлювати ризики та превентивно виявляти та усувати слабкі місця, що сприяє підвищенню рівня кібербезпеки. Для будь-якого банку, дата-центру, ІТ-компанії чи онлайн-бізнесу, що працює з великими масивами даних клієнтів, сертифікат ISO/IEC 27001 є важливою ознакою того, що компанія приділяє особливу увагу безпеці та захисту даних [139].

Процедура державної експертизи у сфері технічного захисту інформації проводиться відповідно до «Положення про державну експертизу у сфері технічного захисту інформації» [89], затвердженого наказом Адміністрації Держспецзв'язку [9] та є національним інструментом підтвердження гарантій безпеки. Атестат відповідності КСЗІ підтверджує, що компанії можуть гарантувати своїм клієнтам захист інформації від несанкціонованого доступу, захист конфіденційної інформації, аудит та протоколювання дій користувачів, контроль за цілісністю даних та ін. [4].

Позитивним мотиваційним механізмом є й створення органами публічного управління рейтингів прозорості та рівня захищеності організацій. Прикладами таких рейтингів може бути «Рейтинг Кращих Компаній з Інформаційної Безпеки в Україні від Ukrainian Business Award» (2026) [108]. Державний центр кіберзахисту Держспецзв'язку проводить оцінку стану захищеності державних інформаційних ресурсів та сканування на предмет вразливості державних інформаційних ресурсів [71]. Адміністрацією Державної служби спеціального зв'язку та захисту інформації України розроблено «Критерії і показники оцінки стану захищеності об'єктів критичної інфраструктури» [53]. Така процедура є сукупністю заходів, спрямованих на виявлення загроз державним інформаційним ресурсам в інформаційних, комунікаційних та інформаційно-комунікаційних системах органів державної влади, органів місцевого самоврядування, військових формувань, підприємств, установ і організацій незалежно від форм власності та запобігання несанкціонованим діям щодо інформації [71] та полягає у дистанційному виявленні уразливих місць програмно-апаратних засобів, що забезпечують функціонування державних інформаційних ресурсів, розміщених в Інтернеті. Такими місцями можуть бути ті, використовуючи які зловмисник може порушити цілісність, доступність,

конфіденційність інформації або спостережність системи.

Позитивними мотиваційними механізмами можна вважати також впровадження програм визнання для системних адміністраторів, CISO та фахівців з інформаційної безпеки за завчасне виявлення вразливостей. Зокрема, таким інноваційним інструментом є Bug Bounty – програма пошуку вразливостей у програмному забезпеченні, мережах та інформаційних системах за винагороду, фінансове або репутаційне заохочення, за якою відбувається залучення незалежних фахівців із кібербезпеки – «етичних хакерів», білих капелюхів [200]. До мотиваційних механізмів належать також преміювання та просування фахівців з кібербезпеки по службі в державних органах.

Мотиваційні механізми на мікрорівні сприяють формуванню у індивіда почуття залученості та причетності до захисту національної безпеки. Кожен працівник, дотримуючись правил кібергігієни (створення складного паролю, протидія фішингу, MFA (Multi-Factor Authentication / Багатофакторна автентифікація)), відчуває, що саме він безпосередньо захищає державний реєстр чи критичний об’єкт інфраструктури від ворожих атак.

Симуляції фішингових атак (Phishing Simulations) та проведення раптових кібернавчань (Red Teaming) є мотиваційними механізмами, але вже запобіжного характеру. За їх допомогою працівники на практиці мають відчути вразливість систем та здолати ілюзії безпеки («це станеться не зі мною»). Симуляції виступають механізмом подолання когнітивних спотворень (ілюзії безпеки) та оцінки готовності.

Стримуючим мотиваційним механізмом виступають також чіткі посадові інструкції, де закріплена персональна відповідальності керівника установи чи CISO (Chief Information Security Officer / Керівник з інформаційної безпеки) за незабезпечення базових заходів захисту.

Страх втратити довіру клієнтів мотивує керівництво інвестувати в інформаційну безпеку краще, ніж погрози штрафів, а тому ще одним стримуючим мотиваційним механізмом буде законодавча вимога щодо обов’язкового публічного сповіщення про факт масового витоку даних.

Мотиваційний компонент механізму регулювання інформаційної безпеки

є системою соціально-психологічних, кадрових, репутаційних та морально-етичних чинників і стимулів, спрямованих на формування стійкої кіберкультури, свідоме дотримання вимог кібергігієни суб'єктами публічного та приватного секторів, а також на мінімізацію ризиків, зумовлених людським чинником у сфері захисту критичної інформаційної інфраструктури та державних ресурсів.

Комплексний механізм державного регулювання інформаційної безпеки зображено на рис. 2.6.

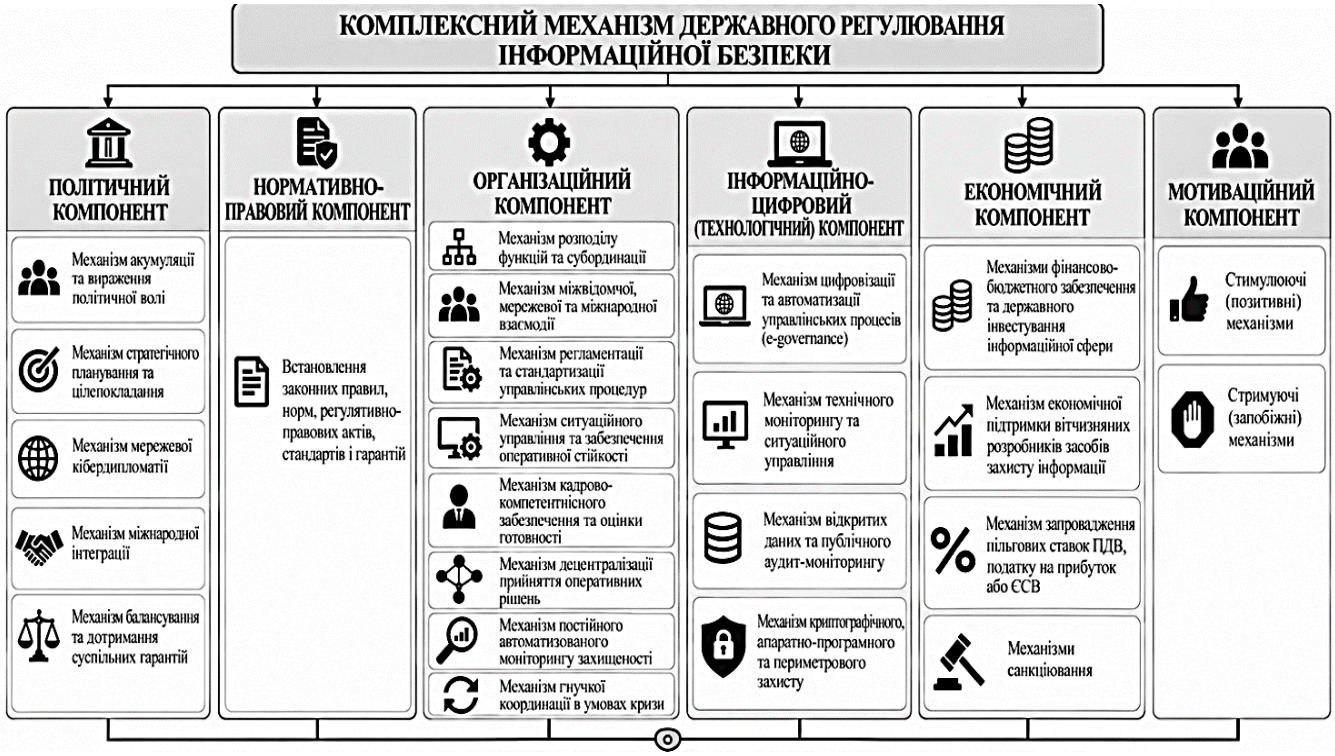

Рис. 2.6. Комплексний механізм державного регулювання інформаційної безпеки

Джерело: власна розробка автора

Отже, механізм державного регулювання сфери інформаційної безпеки виступає складною, багаторівневою та динамічною системою, покликаною забезпечувати захищеність національних інтересів, суверенітету та кіберстійкості критичної інфраструктури в умовах сучасних цивілізаційних викликів. Деструкція або системне ослаблення хоча б одного з елементів призводить до втрати ефективності всього регуляторного механізму. Зокрема, наявність досконалої нормативно-правової бази та інституційного апарату без належного економічного забезпечення перетворює нормативні приписи на

декларативні заяви. Подібним чином, акумуляція фінансових ресурсів і придбання високотехнологічних засобів захисту виявляються малоефективними за відсутності сформованої мотивації та кібергігієни у працівників, що залишає критичні системи вразливими для атак через соціальну інженерію. Таким чином, механізм державного регулювання інформаційної безпеки у науці про публічне управління слід визначати як інтегровану систему політичних, нормативно-правових, організаційних, економічних, техніко-технологічних та мотиваційних інструментів і процедур, за допомогою яких суб'єкти публічної влади здійснюють цілеспрямований, синхронізований та координуючий вплив на інформаційну сферу з метою забезпечення національної безпеки, стійкості критичної інфраструктури та сталого розвитку суспільства.

Проведений аналіз механізмів державного регулювання сфери інформаційної безпеки дозволяє виокремити загальні функції державного регулювання. Основою для цього можуть бути теоретико-методологічні дослідження функціонального наповнення регуляторного впливу, здійснені О. Чечелем. Науковець розглядає державне регулювання економіки та акцентує увагу на тому, що його функції відображають головні напрями та зміст цілеспрямованого впливу держави на суспільні економічні відносини та охоплюють цільову, стимулюючу, нормативну, коригувальну, соціальну й контрольну складові [134]. Такий підхід відображає базову архітектуру регуляторного впливу у публічному управлінні, а тому, скориставшись ним, варто розглянути функції державного регулювання інформаційної безпеки, під якими автор дисертаційного дослідження розуміє основні напрями діяльності органів державної влади, спрямовані на захист цифрового простору, об'єктів критичної інфраструктури та інформаційних ресурсів. Вони охоплюють аналіз загроз, організацію системи захисту, оперативне реагування на кібератаки, встановлення технічних стандартів і постійний контроль задля забезпечення стійкості держави та захисту її суверенітету. Отже, функціями державного регулювання інформаційної безпеки будуть цільова, стимулююча, нормативна, коригувальна, соціальна й контрольна, що відповідає тим механізмам державного регулювання інформаційної безпеки, які описані вище.

Таким чином механізми державного регулювання інформаційної безпеки в умовах цифровізації, глобалізації та розвитку інформаційного суспільства являють собою не просто сукупність елементів, а постають динамічною системою взаємодій, яка забезпечує трансформацію ресурсів та управлінського впливу в конкретний результат.

Інформаційна безпека більше не є сферою, обмеженою технічними чи юридичними параметрами; вона перетворилася на основу національної стійкості, інтегруючи в собі правову, технологічну, політичну та соціальну складові.

Висновки до розділу 2

У сучасному суспільстві, де інформаційні технології інтегровані у всі сфери життя, інформаційна безпека стає необхідною складовою національної безпеки. У розділі 2 дисертаційного дослідження доведено, що безпека інформаційної сфери має забезпечуватись як на рівні законодавства, так і на рівні міжнародного співробітництва, адже кіберзагрози мають глобальний характер.

Аналіз міжнародних та національних нормативних документів продемонстрував різноманітність підходів до правового регулювання інформаційної безпеки, захисту даних та боротьби з кіберзлочинністю. Було розглянуто законодавчі акти різних країн, які регулюють питання доступу до інформації, її конфіденційності та цілісності. Також проаналізовано досвід міжнародних організацій, таких як ООН та Рада Європи, що сприяють створенню спільної системи безпеки у глобальному інформаційному просторі.

Встановлено, що нормативно-правове забезпечення державного регулювання інформаційної безпеки потребує розгалуженої законодавчої бази, яка наразі позбавлена необхідної системності, відсутній єдиний понятійно-термінологічний апарат, правове регулювання сфери інформаційної безпеки досі залишається складним та великим за обсягом. Позитивною рисою нормативно-правової бази забезпечення інформаційної безпеки в Україні є її здатність модернізуватися, адаптуватися до сучасних викликів.

Запропоновано вдосконалити модель нормативно-правового забезпечення

інформаційної безпеки, залишивши в ній лише фундаментальні блоки, які можна змістовно наповнювати відповідно до динамічних трансформацій законодавства. Це дозволить здійснювати ефективне державне регулювання інформаційної безпеки, систематично актуалізуючи кожен елемент структури суб'єктами державного управління. Пропонується зробити таку модель інтерактивною та інтегрувати її з інформаційно-правовими системами, що забезпечить автоматизоване відстеження та оперативно-структуроване розміщення нових нормативно-правових актів у відповідних сегментах пропонованої моделі.

Проаналізовано нормативно-правове регулювання інформаційної безпеки, визначено, що воно є системою, елементами якої виступають сфери застосування нормативно-правового забезпечення інформаційної безпеки: економічна, політична, військова, науково-технологічна, екологічна, соціальна. Окремої уваги потребує кібербезпека як самостійний і ключовий складник інформаційної безпеки.

Встановлено, що дієва державна політика у сфері інформаційної безпеки має базуватися не на механічному поєднанні окремих напрямів, а на глибокій синергії технологічного, організаційно-управлінського та освітнього кластерів:

Інституційний компонент регулювання інформаційної безпеки передбачає ефективну взаємодію та співпрацю різних органів влади, структур публічного управління, правоохоронних організацій, представників бізнес-середовища та інститутів громадянського суспільства.

Доведено, що в епоху гібридних цивілізаційних викликів питання національної та інформаційної безпеки виходять на перший план та стають пріоритетними напрямами діяльності кожного органу влади системи державного управління, жоден з яких не функціонує відірвано від безпекового контексту, оскільки гібридна агресія здійснюється одночасно у військовому, цифровому, когнітивному, економічному, енергетичному та соціальному вимірах. Ця теза надала можливість побудувати цілісну ієрархію суб'єктів забезпечення інформаційної безпеки, розташувавши органи виконавчої влади за рівнями значимості та функціональним призначенням на стратегічному; оперативно-силовому; технологічно-інфраструктурному; зовнішньому; рівні ресурсної,

макроекономічної та екологічної безпеки; рівні соціально-демографічної стійкості; гуманітарно-освітньому та когнітивному рівнях.

Крім того, до інституційної системи забезпечення інформаційної безпеки держави можуть бути віднесені наукові та науково-дослідні установи під час забезпечення науково-аналітичного та експертного супроводження процесу формування та реалізації державної інформаційної політики.

Однак організаційна архітектура – органи публічного управління та установи, які запобігають безпековим загрозам, – становить лише частину інституційного забезпечення інформаційної безпеки. До нього потрібно віднести також комплекс відносин, принципів, процедур, цінностей і функцій, якими керуються ці суб'єкти у своїй діяльності.

Розглянуто механізми державного регулювання інформаційної безпеки в умовах цифровізації, глобалізації та розвитку інформаційного суспільства. Встановлено, що комплексний механізм має охоплювати політичний, нормативно-правовий, організаційний, інформаційно-цифровий (технологічний), економічний та мотиваційний компоненти. Надано ґрунтовну характеристику кожного з компонентів механізму державного регулювання інформаційної безпеки. Проведений аналіз вказує на те, що кожен із зазначених компонентів виконує чітко детерміновану функціональну роль, а саме: цільову, стимулюючу, нормативну, коригувальну, соціальну й контрольну. З'ясовано, що деструкція або системне ослаблення хоча б одного з елементів призводить до втрати ефективності всього регуляторного механізму.

Доведено, що механізм державного регулювання сфери інформаційної безпеки виступає складною, багаторівневою та динамічною системою, покликаною забезпечувати захищеність національних інтересів, суверенітету та кіберстійкості критичної інфраструктури в умовах сучасних цивілізаційних викликів.

Отже, в умовах глобальної цифровізації забезпечення інформаційної безпеки потребує комплексного підходу, що включає правові, управлінські, технічні та міжнародні механізми.

РОЗДІЛ ІІІ
УДОСКОНАЛЕННЯ ДЕРЖАВНОГО РЕГУЛЮВАННЯ ІНФОРМАЦІЙНОЇ БЕЗПЕКИ В УМОВАХ СУЧАСНИХ ЦИВІЛІЗАЦІЙНИХ ВИКЛИКІВ

3.1. Зарубіжний досвід державного регулювання інформаційної безпеки та можливості його адаптації в Україні

Масштабна цифрова трансформація суспільних відносин виводить інформаційну безпеку на стратегічний рівень, утверджуючи її як фундаментальну складову національної безпеки держави. Сучасна держава діє в інформаційному просторі, де державні установи, громадяни, представники бізнесу, медіа та цифрові платформи постійно взаємодіють між собою. Тому порушення захищеності інформаційних систем, незаконне здобуття чи розповсюдження даних, кібератаки, вплив на громадську думку, дезінформаційні кампанії та інші різновиди інформаційного впливу здатні позначатися не лише на окремих інформаційних ресурсах, а й на роботі державних органів, економіці, критичній інфраструктурі та суспільній стабільності .

Значення цієї проблематики істотно зростає на тлі посилення міжнародного суперництва, збільшення кількості збройних протистоянь, активізації державних і недержавних кіберугруповань, поширення технологій штучного інтелекту та змін інформаційного простору. Відповідно до Global Risks Report 2026, підготовленого Всесвітнім економічним форумом, дезінформація та маніпуляції з інформацією й надалі належать до найсерйозніших короткострокових глобальних ризиків поряд із кіберзагрозами. У документі наголошується, що технологічний прогрес водночас відкриває нові перспективи й підвищує вразливість інформаційного середовища, адже розмежувати справжні текст, аудіо або відео та синтетичний контент, згенерований цифровими технологіями, стає дедалі важче [216].

Міжнародний досвід свідчить, що інформаційну безпеку держави не варто

зводити лише до кібербезпеки. Кібербезпека насамперед охоплює захист мереж, інформаційних систем, пристроїв, даних і цифрової інфраструктури від кіберзагроз. Натомість інформаційна безпека є ширшим поняттям: вона передбачає гарантування достовірності, доступності, цілісності та надійності інформації, захист інформаційного простору від маніпулятивного впливу, належне функціонування державних комунікацій і збереження довіри громадян до офіційних інформаційних джерел [24].

Запропоноване бачення особливо виразно відображене у документах Організації економічного співробітництва та розвитку (далі – ОЕСР), зокрема, у звіті «Факти, а не фейки: протидія дезінформації та зміцнення інформаційної цілісності» ОЕСР розглядає інформаційну цілісність як одну з необхідних умов функціонування демократичних суспільств. Організація підкреслює, що державна політика має зосереджуватися не тільки на безпосередньому протидіянні неправдивому контенту, а насамперед на формуванні інформаційного середовища, у якому громадяни мають доступ до своєчасної, різноманітної, достовірної та перевіреної інформації [192].

Водночас ОЕСР не визначає державу суб'єктом, який повинен визначати «правильність» інформації, що надходить до суспільства. Навпаки, у звіті наголошено на потребі одночасно забезпечувати інформаційну стійкість і фундаментальні свободи, зокрема свободу слова та можливість доступу до різних інформаційних джерел.

Розмежування інформаційної та кібербезпеки має методологічне значення: нормативні інструменти кіберзахисту не охоплюють усіх ризиків дезінформації, маніпуляцій та кризової комунікації. Водночас не слід ототожнювати інформаційну цілісність у підході ОЕСР із юридично визначеним обов'язком держави контролювати зміст усіх повідомлень. Саме поєднання захисної та правозабезпечувальної функцій є критерієм оцінювання зарубіжних практик [192].

Одним із найпослідовніших прикладів розбудови сучасної політики інформаційної безпеки є Європейський Союз, який поетапно створив багаторівневу нормативну базу, що охоплює кібербезпеку, захист критичної

інфраструктури, цифрові платформи, персональні дані, протидію дезінформації та підтримання цифрової стійкості.

Важливе місце в цій системі посідає Директива (ЄС) 2022/2555, відома як NIS2 Directive, яка істотно розширила межі європейського регулювання у сфері кібербезпеки. Її концепція ґрунтується на тому, що кіберстійкість держави не може забезпечуватися виключно захистом центральних органів влади. Вразливість одного сектора здатна спричинити ланцюгові наслідки для інших сфер суспільного життя, тому до системи безпеки залучаються організації, що працюють у критично важливих секторах [162].

NIS2 вирізняється посиленням вимог щодо управління кіберризиками, інформування про суттєві інциденти, відповідальності керівників організацій і взаємодії між компетентними органами. Отже, кібербезпека трактується не просто як технічне завдання IT-підрозділу, а як складова стратегічного управління [162].

Європейська модель також ґрунтується на розвитку спеціалізованої інституційної структури. Важливу роль у ній відіграє Агентство Європейського Союзу з кібербезпеки ENISA, яке оцінює кіберзагрози та готує галузеві аналітичні звіти. У ENISA Threat Landscape 2025 було розглянуто 4875 інцидентів за період від липня 2024 року до червня 2025 року, що дало змогу визначити ключові тенденції еволюції кіберзагроз у Європі [166].

Окреме дослідження ENISA присвячене державному управлінню. У ENISA Sectorial Threat Landscape – Public Administration розглядаються кіберзагрози, які впливали на сектор публічного адміністрування ЄС, а також поширені способи атак і профілі загроз. Виокремлення публічного управління в самостійну категорію свідчить про те, що державні інформаційні системи сприймаються як окремий стратегічний об’єкт кіберзахисту [165].

Водночас європейський підхід значно ширший за питання кібербезпеки, а тому важливе місце в ньому займає протидія інформаційним маніпуляціям та дезінформації. Саме тому ЄС розробив комплекс регуляторних та інституційних інструментів, що стосуються роботи цифрових платформ, прозорості алгоритмів і системних ризиків для суспільства.

Центральну роль у цій системі відіграє Digital Services Act (DSA). Законодавство ЄС зобов'язує великі онлайн-платформи виявляти та знижувати системні ризики, зокрема пов'язані з поширенням незаконного контенту й загрозами для інформаційного середовища [201]. Європейська Комісія також застосовує механізми співпраці з платформами у випадках масштабних інформаційних загроз.

При цьому Директива NIS2 встановлює вимоги до управління кіберризиками та повідомлення про інциденти для визначених категорій суб'єктів, тоді як Регламент DSA регулює відповідальність посередницьких онлайн-сервісів і передбачає особливі обов'язки щодо оцінювання та зменшення системних ризиків для дуже великих онлайн-платформ і пошукових систем. Отже, ці акти не є взаємозамінними: вони охоплюють різні об'єкти регуляторного впливу [162; 201].

Особливої актуальності в сучасній системі інформаційної безпеки набуває питання іноземного інформаційного впливу. Глобалізація цифрового простору дала змогу державним і недержавним акторам проводити інформаційні операції без фізичної присутності на території іншої країни [21].

До ключових інструментів такого впливу належать створення й поширення недостовірного контенту, застосування фальшивих акаунтів, координація інформаційних мереж, викривлення реальних подій, використання ботів, підроблених документів, синтетичних фото-, аудіо- та відеоматеріалів, а також соціальних мереж для штучного посилення окремих інформаційних наративів [192].

У цьому контексті OECD пропонує розглядати протидію дезінформації за трьома взаємопов'язаними напрямами: забезпечення прозорості, підзвітності та плюралізму інформаційних джерел; формування суспільної стійкості до дезінформації; удосконалення державного управління й інституційної структури задля збереження цілісності інформаційного простору [192].

Перший напрям передбачає створення таких умов, за яких громадяни матимуть доступ до різноманітних джерел інформації та зможуть самостійно перевіряти отримані повідомлення. Практичним втіленням принципів

прозорості, підзвітності та плюралізму інформаційних джерел у системі державного регулювання є впровадження норм Європейського акта про свободу медіа (EMFA), який, зокрема, гарантує прозорість через обов'язкове розкриття кінцевих бенефіціарних власників та джерел фінансування медіа-ресурсів, забезпечує їх підзвітність через механізми публічного контролю й аудиту алгоритмів цифрових платформ, а також підтримує плюралізм шляхом недопущення монополізації інформаційного простору та нормативного захисту редакційної незалежності від державного чи олігархічного тиску. Другий напрям стосується розвитку медіаграмотності, критичного мислення та здатності суспільства виявляти маніпулятивний контент. Концепція наскрізної медіаосвіти та формування критичного мислення успішно імплементовані у країнах ЄС. Зокрема, фінська модель «наскрізного когнітивного захисту» передбачає системне інтегрування навичок фактчекінгу у заклади освіти всіх рівнів. Традиція розвитку медіаграмотності у фінських школах є тривалою, а протягом останнього десятиліття вона стала наскрізною темою всіх дисциплін. Основний акцент при цьому робиться не стільки на боротьбі з неправдивою інформацією, скільки на розвитку критичного мислення [75]. Європейська рамка компетенцій DigComp 2.2 нормативно визначає здатність виявляти маніпулятивний контент як базовий елемент цифрової грамотності громадянина та є головним міжнародним орієнтиром для оцінки та розвитку цифрової грамотності [161]. Третій напрям безпосередньо пов'язаний із діяльністю органів державної влади, їхньою спроможністю оперативно реагувати на інформаційні кризи й забезпечувати населення достовірними відомостями [192].

Важливість таких напрямів набуває особливого значення під час криз, катастроф і воєнних конфліктів. В умовах інформаційної невизначеності населення потребує від органів влади швидкої, чіткої та зрозумілої комунікації. Якщо офіційні повідомлення надходять із запізненням, інформаційний вакуум можуть заповнити неперевірені відомості або навмисно поширюваний дезінформаційний контент.

Європейський досвід свідчить, що регуляторний ефект досягається не лише встановленням заборон, а й визначенням процедур оцінювання ризиків,

обов’язків суб’єктів, компетенцій наглядових органів та механізмів співпраці. Імплементація зазначеного досвіду в Україні передбачає розмежування нормативних вимог до кіберзахисту суб’єктів критичної інфраструктури та гарантій прозорого й відповідального функціонування цифрових платформ на основі принципу пропорційності.

Що стосується США, то вони використовують дещо іншу модель, у межах якої особливе значення надається розподілу відповідальності між державними установами, приватним бізнесом і власниками критичної цифрової інфраструктури. Так, Національна стратегія кібербезпеки США 2023 року ґрунтується на необхідності створення безпечного та стійкого кіберпростору, де відповідальність за кіберзахист покладається на тих суб’єктів, які мають найкращі можливості для контролю відповідних ризиків [184].

Визначальною особливістю американської моделі є вагома роль Cybersecurity and Infrastructure Security Agency (CISA). Агентство координує заходи із захисту критичної інфраструктури, готує рекомендації для органів влади й приватного сектору, організовує обмін інформацією про загрози та сприяє зміцненню загальної кіберстійкості [155].

Досвід США засвідчує, що забезпечення інформаційної безпеки держави неможливе без систематичної участі приватного сектору. Значна частина телекомунікаційних мереж, хмарних сервісів, дата-центрів, енергетичних систем та інших критично важливих об’єктів належить приватним власникам. Через це держава не здатна захистити їх лише адміністративними інструментами.

Відтак американський підхід значною мірою спирається на державно-приватне партнерство, обмін даними про кіберзагрози, проведення спільних навчань і формування уніфікованих стандартів кіберзахисту.

Важливим напрямом роботи є також безпека ланцюгів постачання. Цифрова інфраструктура сучасної держави залежить від програмного забезпечення, хмарних ресурсів, технічного обладнання та зовнішніх постачальників. Компрометація одного елемента може відкрити шлях до порушення безпеки всієї ширшої системи. Саме тому сучасна політика США приділяє значну увагу захисту програмного забезпечення, постачальників і

цифрових технологій [184].

Окреме місце посідає міжнародна кібердипломатія, Державний департамент США трактує кіберпростір не тільки як технологічне середовище, а й як сферу міжнародних відносин, що потребує взаємодії союзників, протидії кіберзлочинності, підтримки глобальних норм відповідальної поведінки держав і захисту прав людини [209].

Важливим методичним орієнтиром є NIST Cybersecurity Framework 2.0, який структурує управління кіберризиками за шістьма функціями: управління (Govern), ідентифікація (Identify), захист (Protect), виявлення (Detect), реагування (Respond) та відновлення (Recover). Послідовна реалізація цих функцій дозволяє сформувати безперервний цикл управління кіберризиками на всіх рівнях державного врядування. Видається можливим представити забезпечення кіберстійкості за стандартом NIST CSF 2.0 у вигляді схеми (рис.3.1).

Рис. 3.1. Функціонально-структурна схема забезпечення кіберстійкості за стандартом NIST CSF 2.0

Джерело: власна розробка автора

Представлена схема на рис 3.1. може використовуватись як концептуальна модель забезпечення кіберстійкості, де функція GOVERN (Управління / Врядування) виступає надсистемним, скріплювальним ядром, відображає стратегічний рівень державного управління інформаційною безпекою. Саме ця функція визначає стратегічні орієнтири, безпекові політики та процедури оцінки ризиків, на основі яких послідовно розгортається безперервний операційний цикл кіберзахисту: від початкової ідентифікації активів, які несуть загрозу інформаційній та національній безпеці країни, та їх інструментального захисту – до безперервного моніторингу й виявлення аномалій (SIEM/EDR), локалізації інцидентів (реагування) та підсумкового відновлення стійкості інформаційно-комунікаційних систем суб'єктів публічного управління.

Слід, однак, зазначити, що стандарт NIST CSF 2.0 є рамковою системою рекомендацій, і не виступає в якості універсального обов'язкового федерального закону США. Застосування американського досвіду потребує врахування різниці між обов'язковими правовими вимогами та добровільними стандартами. Перенесення рамкових рекомендацій NIST без визначення відповідальних суб'єктів, процедур перевірки та джерел фінансування не створить дієвого регуляторного механізму [189]. Але практична цінність такого підходу надає можливість узгодження управлінських рішень, показників ризиків та заходів відновлення в межах безперервного циклу, що може стати орієнтиром для вдосконалення системи державного управління інформаційною безпекою України [189].

Вагомий досвід у сфері забезпечення інформаційної безпеки напрацьовано також в межах НАТО. Альянс визначає кіберпростір як самостійний операційний домен і розглядає кіберзахист як невіддільний елемент стримування та оборони [185]. НАТО підкреслює, що кіберзагрози можуть бути різномасштабними – від порівняно локальних інцидентів до атак, спроможних спричинити серйозні порушення роботи державних систем, критичної інфраструктури й оборонного потенціалу. Саме тому Альянс використовує поєднання технічних, політичних, дипломатичних і військових засобів реагування [185]. У структурі НАТО діють механізми обміну даними про кіберзагрози, співпраці між державами-членами,

проведення навчань, а також підтримки країн у разі масштабних кіберінцидентів. У 2024 році країни НАТО домовилися заснувати NATO Integrated Cyber Defence Centre, покликаний посилити захист мереж, ситуаційну обізнаність і розвиток кіберспроможностей Альянсу [185].

Важливим елементом сучасної політики НАТО є також інформаційна стійкість. Альянс визначає інформаційні загрози як навмисні, шкідливі, маніпулятивні та скоординовані дії, спрямовані на поширення плутанини, загострення суспільних розбіжностей, дестабілізацію суспільства й послаблення державних та міжнародних інституцій [187]. Поняття «стійкість» – «resilience» – має особливе значення в підході Альянсу. Воно охоплює не тільки здатність запобігати атакам, а й спроможність зберігати функціонування після їх здійснення та швидко відновлюватися [187].

Принцип резильєнтності має важливе практичне значення для держав, адже повністю захистити всі інформаційні системи фактично неможливо. Тому державна політика має бути спрямована на створення систем, здатних витримувати порушення, обмежувати їхні наслідки та відновлювати роботу в найкоротші строки. Якщо класична інформаційна безпека фокусувалася переважно на запобіганні загрозам (пасивні бар'єри, периметр, фільтрація), то кіберрезильєнтність визнає: компрометація або технічний збій рано чи пізно стануться, тому система має бути сконструйована так, щоб витримувати удар, адаптуватися та максимально швидко відновлюватися. Це стосується насамперед системи публічного управління, яка, навіть за умов успішної атаки на окремі елементи, повинна зберігати спроможність виконувати свої базові функції та надавати критичні послуги громадянам, оперативно аналізувати атаки та аномалії та корегувати політику захисту [25].

Не менш важливою за резильєнтність технічно-програмного комплексу є стійкість людського капіталу. Кожен член управлінської команди повинен вміти правильно реагувати на інциденти, сповідувати принципи кібер- та інформаційної гігієни та критичного мислення.

Резильєнтність стає необхідною умовою функціонування публічного управління в умовах цивілізаційних викликів та загроз, що виявляється у

здатності системи передбачати, витримувати, відновлюватися та адаптуватися. Розглядаючи державне регулювання інформаційної безпеки як систему, потрібно зважати на те, що вона має ознаки нелінійних динамічних систем, а тому резильєнтність є відповіддю на складні виклики, що пов'язані з управлінням і підтриманням її функціонування, та враховує складність, хаотичність і потенційну нестабільність середовища [61]. Українські дослідники виокремлюють складові інституційної резильєнтності органів державної влади та їхній управлінський зміст та зазначають, що ключовою складовою виступає інформаційно-кібернетична резильєнтність, оскільки «цифрові реєстри, системи документообігу і канали комунікації забезпечують виконання майже всіх функцій держави» [112].

Документ НАТО щодо протидії інформаційним загрозам від 18 жовтня 2024 року передбачає взаємопов'язані напрями: розуміння інформаційного середовища, запобігання загрозам, обмеження їхнього впливу та відновлення. Водночас Альянс не встановлює єдиних для всіх держав національних адміністративних процедур регулювання медіа. Тому для України насамперед релевантними є методики аналізу загроз, міжвідомча сумісність та механізми оперативної координації [186]. У практичному вимірі органам влади потрібні сценарії відновлення після інцидентів, резервні канали зв'язку, сегментація доступів, навчання персоналу і регулярні перевірки готовності протистояти загрозам.

Особливе значення у міжнародній практиці має захист критичної інфраструктури, до якої належать енергетична сфера, транспорт, зв'язок, медицина, фінансовий сектор, водопостачання та державні цифрові послуги Всі вони потребують інформаційного захисту, оскільки активно використовують сучасні інформаційні технології. Тому кібератака на інформаційну систему здатна спричинити не лише технічні збої, а й фізичну або суспільну кризу [36]. У своїх аналітичних матеріалах ENISA підкреслює, що кіберзагрози стають дедалі складнішими, а управління ними потребує системного підходу. Дослідження тисяч інцидентів у Європі свідчить: кіберзагрози впливають не тільки на окремі підприємства, а й на всю сукупність суспільних та державних

функцій [166].

Для державного управління це означає потребу відмовитися від суто реактивної моделі на користь превентивної. Реактивний підхід полягає в діях уже після здійснення атаки. Натомість превентивна модель передбачає безперервний моніторинг, оцінювання ризиків, резервування систем, поділ мереж на сегменти, перевірку планів відновлення та регулярне проведення кібернавчань.

Не менш важливим є принцип «security by design», за яким питання безпеки враховуються ще на етапі проєктування інформаційної системи. Він узгоджується із сучасними практиками управління ризиками та безпечної розробки цифрових рішень [184].

Міжнародний досвід також свідчить, що багато інформаційних інцидентів зумовлені не лише технічними недоліками, а й людським фактором. Фішингові атаки, соціальна інженерія, застосування ненадійних паролів, відкриття шкідливих вкладень і недбале поводження з конфіденційною інформацією можуть поставити під загрозу навіть систему з високим рівнем технічного захисту [21]. Окремого значення набуває навчання державних службовців, державні установи працюють із великими масивами персональних, фінансових, службових і стратегічних даних, тому помилка одного працівника може призвести до серйозних наслідків.

Однією з ключових рис інформаційної безпеки є транскордонний характер загроз: наприклад, сервер, через який здійснюється атака, може бути розташований в одній країні, жертва – в іншій, а особи, що керують атакою, – у третій. Так само інформаційна кампанія може розроблятися однією групою, поширюватися через платформи, що належать до іншої юрисдикції, і бути спрямованою на критичну інфраструктуру та населення третьої держави.

Отже, жодна країна не здатна повною мірою гарантувати власну інформаційну безпеку самостійно. Саме тому важливого значення набувають міжнародні організації, двосторонні домовленості, обмін даними та спільні навчання [207].

Сучасне інформаційне середовище вирізняється появою нових видів загроз, які набагато важче виявляти за допомогою традиційних методів. Одним

із ключових чинників цього процесу є розвиток генеративного штучного інтелекту. ШІ дає змогу автоматизувати виробництво значних обсягів текстів, зображень, аудіо та відеоматеріалів. Завдяки цьому суб'єкти інформаційного впливу можуть створювати персоналізований контент у набагато більших масштабах, ніж раніше [66].

Особливу небезпеку становлять deepfake-технології, відео або аудіо, згенеровані за допомогою ШІ, що здатні імітувати реальну людину та формувати хибне уявлення про позицію державного діяча, військового керівництва чи іншої публічної особи [109].

Важливим викликом також є автоматизація кіберзлочинності: ШІ може застосовуватися для підготовки більш переконливих фішингових повідомлень, опрацювання великих обсягів даних і автоматизації окремих етапів кібератак [157].

Отже, сучасна інформаційна безпека повинна враховувати не тільки традиційні кіберзагрози, а й поєднання кібероперацій, інформаційних операцій і технологій штучного інтелекту. Важливою рисою сучасного міжнародного підходу є перенесення уваги від виключно технічного захисту інформаційних систем до стійкості суспільства.

Стійке суспільство – це не те суспільство, у якому дезінформація цілком відсутня, така мета практично недосяжна. Йдеться про спроможність громадян виявляти маніпуляції, перевіряти відомості, використовувати кілька джерел і зберігати здатність ухвалювати раціональні рішення в умовах інформаційного тиску [67].

ОЕСР наголошує на важливості підтримки незалежної журналістики, прозорості інформаційних платформ, розвитку медіаграмотності та забезпечення громадянам доступу до різноманітних інформаційних джерел [192].

НАТО, зі свого боку, підкреслює потребу посилення стійкості суспільств до інформаційних загроз, адже інформаційні операції можуть бути спрямовані не тільки проти державних систем, а й проти суспільної єдності [186].

Окремо слід ураховувати обмеженість висновків, отриманих із статистики інцидентів: показники ENISA характеризують зареєстровані й досліджені

випадки у визначений період, а не абсолютну кількість усіх кібератак у Європі. У звіті ENISA Threat Landscape 2025 проаналізовано 4875 інцидентів за липень 2024 – червень 2025 року. У звіті за 2026 рік окремо підкреслено ризики цифрової взаємозалежності та значну частку атак на публічне адміністрування [167].

Аналіз зарубіжних регуляторних підходів інформаційної безпеки дозволив виокремити критерії для їх порівняння (табл. 3.1). Такими критеріями є за об'єкт регулювання, інструменти впливу, механізми координації. Практичне значення цього порівняльного аналізу дозволяє визначити можливості застосування цих інструментів в Україні. Зауважимо, що НАТО у цьому зіставленні виступає джерелом координаційних практик, а не національною регуляторною моделлю.

Таблиця 3.1

Порівняльна характеристика зарубіжних механізмів державного регулювання інформаційної безпеки

Підхід	Провідні інструменти	Можливості для України
ЄС	NIS2: вимоги до управління кіберризиками; DSA: оцінювання системних ризиків платформ; аналітика ENISA.	Правова гармонізація; диференційовані обов'язки суб'єктів; оцінювання системних ризиків.
США	Рамка NIST CSF 2.0; CISA; державно-приватна взаємодія.	Управлінський цикл кіберризиків; координація з операторами критичної інфраструктури.
НАТО	Колективний кіберзахист; аналіз інформаційних загроз; координація та відновлення.	Спільні процедури обміну інформацією, раннього попередження і кризової комунікації.

Джерело: систематизовано автором на основі проведених досліджень

Проведене дослідження, результати якого представлено у табл. 3.1, показує, що ці підходи не є взаємовиключними альтернативами, між якими необхідно обрати лише одну. ЄС пропонує нормативні обов'язки, США позиціонує практики розподіленого управління ризиками, а НАТО вказує на координаційні інструменти колективної стійкості. Оптимальним шляхом є виокремлення та систематизація найефективніших інструментів із зазначених практик із метою подальшої гармонізації міжнародних підходів до державного регулювання інформаційної безпеки в Україні. Водночас цей процес не повинен зводитися до механічного запозичення чи формальної імплементації зарубіжних

механізмів у практику публічного управління. Пріоритетом має бути забезпечення їхньої правової сумісності із національним законодавством та послідовне нарощування інституційної спроможності органів публічної влади.

На основі здійсненого порівняльного аналізу автором дисертаційного дослідження запропоновано критеріально-адаптаційний підхід до адаптації зарубіжних механізмів державного регулювання інформаційної безпеки, відповідно до якого зарубіжні практики оцінюються не за фактом їх успішної реалізації в іноземній юрисдикції, а за ступенем відповідності конкретним безпековим та управлінським потребам України. Запропоновано шість критеріїв такої адаптації, які виокремлено у ході даного дослідження на основі вивчення міжнародної документальної бази (табл. 3.2).

Таблиця 3.2

Критерії адаптації зарубіжних механізмів державного регулювання інформаційної безпеки

Критерій	Визначене питання для оцінювання	Управлінське рішення
Нормативно-правова сумісність	Чи допускає механізм українське законодавство та міжнародні зобов'язання?	Правова допустимість; необхідні зміни
Інституційна спроможність	Хто уповноважений реалізувати механізм і координувати суб'єктів?	Організаційні передумови
Безпекова релевантність	Які саме актуальні загрози та вразливості зменшує механізм?	Пріоритетність
Ресурсна забезпеченість	Які кошти, кадри й технології необхідні?	Здійсненність і строки
Превентивність та адаптивність	Чи забезпечує механізм прогнозування, моніторинг і коригування?	Здатність попереджати загрози
Дотримання прав людини	Чи є втручання законним, необхідним і пропорційним?	Правозахисна прийнятність

Джерело: розроблено автором на основі проведених досліджень

Такими критеріями виступають нормативно-правова сумісність, інституційна спроможність, безпекова релевантність, ресурсна забезпеченість, превентивність та адаптивність, дотримання прав людини.

Так, нормативно-правова сумісність передбачає оцінювання юридичної допустимості застосування певного механізму, потреби у внесенні змін до національного законодавства та відповідності зобов'язанням України щодо наближення до права ЄС. Зокрема, нормативні приписи Директив NIS2 та Закону

про цифрові послуги (DSA) не підлягають механічній екстраполяції за межі визначеного ними предмета правового регулювання та нормативно встановленого кола адресатів.

Інституційна спроможність охоплює можливості компетентних органів здійснювати координацію, моніторинг, нагляд і реагування. Підходи OECD до цілісності інформаційного середовища наголошують на узгодженості політики, міжсекторальній взаємодії та прозорості зазначених процедур.

Безпекова релевантність визначається здатністю конкретного механізму зменшувати інформаційні вразливості, пов'язані зі збройною або гібридною агресією, кібератаками, іноземним інформаційним втручанням і технологічними ризиками. Зазначене підтверджує, що не кожен інструмент, який довів свою ефективність у мирних умовах або в умовах стабільного середовища, автоматично відповідає актуальним безпековим та управлінським потребам України в період воєнного стану або повоєнного відновлення.

Ресурсна забезпеченість потребує оцінювання фінансових витрат, технологічної бази, кадрового потенціалу та строків реалізації. При цьому кожен із зазначених ресурсних факторів впливає на ефективність державного регулювання інформаційної безпеки. У такому контексті, наприклад, варто розмежувати короткострокові заходи, визначити поетапність реформ і рішень, що потребують попереднього формування або розбудови відповідних спроможностей.

Превентивність та адаптивність означають спроможність механізму забезпечувати оцінювання ризиків, раннє виявлення загроз, безперервність критичних функцій та коригування регуляторних інструментів. Саме цей критерій пов'язує зарубіжний досвід із превентивно-адаптивною моделлю, обґрунтованою в підрозділі.

Дотримання прав людини передбачає оцінювання законності, необхідності та пропорційності обмежень, гарантій свободи вираження поглядів, доступу до інформації й захисту персональних даних, що повинно відбуватися на рівні особи, держави та суспільства. Відповідні вимоги є умовою допустимості запозичення, а не другорядним показником його ефективності.

Запропонована послідовність застосування критеріїв охоплює три етапи: спочатку перевіряються нормативно-правова сумісність і дотримання прав людини; далі оцінюються інституційна спроможність, безпекова релевантність, ресурси, превентивність та адаптивність; після цього визначається спосіб адаптації, а саме використання сумісної практики, модифікація з необхідними змінами або відмова від запозичення (рис. 3.2). Цей алгоритм не є чинною адміністративною процедурою української управлінської практики, а виступає авторською методичною пропозицією, спрямованою на оптимізацію застосування механізмів державного регулювання інформаційної безпеки, що, звичайно потребує подальшої практичної апробації.

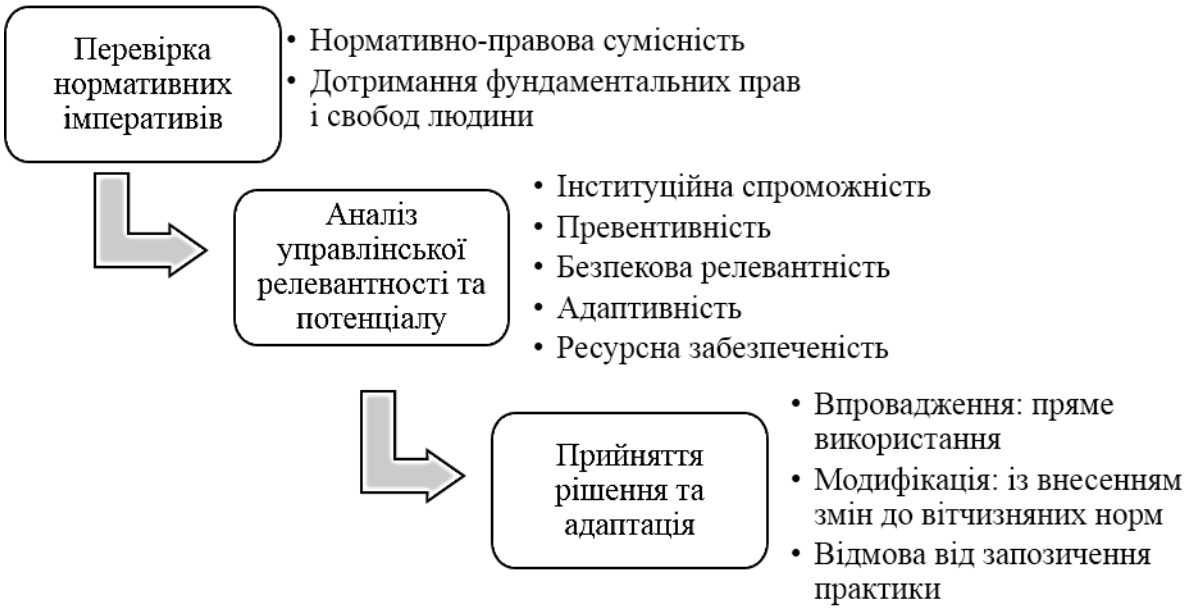

Рис. 3.2. Алгоритм адаптації зарубіжних механізмів державного регулювання інформаційної безпеки в управлінську практику української держави

Джерело: розроблено автором на основі проведених досліджень

Наведеній алгоритмічній послідовності притаманний ступеневий характер: перший етап виступає нормативно-ціннісним «фільтром», що унеможливлює імплементацію правово несумісних рішень; другий – забезпечує розрахунково-аналітичну діагностику потенціалу практики за п’ятьма функціональними критеріями; третій етап формулює управлінську альтернативу

(імплементація, адаптивна модифікація або відхилення практики).

Для України використання міжнародного досвіду у сфері інформаційної безпеки є особливо важливим через тривале поєднання воєнних, кібернетичних та інформаційних загроз. Тому зарубіжні практики варто застосовувати не через пряме копіювання окремих моделей, а шляхом пристосування найрезультативніших інструментів до українських інституційних і безпекових реалій [154].

Насамперед доцільно й надалі зміцнювати ризик-орієнтований підхід, практика ЄС засвідчує, що держава повинна не лише реагувати на вже проведені атаки, а й регулярно оцінювати потенційні загрози для критичної інфраструктури.

Другим напрямом має стати розширення державно-приватного партнерства. Досвід США доводить, що надійний захист інформаційної інфраструктури неможливий без участі приватного сектору, у власності якого перебуває значна частина цифрової інфраструктури.

Третім напрямом може бути подальший розвиток міжнародного обміну даними про кіберзагрози. Досвід НАТО показує, що швидке обговорення інцидентів і спільні дії у відповідь дають змогу обмежити наслідки атак.

Четвертим напрямом є зміцнення інформаційної стійкості суспільства, саме для цього слід поєднувати медіаграмотність, цифрову освіту, підтримку незалежних медіа, відкритість державної комунікації та оперативне спростування дезінформації.

Шостим напрямом є підготовка до нових технологічних викликів, зокрема, розвиток штучного інтелекту вимагає одночасного формування засобів протидії автоматизованому створенню дезінформації, deepfake-контенту, автоматизованим кібероперація̆м та іншим видам технологічного впливу.

Не менш важливим є поступовий перехід до проактивної моделі інформаційної безпеки. Вона передбачає безперервне спостереження за інформаційним середовищем, виявлення аномалій, оцінювання ризиків, прогнозування можливих атак, регулярну перевірку систем і розроблення сценаріїв кризового реагування.

Встановлено, що регуляторні підходи ЄС, США та координаційні механізми НАТО мають різну правову природу, однак поєднуються спільною увагою до управління ризиками, міжсекторальної взаємодії та стійкості. Удосконалення державного регулювання інформаційної безпеки України доцільно здійснювати шляхом вибіркової, юридично обґрунтованої адаптації інструментів, а не механічного копіювання іноземних моделей.

Запропоновано критеріально-адаптаційний підхід, що включає шість критеріїв і три послідовні етапи оцінювання. Він забезпечує зв'язок між порівняльним аналізом зарубіжних практик та превентивно-адаптивною моделлю, обґрунтованою в першому розділі дисертації.

Отже, з огляду на результати здійсненого аналізу, пріоритетними напрямами вдосконалення державного регулювання визначено: удосконалення ризик-орієнтованих вимог до суб'єктів критичної інфраструктури; нормативне запровадження процедур регулярного оцінювання ризиків; посилення обміну інформацією між державою та приватними операторами; розвиток стратегічних комунікацій; підвищення кваліфікації державних службовців; створення правових гарантій пропорційності заходів протидії інформаційно-кібернетичним загрозам. Реалізація кожного із зазначених напрямів вимагає чіткого визначення відповідального суб'єкта публічного управління (інституційне забезпечення), нормативно-правового підґрунтя (нормативно-правове забезпечення), а також механізмів державного регулювання інформаційної безпеки з урахуванням світового та національного досвіду.

3.2. Удосконалення механізмів державного регулювання інформаційної безпеки України в умовах сучасних цивілізаційних викликів

Сучасний етап розвитку інформаційного суспільства характеризується поглибленням цифрової взаємозалежності державних інституцій, суб'єктів господарювання та громадян, інтенсивним впровадженням технологій штучного інтелекту, розширенням цифрових комунікацій і зростанням масштабів інформаційних та кібернетичних загроз. В умовах збройної агресії проти України

зазначені процеси набувають особливого значення, оскільки порушення функціонування інформаційних систем, деструктивні інформаційні впливи й кібератаки на критичну інфраструктуру здатні спричиняти міжсекторальні наслідки для національної безпеки.

У розділі 2 дисертаційного дослідження було доведено, що механізми державного регулювання інформаційної безпеки утворюють динамічну, багаторівневу систему та складають єдиний комплексний механізм державного регулювання інформаційної безпеки в умовах цифровізації, глобалізації та розвитку інформаційного суспільства, який охоплює політичний, нормативно-правовий, організаційний, інформаційно-цифровий (технологічний), економічний та мотиваційний компоненти. Кожен з цих компонентів має складну структуру, а їх ефективність визначає здатність держави забезпечити безпеку інформаційного середовища, запобігати кібератакам і дезінформації, підтримувати довіру громадян до державних інститутів, тобто реалізовувати завдання загальної національної безпеки.

Звичайно, комплексний механізм державного регулювання інформаційної безпеки в умовах цифровізації, глобалізації та розвитку інформаційного суспільства не може залишатися статичним, він повинен постійно вдосконалюватися та адаптуватися під ті виклики, які генерує сучасне безпекове середовище та які постають перед вітчизняною системою публічного врядування. Зокрема, мова йде про високу динаміку гібридних загрозових чинників, трансформацію кіберзагроз в елемент збройної агресії та прискорений розвиток новітніх технологій (штучного інтелекту, розподілених систем та ін.). Це зумовлює необхідність переходу від пасивної реактивної захищеності до адаптивної, ризик-орієнтованої кіберстійкості, здатної функціонувати в умовах високого рівня невизначеності. Ключовими напрямами такої адаптації є гнучке оновлення нормативно-правового поля, підвищення інституційної спроможності суб’єктів забезпечення безпеки, інтеграція передових міжнародних стандартів (зокрема NIST CSF 2.0) та розбудова дієвого партнерства з міжнародними партнерами, приватним сектором та громадськими організаціями особливо в період воєнного стану й повоєнного відновлення. Одним із нагальних питань

вдосконалення механізму державного регулювання інформаційної безпеки постає питання формування колективної інформаційної культури, стимулювання проактивної поведінки громадян у сфері кібергігієни, вироблення комплексної та адаптивної стратегії інформаційної безпеки. Потрібно створювати оперативні підсистеми моніторингу загроз, аналітичні центри прогнозування інформаційних ризиків, інтегрувати новітні технології штучного інтелекту та систем автоматизованого аналізу даних у державні структури. Не менш важливим є включення у механізм інформаційної безпеки елементів комунікаційної стратегії, що забезпечує прозорість, довіру та координацію між державою, громадянами та міжнародними партнерами. 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. Комплексне впровадження зазначених заходів створює ефект синергії та робить механізм 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, підтримувати стійкість державного інформаційного середовища, що робить захист державного суверенітету в інформаційній сфері надійним, цілісним та ефективним [8].

У підрозділі 2.3 дисертації систему державного регулювання інформаційної безпеки розкрито як цілісний багатовимірний механізм, який інтегрує ключові виміри публічно-управлінського впливу. Кожен з компонентів – політичний, нормативно-правовий, організаційний, інформаційно-цифровий (технологічний), економічний та мотиваційний – має власну структуру, тобто спирається на механізми забезпечення того чи іншого компонента комплексного механізму державного регулювання інформаційної безпеки. Так, політичний компонент механізму державного регулювання інформаційної безпеки включає в себе механізм акумуляції та вираження політичної волі; механізм стратегічного планування та цілепокладання; механізм мережевої кібердипломатії; механізм міжнародної інтеграції; механізм балансування та дотримання гарантій.

Нормативно-правовий компонент установлює правові підстави діяльності компетентних органів, вимоги до захисту інформаційних ресурсів, права й обов'язки суб'єктів та процедури застосування відповідних заходів. Організаційний компонент базується на використанні механізму розподілу функцій та субординації; механізму міжвідомчої, мережевої та міжнародної взаємодії; механізмі регламентації та стандартизації управлінських процедур, механізмі ситуаційного управління та забезпечення оперативної стійкості та інших механізмах, описаних у підрозділі 2.3 даного дисертаційного дослідження.

Наявність зазначених механізмів не гарантує їх результативності: нормативно встановлені вимоги потребують організаційного забезпечення, технічні заходи – фахівців і фінансування, а результати моніторингу – належного врахування в управлінських рішеннях. Тому варто розглядати не лише кожен механізм окремо, а й правила та процедури їх узгодженої взаємодії.

Тому одним із завдань даного дисертаційного дослідження є надання рекомендацій щодо удосконалення механізмів державного регулювання інформаційної безпеки України в умовах сучасних цивілізаційних викликів.

Наприклад, удосконалення нормативно-правового компонента механізму державного регулювання інформаційної безпеки має передбачати узгодження правового регулювання інформаційної безпеки, кібербезпеки, захисту персональних даних і стійкості критичної інформаційної інфраструктури [110].

Практичним кроком до вдосконалення механізмів державного регулювання інформаційної безпеки є запровадження проведення міжвідомчого правового аудиту: формування реєстру чинних вимог, виявлення дублювання та прогалин, перевірка узгодженості процедур повідомлення про інциденти, реагування й відновлення. Результатом має бути перелік конкретних норм, що потребують уточнення, із зазначенням компетентного суб'єкта та необхідного нормативного рішення.

Другим кроком на шляху до вдосконалення механізму державного регулювання інформаційної безпеки є ризик-орієнтована диференціація вимог залежно від критичності інформаційних ресурсів, можливих наслідків порушення їх функціонування та характеру загроз. Вимоги повинні бути

пропорційними ризику, щоб уникнути однакового регуляторного навантаження на суб’єктів із різним рівнем критичності.

Третім напрямом виступає установлення процедур періодичного перегляду підзаконних вимог за результатами моніторингу загроз, аналізу інцидентів та оцінювання правозастосування. Доцільно передбачати документовані підстави перегляду, участь заінтересованих сторін і оцінювання регуляторного впливу.

Окремий напрям становить правове врегулювання застосування штучного інтелекту в аналітиці інформаційної безпеки: визначення меж автоматизації, вимог до підзвітності, перевірюваності результатів, захисту даних і людського контролю. Представлені заходи мають відповідати принципам законності, необхідності, пропорційності та гарантіям свободи вираження поглядів.

Організаційний компонент механізму забезпечує розподіл компетенцій, координацію дій і обмін інформацією. Його вдосконалення доцільно спрямувати передусім на якість управлінських процесів у межах повноважень, уже визначених законодавством, а не на створення додаткових органів без доведеної потреби.

Пропонується запровадити функціональне картування відповідальності за ключовими процесами: прогнозування загроз, оцінювання ризиків, попередження інцидентів, міжвідомче реагування, відновлення систем і аналіз результатів. Для кожного процесу слід визначити відповідального виконавця, учасників погодження, інформаційні потоки, строки та порядок ескалації.

Доцільно розробляти стандартизовані міжвідомчі протоколи повідомлення про загрози й координації реагування. При цьому процедури мають відрізнятися для кіберінцидентів, дезінформаційних кампаній, порушень захисту персональних даних та інших загроз, оскільки їх правовий режим і коло компетентних суб’єктів не тотожні.

Практично значущими є регулярні спільні навчання, сценарне моделювання комплексних криз та аналіз дій після інцидентів. Результати таких перевірок повинні не залишатися звітними показниками, а спричиняти коригування протоколів, підготовки персоналу та ресурсних пріоритетів.

Для міжсекторальної взаємодії з операторами критичної інфраструктури, бізнесом, науковими установами й громадянським суспільством необхідно визначати правила інформаційного обміну, обмеження доступу до чутливих даних та механізми підзвітності.

Технологічний компонент механізму охоплює практичне виявлення, запобігання, локалізацію й нейтралізацію загроз, а також резервування та відновлення інформаційних ресурсів. У межах публічного управління акцент слід робити на управлінні застосуванням технологій, а не на конструюванні окремих технічних засобів.

Пропонується запровадити ризик-орієнтоване планування захисту державних інформаційних систем із попередньою класифікацією їх критичності, визначенням допустимих наслідків простою та пріоритетів відновлення, і тоді це дозволить обґрунтовувати черговість заходів, а не розподіляти ресурси за формальним принципом.

Результати технічного моніторингу мають бути інтегровані з управлінським оцінюванням ризиків: для критичних сигналів слід визначити процедури перевірки, передачі компетентному суб’єкту та прийняття рішення. Доцільно встановлювати показники часу виявлення, реагування і відновлення, але цільові значення визначати лише після встановлення базового рівня.

Необхідно регулярно перевіряти резервування, плани безперервності та відновлення, зокрема шляхом навчань і тестування, де показником результативності має бути не лише наявність документа або резервної копії, а доведена спроможність відновити критично важливу послугу.

Застосування штучного інтелекту для виявлення аномалій і підтримки аналітики може розглядатися як допоміжний інструмент за умови перевірки точності, контролю хибних спрацювань, захисту інформації та збереження людської відповідальності за управлінські рішення.

Механізм кадрово-компетентнісного забезпечення формує професійні компетентності та науково-аналітичний потенціал, необхідні для реалізації регуляторних рішень. Його вдосконалення слід пов’язувати з конкретними функціями органів і результатами оцінювання кадрових потреб.

Пропонується здійснювати регулярне прогнозування дефіциту компетентностей за функціональними напрямами: управління ризиками, кіберзахист, правове забезпечення, стратегічні комунікації, захист даних та аналітика інформаційних загроз. Відповідні результати мають визначати пріоритети підготовки й перепідготовки.

Програми безперервного професійного розвитку доцільно диференціювати для керівників, аналітиків, технічних фахівців та осіб, відповідальних за комунікації. Результативність навчання необхідно перевіряти практичними завданнями, сценарними вправами й оцінюванням застосування навичок на робочому місці.

Окремої уваги потребує співпраця державних органів, закладів вищої освіти, наукових установ і технологічного сектору через спільні дослідницькі програми, експертизу регуляторних рішень та апробацію методик прогнозування ризиків. Науковий супровід має бути інтегрований у підготовку й оцінювання управлінських рішень, а не обмежуватися епізодичними консультаціями.

Економічний компонент комплексного механізму забезпечує фінансові, матеріально-технічні та інвестиційні умови реалізації заходів інформаційної безпеки. В умовах бюджетних обмежень його вдосконалення повинно орієнтуватися на обґрунтування пріоритетів і вимірюваність результатів.

Пропонується застосовувати ризик-орієнтоване планування видатків: першочергове фінансування спрямовувати на системи з високою критичністю, значними потенційними наслідками інцидентів і підтвердженими прогалинами захисту. Рішення мають ґрунтуватися на порівнянні очікуваного зниження ризику та повної вартості заходу.

У межах програмно-цільового планування фінансування доцільно пов’язувати з показниками готовності до реагування, безперервності функціонування та виконання планів зниження ризиків, а не лише з кількістю закуплених засобів.

Залучення приватних інвестицій, міжнародної технічної допомоги й механізмів державно-приватної взаємодії слід здійснювати відповідно до законодавства та з урахуванням режиму доступу до інформації, вимог безпеки й

розподілу відповідальності.

Окремий напрям тут чітко вказує на підтримку науково-технологічних розробок у сфері захищених комунікацій, моніторингу, аналітики та відновлення інформаційних систем за прозорими критеріями відбору, практичної придатності й результативності.

Порівняння практичних рекомендацій показує, що кожен механізм має власні інструменти, проте результативність залежить від їх синхронізації. Правові вимоги потребують відповідальних виконавців і ресурсів; технічний моніторинг має впливати на управлінські пріоритети; навчання персоналу повинно відповідати ризикам, виявленим у реальній практиці.

Запропонований комплексний підхід вдосконалення механізму державного регулювання інформаційної безпеки передбачає шість послідовних етапів: (1) виявлення та оцінювання інформаційних загроз і міжсекторальних наслідків; (2) визначення регуляторних пріоритетів; (3) планування заходів, відповідальності й ресурсів; (4) узгодження використання інструментів кожного з механізмів; (5) моніторинг виконання й оцінювання результативності; (6) коригування управлінських рішень. Ці етапи мають циклічний характер: результати оцінювання формують підстави для нового перегляду ризиків і пріоритетів. Ця циклічна модель перегукується з превентивно-адаптивною моделлю державного регулювання інформаційної безпеки, представленою у Розділі 1 цього дисертаційного дослідження. Превентивно-адаптивна модель акцентує увагу на безперервності управлінського циклу державного регулювання інформаційної безпеки та пояснює логіку адаптивного регулювання, а запропонований тут цикл вдосконалення механізму відображає практичний порядок узгодженого застосування його інструментів. У такий спосіб державне регулювання набуває здатності не лише реагувати на наявні інформаційні загрози, а й адаптуватися до постійної зміни умов їх формування, послідовно застосовуючи наявні механізми.

Практична реалізація запропонованих шляхів удосконалення механізмів державного регулювання інформаційної безпеки України потребує формування узгодженої системи управлінських заходів, орієнтованих не лише на усунення

наявних недоліків функціонування відповідних механізмів, а й на створення передумов для своєчасного реагування на нові інформаційні загрози, зумовлені сучасними цивілізаційними трансформаціями. При цьому особливого значення набуває забезпечення взаємозв'язку між стратегічними пріоритетами державної політики, інституційними можливостями уповноважених суб'єктів, ресурсним забезпеченням та фактичними результатами реалізації регуляторних рішень.

З огляду на це доцільно обґрунтувати комплекс практичних рекомендацій, спрямованих на вдосконалення політичного, нормативно-правового, організаційного, інформаційно-цифрового (технологічного), економічного та мотиваційного компонентів комплексного механізму державного регулювання інформаційної безпеки. Запропоновані рекомендації мають взаємодоповнювальний характер, оскільки реалізація заходів у межах одного компонента механізму без відповідних змін в інших складових системи може обмежувати їх загальну результативність.

Зокрема, удосконалення нормативно-правової складової механізму має супроводжуватися організаційним забезпеченням виконання нових регуляторних вимог, підготовкою відповідних фахівців і залученням необхідних фінансових ресурсів. Аналогічно модернізація інформаційно-цифрового (технологічного) компоненту захисту інформації потребує встановлення процедур їх застосування, розмежування відповідальності між суб'єктами та запровадження механізмів контролю за результативністю відповідних заходів.

Тут основним принципом формування практичних рекомендацій пропонується визначити функціональну узгодженість механізмів, які складають зміст кожного з компонентів системи державного регулювання інформаційної безпеки, відповідно до якої кожен запропонований захід повинен мати чітко визначену управлінську мету, відповідальних суб'єктів, необхідні ресурси, очікуваний результат та показники його досягнення.

Особливу увагу доцільно приділити ризик-орієнтованому визначенню пріоритетності практичних заходів. За умов обмеженості фінансових, кадрових і технологічних ресурсів одночасна реалізація всіх можливих напрямів удосконалення може виявитися недостатньо ефективною. Тому першочергового

значення мають набувати заходи, спрямовані на зниження найбільш критичних інформаційних ризиків, забезпечення безперервності функціонування державних інформаційних ресурсів, підвищення готовності до комплексних інформаційних впливів і запобігання міжсекторальним наслідкам реалізації загроз.

На основі проведеного дослідження систематизовано практичні напрями вдосконалення механізму державного регулювання інформаційної безпеки України, визначено зміст рекомендованих управлінських заходів та очікувані результати їх реалізації.

Зважаючи на запропонований комплексний механізм державного регулювання інформаційної безпеки, розроблені практичні рекомендації щодо його вдосконалення вважаємо за потрібне розглянути окремими блоками, у відповідності до кожного з компонентів цього механізму.

У табл. 3.3 наведено практичні рекомендації для вдосконалення нормативно-правового компоненту, який забезпечує юридичне закріплення відповідних управлінських рішень, усунення регуляторних неузгодженостей, запровадження ризик-орієнтованих вимог і своєчасне оновлення правового регулювання.

Таблиця 3.3

Практичні рекомендації щодо вдосконалення нормативно-правового компоненту комплексного механізму державного регулювання інформаційної безпеки України

Компонент	Механізми	Рекомендовані заходи	Очікуваний результат
Нормативно-правовий компонент	Встановлення законних правил, норм, регулятивно-правових актів, стандартів і гарантій	Провести правовий аудит, усунути неузгодженості, визначити ризик-орієнтовані вимоги, проводити регулярний перегляд актів	Узгодженість та адаптивність регулювання

Джерело: власна розробка автора

Як зазначено у табл. 3.3., вдосконалення нормативно-правового компоненту механізму державного регулювання інформаційної безпеки передбачає проведення правового аудиту з метою узгодження понятійного

апарату нормативно-правової бази, приведення її у відповідність до тих ризиків та викликів, що зумовлені сучасними процесами невизначеного світу. Органи державного управління повинні проводити моніторинг інформаційних загроз та викликів та оперативно реагувати на них, створюючи адекватні норми та закони.

Кожен з компонентів комплексного механізму потребує власного регулювання. Так, політичний компонент визначає стратегічну спрямованість державної політики у сфері інформаційної безпеки та передбачає узгодження державних пріоритетів, розвиток кібердипломатії, міжнародної інтеграції й забезпечення балансу між безпековими потребами та суспільними гарантіями. Його провідними механізмами виступають механізм акумуляції та вираження політичної волі, механізм стратегічного планування та цілепокладання, механізм мережевої кібердипломатії, механізм міжнародної інтеграції. Пропозиції щодо їх вдосконалення наведено у табл. 3.4.

Таблиця 3.4

Практичні рекомендації щодо вдосконалення політичного компоненту комплексного механізму державного регулювання інформаційної безпеки України

Компонент	Механізми	Рекомендовані заходи	Очікуваний результат
Політичний компонент	Механізм акумуляції та вираження політичної волі	Формалізувати міжвідомче погодження стратегічних пріоритетів, проводити щорічний огляд ключових інформаційних ризиків на рівні державної політики.	Послідовність державних пріоритетів та узгодженість політичних і управлінських рішень.
	Механізм стратегічного планування та цілепокладання	Установити вимірювані цілі, відповідальних виконавців, строки й індикатори, передбачити періодичне коригування планів за результатами оцінювання ризиків.	Перехід до планування за результатами та своєчасне оновлення безпекових пріоритетів.
	Механізм мережевої кібердипломатії	Розвивати захищені канали обміну даними про кіберзагрози з міжнародними партнерами, узгоджувати формати сповіщення та спільні навчання.	Оперативніший міжнародний обмін попередженнями та посилення спроможності протидії транскордонним загрозам; підсилення інформаційного суверенітету.

Продовження табл. 3.4

Компонент	Механізми	Рекомендовані заходи	Очікуваний результат
Політичний компонент	Механізм міжнародної інтеграції	Визначати пріоритети наближення до стандартів ЄС і співпраці з НАТО, оцінювати сумісність процедур та інтегрувати перевірені практики з урахуванням умов України.	Підвищення сумісності національних практик з міжнародними підходами без механічного запозичення.
	Механізм балансування та дотримання суспільних гарантій	Запроваджувати оцінку пропорційності обмежень, консультації із заінтересованими сторонами та перевірку впливу регуляторних рішень на права людини.	Баланс між безпековими потребами, свободою вираження поглядів і захистом персональних даних.

Джерело: власна розробка автора

Політичний компонент комплексного механізму державного регулювання інформаційної безпеки передбачає, що рішення у цій сфері сприятимуть визначенню стратегічних цілей та завдань держави, розробці окремих напрямів політичної діяльності, забезпечать сталість демократичного режиму та дотримання демократичних принципів, як то доступ до публічної інформації, захист особистісних свобод тощо.

Організаційний компонент спрямований на вдосконалення розподілу повноважень, міжвідомчої координації, стандартизації управлінських процедур, кадрового забезпечення та оперативного реагування на кризові ситуації (табл. 3.5).

Таблиця 3.5

Практичні рекомендації щодо вдосконалення організаційного компоненту комплексного механізму державного регулювання інформаційної безпеки України

Компонент	Механізми	Рекомендовані заходи	Очікуваний результат
Організаційний компонент	Механізм розподілу функцій та субординації	Скласти матрицю функцій і відповідальності, визначити головного координатора, учасників та порядок ескалації для кожного типу загроз.	Усунення дублювання функцій і невизначеності відповідальності.

Продовження табл. 3.5

Компонент	Механізми	Рекомендовані заходи	Очікуваний результат
Організаційний компонент	Механізм міжвідомчої, мережевої та міжнародної взаємодії	Уніфікувати протоколи сповіщення та інформаційного обміну, проводити спільні міжвідомчі й міжсекторальні навчання.	Швидша координація та зменшення затримок під час реагування.
	Механізм регламентації та стандартизації управлінських процедур	Затвердити типові алгоритми оцінювання ризиків, реагування, звітування та перегляду рішень, передбачити регулярне тестування процедур.	Передбачуваність управлінських дій і порівнюваність результатів їх виконання.
	Механізм ситуаційного управління та забезпечення оперативної стійкості	Розробити сценарні плани для комплексних інцидентів, перевіряти резервні канали управління та процедури безперервності послуг.	Підвищення готовності органів влади до кризових ситуацій.
	Механізм кадрово-компетентнісного забезпечення та оцінки готовності	Визначити профілі компетентностей, проводити оцінювання готовності персоналу й цільові тренування за результатами виявлених прогалин.	Зменшення кадрових дефіцитів і підвищення професійної готовності.
	Механізм децентралізації прийняття оперативних рішень	Установити межі делегованих повноважень і критерії оперативного рішення, забезпечити документування та подальший контроль.	Скорочення часу реагування зі збереженням підзвітності.
	Механізм постійного автоматизованого моніторингу захищеності	Визначити вимоги до безперервного моніторингу, пороги ескалації та порядок передавання технічних індикаторів управлінським суб’єктам.	Раннє виявлення критичних відхилень і своєчасне ухвалення рішень.

Джерело: власна розробка автора

Інформаційно-цифровий (технологічний) компонент передбачає розвиток цифровізації управлінських процесів, технічного моніторингу, захисту

інформаційних ресурсів і механізмів публічної підзвітності з урахуванням вимог інформаційної безпеки. Його вдосконалення зачепить, передусім, технологічну складову інформаційної безпеки, яка дозволить оптимізувати та підвищити рівень державного управління у цій сфері (табл. 3.6).

Таблиця 3.6

Практичні рекомендації щодо вдосконалення інформаційно-цифрового (технологічного) компоненту комплексного механізму державного регулювання інформаційної безпеки

Компонент	Механізми	Рекомендовані заходи	Очікуваний результат
Інформаційно-цифровий (технологічний) компонент	Механізм цифровізації та автоматизації управлінських процесів (e-governance)	Автоматизувати маршрути погодження, облік інцидентів і контроль виконання рішень, запровадити рольовий доступ та журналювання дій.	Зменшення управлінських затримок і підвищення простежуваності рішень.
	Механізм технічного моніторингу та ситуаційного управління	Узгодити технічні індикатори з управлінськими рівнями ризику, встановити порядок передавання сигналів і перевірки реагування.	Перетворення результатів моніторингу на своєчасні регуляторні дії.
	Механізм відкритих даних та публічного аудит-моніторингу	Оприлюднювати безпечні для розкриття агреговані показники, запровадити публічну звітність і незалежний перегляд процедур без розголошення чутливих даних.	Прозорість та суспільна підзвітність без створення додаткових вразливостей.
	Механізм криптографічного, апаратно-програмного та периметрового захисту	Проводити ризик-орієнтовані перевірки захисту, тестування резервування й відновлення, пріоритезувати усунення критичних вразливостей.	Підвищення фактичної захищеності та безперервності роботи інформаційних систем.

Джерело: власна розробка автора

У табл. 3.7. надано практичні рекомендації для роботи з економічним компонентом комплексного механізму, який охоплює вдосконалення бюджетного фінансування, підтримку вітчизняних технологічних розробок, оцінювання доцільності інвестиційних стимулів і застосування передбачених

законодавством санкційних інструментів.

Таблиця 3.7

Практичні рекомендації щодо вдосконалення економічного компоненту комплексного механізму державного регулювання інформаційної безпеки

Компонент	Механізми	Рекомендовані заходи	Очікуваний результат
Економічний компонент	Механізми фінансово-бюджетного забезпечення та державного інвестування інформаційної сфери	Пов'язати бюджетні програми з оцінкою критичності ризиків, планами заходів і показниками результативності, передбачити аудит витрат.	Цільове фінансування пріоритетних заходів та краща результативність використання коштів.
	Механізм економічної підтримки вітчизняних розробників засобів захисту інформації	Запроваджувати прозорі конкурси прикладних розробок, пілотні закупівлі й оцінювання технологічної придатності рішень.	Розвиток вітчизняних технологій захисту та їх практичного застосування.
	Механізм запровадження пільгових ставок ПДВ, податку на прибуток або ЄСВ	Провести оцінку фіскальних наслідків і правової допустимості можливих податкових стимулів, за позитивного висновку підготувати законодавчі пропозиції.	Обґрунтовані, адресні стимули для інвестицій без необґрунтованих бюджетних втрат.
	Механізми санкціювання	Визначити прозорі підстави та процедури застосування передбачених законом санкцій, забезпечити пропорційність, оскарження і контроль виконання.	Підвищення дисципліни дотримання вимог із гарантіями законності.

Джерело: власна розробка автора

Мотиваційний компонент доповнює зазначені напрями шляхом поєднання позитивного стимулювання належних практик інформаційної безпеки із запобіжними заходами, спрямованими на підвищення відповідальності суб'єктів за дотримання встановлених вимог (табл. 3.8).

Таблиця 3.8

Практичні рекомендації щодо вдосконалення мотиваційного компоненту комплексного механізму державного регулювання інформаційної безпеки

Компонент	Механізми	Рекомендовані заходи	Очікуваний результат
Мотиваційний компонент	Стимулюючі (позитивні) механізми	Запроваджувати відзнаки за належну практику, підтримку навчання, добровільні оцінювання готовності та поширення ефективних рішень.	Посилення зацікавленості суб'єктів у запобіганні ризикам.
	Стримуючі (запобіжні) механізми	Передбачати попередження, коригувальні приписи й інші законні заходи відповідальності за порушення, застосовувати їх диференційовано за ризиком.	Зниження повторюваності порушень і підвищення дотримання вимог.

Джерело: власна розробка автора

У вищенаведених табл. 3.3., 3.4., 3.5., 3.6., 3.7., 3.8. систематизовано шляхи вдосконалення комплексного механізму державного регулювання інформаційної безпеки України, структурованого за шістьма взаємопов'язаними компонентами: політичним, нормативно-правовим, організаційним, інформаційно-цифровим (технологічним), економічним і мотиваційним. Запропонований підхід дозволяє розглядати державне регулювання інформаційної безпеки не як сукупність відокремлених управлінських заходів, а як цілісну систему взаємодоповнювальних інструментів, спрямованих на своєчасне виявлення інформаційних загроз, запобігання їх реалізації та забезпечення стійкості держави в умовах сучасних цивілізаційних викликів.

Особливістю представлених рекомендацій є їх орієнтація на конкретні управлінські результати, для кожного механізму визначено заходи, реалізація яких має сприяти підвищенню узгодженості регуляторних рішень, скороченню часу реагування на інформаційні загрози, раціональному використанню ресурсів, розвитку кадрових компетентностей і забезпеченню безперервності функціонування критично важливих інформаційних систем. Водночас досягнення зазначених результатів потребує узгодженого застосування всіх шести компонентів, оскільки ефективність окремих заходів безпосередньо

залежить від їх нормативного, організаційного, технологічного та ресурсного забезпечення.

Отже, представлені практичні рекомендації конкретизують напрями вдосконалення комплексного механізму державного регулювання інформаційної безпеки України та формують основу для його узгодженої реалізації. Їх системне застосування створює передумови для посилення превентивного й адаптивного характеру державного регулювання, підвищення результативності управлінських рішень і зміцнення стійкості національної системи інформаційної безпеки в умовах сучасних цивілізаційних викликів.

Представлені рекомендації свідчать, що вдосконалення механізмів державного регулювання інформаційної безпеки має здійснюватися не шляхом ізольованого запровадження окремих організаційних, правових або технічних заходів, а на основі їх системного поєднання. Визначальною умовою результативності такого підходу є встановлення функціональних взаємозв'язків між відповідними механізмами, за яких результати застосування одного з них стають підставою для коригування управлінських рішень у межах інших.

Узгодженість функціонування складових комплексного механізму державного регулювання інформаційної безпеки набуває особливого значення в умовах сучасних цивілізаційних викликів, які характеризуються системністю, транснаціональним характером, високою динамікою розвитку та здатністю спричиняти каскадні наслідки в різних сферах національної безпеки. За таких умов результативність державного регулювання визначається не лише наявністю відповідних політичних, нормативно-правових, організаційних, інформаційно-цифрових (технологічних), економічних і мотиваційних інструментів, а й спроможністю забезпечувати їх своєчасне, взаємоузгоджене та цілеспрямоване застосування.

Зокрема, результати моніторингу інформаційних загроз, отримані в межах інформаційно-цифрового (технологічного) компонента, повинні становити інформаційно-аналітичне підґрунтя для уточнення стратегічних пріоритетів державної політики, перегляду нормативно-правових вимог, визначення організаційних заходів та обґрунтування потреб у фінансовому забезпеченні.

Водночас механізм кадрово-компетентнісного забезпечення та оцінки готовності, що належить до організаційного компонента, має забезпечувати належний рівень професійної підготовки фахівців, розвиток управлінських компетентностей і науково-аналітичний супровід відповідних рішень.

Важливу роль у забезпеченні такої взаємодії відіграють механізми розподілу функцій та субординації, які визначають компетенцію, відповідальність і порядок підпорядкування уповноважених суб'єктів, а також механізм міжвідомчої, мережевої та міжнародної взаємодії, спрямований на координацію їхньої діяльності, налагодження інформаційного обміну та узгодження спільних заходів реагування. При цьому мотиваційний компонент сприяє формуванню належної поведінки учасників відповідних відносин шляхом поєднання стимулюючих і стримуючих інструментів.

Отже, удосконалення комплексного механізму державного регулювання інформаційної безпеки доцільно розглядати як цілеспрямований процес функціонального узгодження його структурних компонентів, за якого результати застосування одних механізмів формують інформаційні, організаційні та ресурсні передумови для реалізації інших. Вищенаведене дозволяє забезпечити перехід від переважно реактивного реагування на інформаційні загрози до превентивного й адаптивного державного регулювання, орієнтованого на прогнозування ризиків, запобігання їх реалізації та мінімізацію можливих міжсекторальних наслідків.

Важливою передумовою практичного впровадження запропонованих рекомендацій є визначення послідовності їх реалізації з урахуванням актуальності інформаційних загроз, інституційної спроможності уповноважених суб'єктів, наявного ресурсного забезпечення та очікуваних результатів. З огляду на це пропонується здійснювати вдосконалення механізмів державного регулювання інформаційної безпеки зважаючи на темпоральні характеристики дійсності: короткострокові (до одного року), середньострокові (від одного до трьох років) та довгострокові (понад три роки).

Зазначені темпоральні характеристики доцільно співвіднести з оперативним, тактичним і стратегічним рівнями реалізації управлінських

рішень. Таке співвідношення має функціональний характер, оскільки стратегічне планування, тактична координація та оперативне реагування здійснюються паралельно й взаємодоповнюють одне одного незалежно від тривалості реалізації окремих рішень.

На короткостроковому (оперативному) рівні, орієнтовною тривалістю до одного року, першочергового значення набуває здійснення заходів, спрямованих на усунення найбільш критичних недоліків у функціонуванні системи державного регулювання інформаційної безпеки, підвищення готовності до реагування на актуальні загрози та забезпечення безперервності роботи критично важливих об'єктів, дотичних до інформаційної сфери.

До пріоритетних заходів цього рівня належать проведення аналізу нормативно-правових неузгодженостей, ідентифікація найбільш критичних інформаційних ризиків, функціональне картування повноважень і відповідальності суб'єктів, перевірка готовності до реагування на інформаційні та кіберінциденти, а також визначення вихідних показників результативності відповідних управлінських процесів.

Особливістю короткострокового (оперативного) рівня має стати переважне використання чинних інституційних повноважень, наявних організаційних можливостей і ресурсів, що дозволить мінімізувати часові витрати на запровадження першочергових заходів. Водночас необхідно забезпечити належну гнучкість управлінських процедур, оперативність міжвідомчої взаємодії та можливість коригування рішень відповідно до змін безпекового середовища.

На середньостроковому (тактичному) рівні, орієнтовною тривалістю від одного до трьох років, основну увагу доцільно зосередити на комплексному вдосконаленні організаційних, нормативно-правових, технологічних і ресурсних інструментів державного регулювання інформаційної безпеки.

Реалізація зазначених заходів має передбачати вдосконалення міжвідомчих процедур координації та інформаційного обміну, запровадження стандартизованих алгоритмів реагування на різні категорії інформаційних загроз, модернізацію пріоритетних державних інформаційних систем, розвиток

програм професійної підготовки та підвищення кваліфікації фахівців, а також удосконалення механізмів фінансового забезпечення заходів інформаційної безпеки.

Окремого значення набуває впровадження регулярного оцінювання результативності управлінських рішень, що дозволяє визначати ступінь досягнення запланованих цілей, виявляти недоліки реалізації відповідних заходів та своєчасно коригувати їх зміст. У цьому контексті тактичний рівень повинен забезпечувати перехід від окремих першочергових завдань до системного вдосконалення механізмів державного регулювання.

На довгостроковому (стратегічному) рівні, тривалістю понад три роки, пріоритетним завданням має стати формування стійких інституційних, нормативно-правових, технологічних та організаційних передумов функціонування адаптивної системи державного регулювання інформаційної безпеки.

До основних напрямів цього рівня доцільно віднести інституціоналізацію результативних управлінських практик, розвиток національного науково-технологічного потенціалу, поглиблення міжнародної взаємодії, інтеграцію прогнозно-аналітичних інструментів у процеси стратегічного планування, а також формування сталої системи професійного розвитку фахівців у сфері інформаційної безпеки, наприклад, підготовка фахівців за спеціальністями «Кібербезпека та захист інформації» та «Управління інформаційною безпекою». Зазначені спеціальності не належать до галузі знань «Публічне управління та адміністрування», саме тому виникає пропозиціястворити нову спеціальність та розпочати підготовку фахівців за спеціальністю «Публічне управління інформаційною безпекою» для роботи в органах державної влади, органах місцевого самоврядування та громадському секторі у цій галузі знань.

Важливим результатом реалізації довгострокових заходів має стати підвищення спроможності держави не лише протидіяти наявним інформаційним загрозам, а й своєчасно ідентифікувати нові ризики, пов’язані з подальшим розвитком цифрових технологій, штучного інтелекту, трансформацією інформаційно-комунікаційного середовища та посиленням глобальної

взаємозалежності.

Водночас виокремлення вищезазначених рівнів має рекомендаційний характер і не передбачає жорсткого розмежування управлінських заходів у часі. В умовах виникнення критичних інформаційних загроз, істотної зміни безпекового середовища або появи нових технологічних вразливостей строки та пріоритетність реалізації відповідних заходів можуть переглядатися за результатами актуального оцінювання ризиків. Саме така гнучкість забезпечує відповідність запропонованого підходу превентивно-адаптивному характеру державного регулювання інформаційної безпеки.

Практична реалізація запропонованих напрямів удосконалення комплексного механізму державного регулювання інформаційної безпеки потребує не лише визначення змісту та послідовності управлінських заходів, а й формування належного організаційного забезпечення їх виконання. У цьому контексті особливо важливим є визначення кола уповноважених суб'єктів, розмежування їхніх функцій, установлення процедур взаємодії та запровадження системи показників, які дозволятимуть оцінювати фактичні результати використання конкретних механізмів забезпечення інформаційної безпеки.

При цьому необхідно враховувати, що державне регулювання інформаційної безпеки охоплює різні за правовою природою, функціональним призначенням та організаційним забезпеченням напрями діяльності. Відповідно, реалізація запропонованих заходів має здійснюватися із дотриманням законодавчо визначеної компетенції органів державної влади, принципів міжвідомчої координації, розмежування відповідальності та забезпечення належного інформаційного обміну.

На нашу думку, організаційне забезпечення вдосконалення комплексного механізму державного регулювання інформаційної безпеки доцільно формувати на засадах функціональної відповідності, відповідно до яких кожному напряму практичної діяльності мають відповідати визначені суб'єкти реалізації, конкретні управлінські завдання та показники оцінювання результативності.

Комплексний механізм державного регулювання інформаційної безпеки дозволить інтегрувати запропоновані у табл. 3.3-3.8 практичні рекомендації в

реальну управлінську діяльність, створити передумови для здійснення систематичного моніторингу, виявлення відхилень від запланованих результатів і своєчасного коригування управлінських рішень з метою забезпечення інформаційного суверенітету держави.

Для конкретизації організаційного забезпечення запропонованих рекомендацій систематизовано основні напрями їх реалізації, визначено потенційних суб'єктів управлінської діяльності в інформаційній сфері, критеріїв оцінювання результативності (табл. 3.9).

Таблиця 3.9

Організаційне забезпечення та показники результативності реалізації рекомендацій щодо вдосконалення комплексного механізму державного регулювання інформаційної безпеки України

Напрям	Потенційні учасники (у межах повноважень)	Показники результативності
Стратегічне планування та координація державної політики	РНБО України, КМУ, профільні міністерства та інші уповноважені органи	Ступінь виконання стратегічних завдань; узгодженість державних пріоритетів; своєчасність перегляду планів
Нормативно-правове вдосконалення	Верховна Рада України, КМУ, профільні міністерства та інші компетентні суб'єкти	Частка переглянутих нормативно-правових актів; кількість усунутих регуляторних неузгодженостей; рівень виконання встановлених вимог
Міжвідомча координація	РНБО України, НКЦК, Держспецзв'язку, інші компетентні органи	Своєчасність інформаційного обміну; результати спільних навчань; узгодженість процедур реагування
Інформаційно-цифрова та оперативно-технічна стійкість	Держспецзв'язку, CERT-UA, власники та адміністратори інформаційних систем	Час виявлення, реагування та відновлення; результати тестування систем; частка усунутих критичних вразливостей
Кадрово-компетентнісне забезпечення	Уповноважені органи державної влади, заклади вищої освіти, наукові установи	Забезпеченість кваліфікованими фахівцями; результати оцінювання компетентностей; ефективність практичних навчань
Фінансово-економічне забезпечення	КМУ, Міністерство фінансів України, головні розпорядники бюджетних коштів	Частка профінансованих пріоритетних заходів; виконання результативних показників бюджетних програм; ефективність використання ресурсів
Формування мотивації та культури інформаційної безпеки	Уповноважені державні органи, заклади освіти, громадські організації, суб'єкти господарювання	Охоплення навчальними заходами; рівень дотримання встановлених вимог; результати оцінювання практичних навичок

Джерело: власна розробка автора

На відміну від попередніх таблиць, у яких систематизовано зміст практичних рекомендацій за окремими компонентами комплексного механізму державного регулювання інформаційної безпеки, у табл. 3.9 акцентовано увагу на організаційних передумовах їх реалізації, що дозволило конкретизувати функціональні обов'язки суб'єктів, встановити взаємозв'язки між відповідними механізмами, потенційними учасниками управлінських процесів та очікуваними результатами їх діяльності.

Водночас наведений перелік суб'єктів має орієнтовний характер і не передбачає зміни чи перерозподілу законодавчо встановлених повноважень. Визначення відповідальних виконавців конкретних заходів повинно здійснюватися відповідно до чинного законодавства України, функціонального призначення відповідних органів та особливостей інформаційних загроз, на протидію яким спрямовані управлінські рішення.

Важливим елементом практичної реалізації запропонованих рекомендацій є формування системи оцінювання їх результативності, яка повинна забезпечувати об'єктивне визначення ступеня досягнення встановлених управлінських цілей та фактичного впливу відповідних заходів на стан інформаційної безпеки держави.

У сучасних умовах результативність державного регулювання інформаційної безпеки не може визначатися виключно кількістю прийнятих нормативно-правових актів, проведених міжвідомчих нарад, організованих навчань або придбаних технічних засобів. Зазначені показники характеризують передусім обсяг та інтенсивність управлінської діяльності, однак не завжди відображають її реальний вплив на зниження інформаційних ризиків, підвищення захищеності інформаційних ресурсів і забезпечення стійкості відповідних систем.

Натомість визначальне значення мають показники, які характеризують фактичні зміни у спроможності державних інституцій своєчасно виявляти інформаційні загрози, забезпечувати узгоджене реагування, запобігати виникненню критичних наслідків та відновлювати функціонування інформаційних систем після реалізованих загроз.

З огляду на це пропонується застосовувати дворівневу систему оцінювання результативності практичних заходів з удосконалення комплексного механізму державного регулювання інформаційної безпеки, яка поєднуватиме процесні та результативні показники.

Перший рівень передбачає використання процесних показників, спрямованих на оцінювання повноти, своєчасності, послідовності та якості виконання визначених управлінських заходів. До них можуть належати кількість проведених перевірок, частка переглянутих нормативно-правових актів, виконання затверджених планів, своєчасність проведення міжвідомчих навчань, рівень забезпечення кадрових потреб та дотримання встановлених процедур.

Другий рівень охоплює результативні показники, які характеризують фактичні зміни у стані захищеності інформаційних ресурсів, рівні готовності уповноважених суб'єктів до відповідного реагування, стійкості інформаційних систем, ефективності використання ресурсів та спроможності держави протидіяти інформаційним загрозам.

Принциповою відмінністю запропонованої системи є поєднання оцінювання процесу реалізації управлінських заходів із визначенням їх практичних наслідків, що дозволяє уникати ситуацій, за яких формальне виконання встановлених завдань ототожнюється з досягненням реальних безпекових результатів.

Зокрема, у межах нормативно-правового компонента процесними показниками можуть виступати частка нормативно-правових актів, щодо яких проведено оцінювання актуальності, кількість виявлених регуляторних неузгодженостей та своєчасність перегляду відповідних вимог. Водночас результативність його вдосконалення доцільно визначати за ступенем усунення правових колізій, підвищенням правової визначеності управлінських процедур і рівнем виконання встановлених нормативно-правових вимог.

Для організаційного компонента важливими процесними показниками є своєчасність інформаційного обміну, повнота визначення відповідальних суб'єктів, кількість проведених міжвідомчих навчань та виконання затверджених алгоритмів взаємодії. Результативні показники повинні

відображати фактичну спроможність уповноважених органів забезпечувати координацію дій, оперативне ухвалення рішень і безперервність управління в умовах виникнення комплексних інформаційних загроз.

Окреме місце в межах організаційного компонента посідає механізм кадрово-компетентнісного забезпечення та оцінки готовності. Його результативність доцільно оцінювати за рівнем забезпеченості критично важливих функцій кваліфікованими фахівцями, результатами перевірки професійних компетентностей, здатністю персоналу виконувати практичні завдання в умовах кризових ситуацій, а також ступенем використання науково-аналітичного потенціалу під час підготовки управлінських рішень.

У межах інформаційно-цифрового (технологічного) компонента особливого значення набувають показники часу виявлення інформаційних та кіберінцидентів, тривалості реагування, часу відновлення функціонування інформаційних систем, частки успішних перевірок резервування та рівня усунення критичних вразливостей.

При цьому оцінювання зазначених показників повинно здійснюватися з урахуванням характеру, масштабності та складності відповідних інцидентів. Зокрема, збільшення кількості виявлених інформаційних загроз не завжди свідчить про погіршення стану інформаційної безпеки, оскільки може бути наслідком удосконалення технологій моніторингу та підвищення спроможності відповідних систем до їх ідентифікації.

Для економічного компонента результативність доцільно визначати шляхом зіставлення обсягів використаних фінансових і матеріально-технічних ресурсів із фактично досягнутими результатами. Зокрема, необхідно враховувати частку профінансованих пріоритетних заходів, виконання результативних показників бюджетних програм, своєчасність реалізації відповідних проєктів та обґрунтованість витрат на зниження інформаційних ризиків.

Оцінювання політичного компонента має передбачати визначення ступеня узгодженості стратегічних пріоритетів державної політики, результативності міжнародної взаємодії, своєчасності перегляду стратегічних документів та

відповідності управлінських рішень визначеним цілям забезпечення інформаційної безпеки. Особливого значення набуває також оцінювання дотримання балансу між необхідністю протидії інформаційним загрозам та забезпеченням конституційних прав і свобод людини.

Щодо мотиваційного компонента, то його результативність доцільно визначати за рівнем дотримання встановлених вимог інформаційної безпеки, змінами в поведінці відповідних суб'єктів, ефективністю стимулюючих заходів та зменшенням повторюваності порушень. При цьому оцінювання повинно враховувати не лише кількісні показники участі у відповідних програмах, а й фактичне застосування набутих знань і навичок.

Важливою умовою практичного застосування запропонованої системи оцінювання є встановлення вихідних значень показників, визначення періодичності їх вимірювання, закріплення відповідальних суб'єктів за збирання та узагальнення інформації, а також формування процедур перевірки достовірності отриманих результатів.

Цільові значення показників доцільно встановлювати лише після оцінювання фактичного стану відповідних систем, визначення їх ресурсних можливостей та характеру інформаційних ризиків, що дозволить забезпечити обґрунтованість управлінських рішень і запобігти формальному визначенню показників, які не відображають реальних умов функціонування системи інформаційної безпеки.

Водночас запропонована система оцінювання повинна виконувати не лише контрольну, а й інформаційно-аналітичну функцію. Результати оцінювання мають використовуватися для перегляду стратегічних пріоритетів, уточнення нормативно-правових вимог, удосконалення організаційних процедур, перерозподілу ресурсів та коригування практичних заходів.

Дворівнева система оцінювання результативності дозволяє забезпечити постійний зворотний зв'язок між реалізацією управлінських заходів та фактичними змінами у стані інформаційної безпеки. Її застосування створює передумови для підвищення обґрунтованості державного регулювання та забезпечення його адаптації до нових інформаційних загроз.

Узагальнення запропонованих практичних рекомендацій, визначених темпоральних характеристик їх реалізації, організаційного забезпечення та системи оцінювання результативності дозволяє обґрунтувати необхідність їх інтеграції в межах єдиного управлінського процесу.

В основу такого процесу доцільно покласти принцип функціональної узгодженості, відповідно до якого політичний, нормативно-правовий, організаційний, інформаційно-цифровий (технологічний), економічний та мотиваційний компоненти комплексного механізму державного регулювання інформаційної безпеки повинні забезпечувати взаємопов’язане виконання відповідних управлінських завдань.

Водночас практична реалізація запропонованого підходу має ґрунтуватися на циклічності управлінських процесів, що передбачає послідовне виявлення та оцінювання інформаційних загроз, визначення регуляторних пріоритетів, планування необхідних ресурсів, реалізацію управлінських заходів, моніторинг результатів та коригування відповідних рішень. Результатом таких заходів є забезпечення постійного зворотного зв’язку між окремими етапами управлінського циклу, завдяки якому результати моніторингу та оцінювання стають підставою для перегляду пріоритетів і вдосконалення відповідних механізмів державного регулювання інформаційної безпеки.

Запропоновано комплексний підхід до узгодженої реалізації механізмів державного регулювання інформаційної безпеки, що представлено на рис. 3.3.

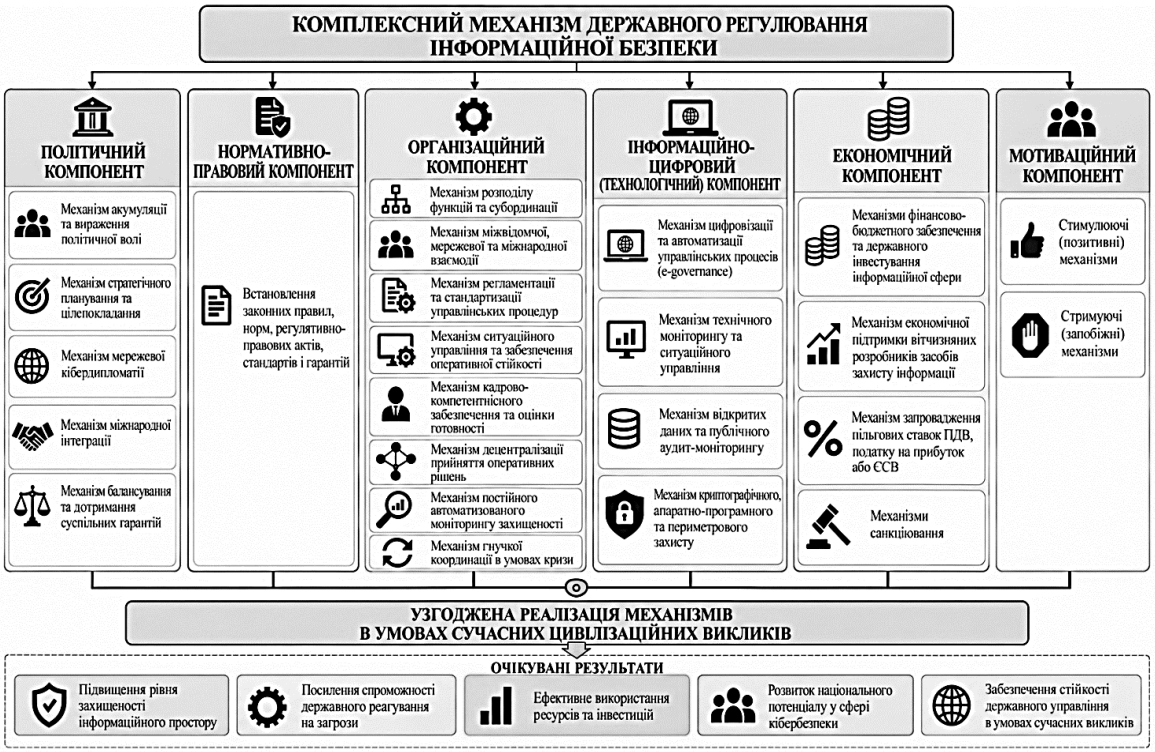

Рис. 3.3. Комплексний підхід до узгодженої реалізації механізмів державного регулювання інформаційної безпеки

Джерело: власна розробка автора

Представлений на рис. 3.3 комплексний підхід відображає перехід від структурного представлення механізмів державного регулювання інформаційної безпеки до їх практичного застосування в межах узгодженого управлінського процесу. На відміну від відокремленого використання окремих регуляторних інструментів, запропонований підхід передбачає забезпечення їх функціональної взаємодії, послідовності реалізації управлінських заходів та систематичного оцінювання отриманих результатів.

Його визначальною особливістю є поєднання структурної цілісності комплексного механізму державного регулювання інформаційної безпеки з циклічністю управлінського процесу, що дозволяє забезпечувати постійне коригування відповідних рішень залежно від змін інформаційного середовища, характеру актуальних загроз і результатів реалізації попередніх заходів.

Важливо підкреслити, що запропонований комплексний підхід не передбачає формування додаткового самостійного механізму державного регулювання інформаційної безпеки. Його призначення полягає в удосконаленні

порядку взаємоузгодженого застосування вже визначених у дисертаційному дослідженні механізмів, забезпеченні їх функціональної взаємодії та підвищенні результативності відповідних управлінських рішень.

У цьому контексті запропонований підхід конкретизує превентивно-адаптивну модель державного регулювання інформаційної безпеки, обґрунтовану в першому розділі дисертаційного дослідження. Якщо зазначена модель розкриває загальну логіку переходу до випереджального, ризик-орієнтованого та адаптивного державного регулювання, то комплексний підхід, представлений на рис. 3.3, визначає практичні організаційно-управлінські передумови реалізації відповідних положень через узгоджене використання інструментів комплексного механізму.

Отже, удосконалення механізмів державного регулювання інформаційної безпеки України в умовах сучасних цивілізаційних викликів доцільно здійснювати на основі поєднання функціональної узгодженості їх структурних компонентів, поетапної реалізації практичних рекомендацій, належного організаційного забезпечення та систематичного оцінювання результативності управлінських заходів. Реалізація запропонованого підходу створюватиме передумови для підвищення превентивності, адаптивності та стійкості системи державного регулювання інформаційної безпеки, посилення спроможності держави своєчасно реагувати на нові інформаційні загрози та мінімізувати їх негативні міжсекторальні наслідки для національної безпеки України.

Висновки до розділу 3.

За результатами дослідження зарубіжного досвіду державного регулювання інформаційної безпеки встановлено, що підходи Європейського Союзу, Сполучених Штатів Америки та НАТО характеризуються відмінностями у нормативно-правовому, інституційному та організаційно-управлінському забезпеченні, водночас мають спільну спрямованість на підвищення стійкості інформаційного середовища, управління ризиками, розвиток міжсекторальної взаємодії та забезпечення превентивного реагування на інформаційні загрози. Обґрунтовано, що використання зарубіжного досвіду в Україні має

здійснюватися не шляхом механічного запозичення окремих регуляторних інструментів, а на основі їх вибіркової адаптації до національних безпекових пріоритетів, особливостей правової системи, інституційної спроможності органів публічної влади та умов протидії сучасним цивілізаційним викликам.

На основі проведеного порівняльного аналізу запропоновано критеріально-адаптаційний підхід до використання зарубіжних механізмів державного регулювання інформаційної безпеки в Україні, який передбачає оцінювання доцільності їх застосування за шістьма взаємопов'язаними критеріями: нормативно-правовою сумісністю, інституційною спроможністю, безпековою релевантністю, ресурсною забезпеченістю, превентивністю та адаптивністю, дотриманням прав людини. Розроблено трьохетапний алгоритм адаптації зарубіжних практик, що охоплює попередню перевірку їх правової допустимості та відповідності правам людини, оцінювання управлінських і безпекових передумов застосування, а також визначення доцільного управлінського рішення щодо безпосереднього використання, адаптивної модифікації або відмови від запозичення відповідного механізму. Запропонований підхід забезпечує методичне підґрунтя для обґрунтованого вибору зарубіжних регуляторних інструментів та узгоджується з превентивно-адаптивною моделлю державного регулювання інформаційної безпеки, розробленою в першому розділі дисертації.

У результаті проведеного у підрозділі 3.2. дослідження обґрунтовано напрями вдосконалення механізмів державного регулювання інформаційної безпеки України в умовах сучасних цивілізаційних викликів, які передбачають забезпечення функціональної узгодженості структурних компонентів комплексного механізму, підвищення результативності їх практичного застосування та формування передумов для своєчасної адаптації регуляторних рішень до змін інформаційного середовища. Розроблено практичні рекомендації щодо вдосконалення політичного, нормативно-правового, організаційного, інформаційно-цифрового (технологічного), економічного та мотиваційного компонентів комплексного механізму, реалізація яких спрямована на підвищення узгодженості державної політики, усунення регуляторних

неузгодженостей, посилення міжвідомчої координації, розвиток технологічної та кадрової спроможності, раціональне використання ресурсів і формування належної мотивації суб'єктів забезпечення інформаційної безпеки.

Обґрунтовано доцільність поетапної реалізації запропонованих рекомендацій у межах короткострокового, середньострокового та довгострокового часових горизонтів, що дозволяє визначати пріоритетність управлінських заходів відповідно до характеру інформаційних загроз, рівня критичності ризиків, інституційних можливостей і наявного ресурсного забезпечення. Визначено організаційні передумови реалізації рекомендацій, зокрема потенційних учасників відповідних процесів та показники оцінювання їх результативності. Запропоновано дворівневу систему оцінювання, яка передбачає поєднання процесних показників, що характеризують виконання управлінських заходів, із результативними показниками, які відображають фактичні зміни у стані захищеності інформаційних ресурсів, готовності уповноважених суб'єктів до реагування та стійкості інформаційних систем.

На основі узагальнення зазначених положень удосконалено комплексний підхід до узгодженої реалізації механізмів державного регулювання інформаційної безпеки, визначальною особливістю якого є поєднання структурної цілісності комплексного механізму з циклічністю управлінського процесу, що охоплює виявлення й оцінювання інформаційних загроз, визначення регуляторних пріоритетів, планування ресурсів, реалізацію заходів, моніторинг результатів та коригування управлінських рішень. Запропонований підхід конкретизує превентивно-адаптивну модель державного регулювання інформаційної безпеки, обґрунтовану в першому розділі дисертації, та створює організаційно-управлінські передумови для підвищення здатності держави своєчасно реагувати на сучасні цивілізаційні виклики, запобігати реалізації інформаційних загроз і мінімізувати їх міжсекторальні наслідки для національної безпеки України.

ВИСНОВКИ

У дисертаційній роботі здійснено теоретико-методологічне обґрунтування та розроблено науково-практичні положення щодо вдосконалення державного регулювання інформаційної безпеки України в умовах сучасних цивілізаційних викликів. Результати проведеного дослідження свідчать про досягнення поставленої мети і дають підстави сформулювати такі висновки та пропозиції.

1. Результати систематизації теоретичних підходів до еволюції інформаційного суспільства дозволили встановити, що наукові уявлення про роль інформації характеризується поступовим переходом від її розуміння як засобу передавання відомостей та ресурсу економічної діяльності до визнання системоутворювальним чинником суспільного розвитку, функціонування держави та публічного управління. Еволюція концепцій постіндустріального, інформаційного, мережевого суспільства, суспільства знань та інформаційної цивілізації засвідчує послідовне розширення масштабів інформаційно-технологічних змін, які на сучасному етапі набувають глобального та цивілізаційного характеру. Визначено, що цифровізація, платформізація, алгоритмізація суспільних процесів, розвиток штучного інтелекту, перетворення даних та знань на стратегічні ресурси, а також посилення транскордонності інформаційних потоків змінюють не лише технологічні способи обробки і поширення інформації, а й характер економічних, політичних, соціальних та управлінських відносин.

2. Обґрунтовано сутність інформаційно-цифрової цивілізаційної трансформації як системного процесу якісних змін суспільних, економічних, політичних та управлінських відносин, зумовленого перетворенням інформації і знань на стратегічні ресурси розвитку, глобальним поширенням цифрових технологій, мережевих форм взаємодії та алгоритмічних систем, унаслідок чого змінюються механізми функціонування держави, суспільства та взаємодії людини з інформаційним середовищем. Запропонований підхід дає змогу розглядати сучасні інформаційно-технологічні зміни не лише в межах концепції інформаційного або цифрового суспільства, а як складову ширших

цивілізаційних трансформацій, що безпосередньо впливають на функціонування державних інститутів і систему публічного управління.

Встановлено, що інформаційно-цифрова цивілізаційна трансформація має дуалістичний характер: з одного боку, вона розширює можливості суспільного розвитку, удосконалення публічного управління, комунікації та використання знань, а з іншого – формує нові системні вразливості, пов'язані з технологічною залежністю, глобалізацією інформаційних процесів, алгоритмічним впливом, цифровою нерівністю та зростанням залежності держави і суспільства від інформаційно-цифрової інфраструктури.

3. За результатами дослідження теоретичних засад інформаційної безпеки в системі національної безпеки встановлено її комплексний і міжсекторальний характер, зумовлений наскрізною роллю інформаційних процесів у функціонуванні держави та суспільства. Обґрунтовано, що сучасний зміст інформаційної безпеки не обмежується технічним захистом інформації та кібербезпекою, а охоплює взаємопов'язані інформаційно-технологічний та інформаційно-комунікаційний виміри, включаючи захист інформації, інформаційних ресурсів та інфраструктури, забезпечення інформаційних прав та інтересів людини, суспільства і держави, а також протидію деструктивним інформаційним і психологічним впливам.

4. Розкрито сутність цивілізаційної безпеки, яку запропоновано визначати як стан захищеності та стійкості держави і суспільства, за якого забезпечується збереження їх ключових ціннісних, інституційних, інформаційних, культурних і технологічних основ, здатність адаптуватися до системних трансформацій цивілізаційного масштабу, протидіяти породженим ними загрозам та забезпечувати безперервність і перспективи сталого розвитку. Цивілізаційна безпека розуміється як окрема сфера захищеності, що дозволяє розглядати її як категорію вищого рівня узагальнення для оцінювання системних, довготривалих, взаємопов'язаних і транснаціональних трансформацій та загроз.

5. Запропоновано концептуальну модель взаємозв'язку цивілізаційної, національної та інформаційної безпеки на підставі уточнення їх співвідношення:

національна безпека визначає базову систему захисту національних інтересів держави, суспільства і людини; інформаційна безпека характеризує специфічний вимір такої захищеності в інформаційній сфері; цивілізаційна безпека формує теоретичну рамку для оцінювання трансформацій і загроз цивілізаційного масштабу. Визначено, що інформаційна безпека виступає одним із ключових функціональних вимірів забезпечення цивілізаційної стійкості держави і суспільства, оскільки одночасно виступає об'єктом захисту, стратегічним ресурсом і каналом поширення цивілізаційних трансформацій та загроз.

6. Систематизовано сучасні цивілізаційні виклики та породжені ними інформаційні загрози, визначено характер їх міжсекторального впливу на національну безпеку й обґрунтовано напрями трансформації державного регулювання інформаційної безпеки. Встановлено, що сучасні цивілізаційні виклики характеризуються масштабністю, системністю, довготривалістю, міжсекторальністю, транснаціональністю та трансформаційним впливом на базові умови функціонування держави і суспільства. На основі зазначених критеріїв здійснено систематизацію ключових цивілізаційних викликів, пов'язаних із трансформацією міжнародного порядку, глобалізацією інформаційного простору, цифровізацією та платформізацією суспільних відносин, розвитком штучного інтелекту, посиленням технологічної взаємозалежності, суспільною поляризацією, культурно-ціннісними, екологічними, демографічними та соціальними трансформаціями. Встановлено, що сучасні цивілізаційні виклики виступають не лише зовнішніми чинниками зміни безпекового середовища, а й визначальними передумовами трансформації державного регулювання інформаційної безпеки.

7. Удосконалено теоретико-методологічний підхід до визначення впливу цивілізаційних викликів на інформаційну безпеку шляхом встановлення причинно-наслідкового взаємозв'язку між цивілізаційними трансформаціями, цивілізаційними викликами, формуванням інформаційних вразливостей, виникненням інформаційних ризиків, реалізацією інформаційних загроз та їх міжсекторальними наслідками для національної безпеки. Визначено, що зазначений взаємозв'язок має динамічний і нелінійний характер, оскільки один

цивілізаційний виклик здатний породжувати сукупність взаємопов'язаних інформаційних ризиків і загроз, а їх реалізація може спричиняти каскадні наслідки для політичної, воєнної, економічної, соціальної, гуманітарної, технологічної та інших складових національної безпеки. Доведено на теоретико-методологічному рівні необхідність трансформації державного регулювання інформаційної безпеки шляхом посилення його превентивної та адаптивної спрямованості.

8. Запропоновано превентивно-адаптивну модель державного регулювання інформаційної безпеки, яка поєднує три взаємопов'язані функціональні контури: превентивно-прогностичний, регуляторно-реактивний та оціночно-адаптаційний. Визначено, що їх функціональна взаємодія забезпечує формування безперервного управлінського циклу, який охоплює моніторинг цивілізаційних трансформацій, прогнозування викликів, виявлення інформаційних вразливостей, оцінювання ризиків, превентивне регулювання, реагування на загрози, забезпечення стійкості та відновлення, оцінювання ефективності здійснених заходів і подальшу адаптацію механізмів державного регулювання. Особливістю запропонованої моделі є наявність зворотного зв'язку між результатами регуляторного впливу та вдосконаленням нормативно-правових, організаційно-інституційних, інформаційно-комунікаційних і технологічних механізмів.

Обґрунтовано доцільність розвитку державного регулювання інформаційної безпеки на засадах превентивності, адаптивності, ризик-орієнтованості, міжсекторальності та циклічності, що створює теоретико-методологічне підґрунтя для своєчасного виявлення й мінімізації інформаційних ризиків, попередження формування інформаційних загроз та підвищення спроможності держави забезпечувати інформаційну безпеку в умовах сучасних цивілізаційних викликів.

9. Досліджено нормативно-правове забезпечення регулювання інформаційної безпеки та встановлено, що його доцільно розглядати як багаторівневу, системну та динамічну конструкцію, яка забезпечує правове

закріплення засад державного управління у сфері інформаційної безпеки, кіберзахисту, визначає повноваження суб'єктів системи національної безпеки, створює надійну основу для захисту інформаційного суверенітету держави в умовах сучасних цивілізаційних викликів. Правова база інформаційної безпеки постійно трансформується під впливом появи нових кібер- та цивілізаційних загроз, технологічних рішень та спрямована на гармонізацію національного законодавства з міжнародними стандартами й нормами.

Запропоновано вдосконалити модель нормативно-правового забезпечення інформаційної безпеки в Україні, зробивши її інтерактивною, на кшталт Дії, інтегрувавши її з інформаційно-правовими системами (наприклад, «Ліга: Закон» або офіційним вебпорталом Верховної Ради України), що забезпечить автоматизоване відстеження та оперативно-структуроване розміщення нових нормативно-правових актів у фундаментальних блоках, допоможе здійснювати ефективне державне регулювання інформаційної безпеки, оскільки дозволить суб'єктам державного управління оперативно реагувати на правові трансформації, систематично актуалізуючи кожен елемент структури.

10. Проаналізовано особливості системи інституційного забезпечення державного регулювання інформаційної безпеки, яка є пріоритетним напрямом діяльності кожного з суб'єктів сучасної системи державного управління, а тому має ієрархічну архітектуру, де органи виконавчої влади розташовано за такими рівнями: стратегічний; оперативно-силовий; технологічно-інфраструктурний; зовнішній; ресурсної, макроекономічної та екологічної безпеки; соціально-демографічної стійкості; гуманітарно-освітній та когнітивний. При цьому функціонування системи інформаційної безпеки не обмежується центральним рівнем державного управління, на регіональному рівні її реалізацію гарантують територіальні органи та підрозділи; до інституційної системи забезпечення інформаційної безпеки держави потрібно віднести також наукові та науково-дослідні установи, які забезпечують науково-аналітичний та експертний супровід.

11. Обґрунтовано, що механізм державного регулювання інформаційної безпеки є складною, багаторівневою й динамічною системою, спрямованою на

захист національних інтересів, державного суверенітету та кіберстійкості в умовах цивілізаційних трансформацій. Встановлено, що ця цілісна система охоплює політичний, нормативно-правовий, організаційний, інформаційно-цифровий (технологічний), економічний і мотиваційний блоки, кожен з яких виконує чітко детерміновану функціональну роль. Детальний аналіз цих компонентів дав змогу виокремити ключові функції державного регулювання у зазначеній сфері: цільову, стимулюючу, нормативну, коригувальну, соціальну та контрольну. Доведено, що системна деструкція чи ослаблення бодай одного з елементів механізму дестабілізує весь регуляторний контур і призводить до втрати його загальної ефективності.

12. На основі узагальнення зарубіжного досвіду державного регулювання інформаційної безпеки Європейського Союзу, США та НАТО обґрунтовано необхідність вибіркової адаптації міжнародних регуляторних практик до національних безпекових та управлінських потреб України. Удосконалено критеріально-адаптаційний підхід до використання зарубіжних механізмів державного регулювання інформаційної безпеки, який, на відміну від механічного запозичення іноземних моделей, передбачає їх комплексне оцінювання за критеріями нормативно-правової сумісності, інституційної спроможності, безпекової релевантності, ресурсної забезпеченості, превентивності та адаптивності, дотримання прав людини.

13. Запропоновано трьохетапний алгоритм застосування зазначеного підходу, що дозволяє визначати правову допустимість, управлінську доцільність і спосіб адаптації відповідних механізмів до умов України. Його використання створює методичні передумови для підвищення обґрунтованості управлінських рішень, розвитку превентивного та ризик-орієнтованого державного регулювання інформаційної безпеки з урахуванням сучасних цивілізаційних викликів.

14. Обґрунтовано напрями вдосконалення механізмів державного регулювання інформаційної безпеки України в умовах сучасних цивілізаційних викликів та удосконалено комплексний підхід до їх узгодженої реалізації, який передбачає функціональну взаємодію шести структурних компонентів

комплексного механізму: політичного, нормативно-правового, організаційного, інформаційно-цифрового (технологічного), економічного та мотиваційного.

15. Розроблено практичні рекомендації щодо вдосконалення відповідних компонентів, обґрунтовано поетапність їх реалізації в межах оперативного, тактичного і стратегічного рівнів реалізації управлінських рішень, визначено організаційне забезпечення й запропоновано дворівневу систему оцінювання результативності. Доведено доцільність узгодженого застосування відповідних механізмів у межах циклічного управлінського процесу, який забезпечує взаємозв'язок між оцінюванням інформаційних загроз, визначенням регуляторних пріоритетів, реалізацією управлінських заходів, моніторингом їх результатів і подальшим коригуванням рішень, що конкретизує практичні засади реалізації превентивно-адаптивної моделі державного регулювання інформаційної безпеки та спрямовує на підвищення узгодженості, адаптивності й результативності державної політики у сфері регулювання інформаційної безпеки.

СПИСОК ВИКОРИСТАНИХ ДЖЕРЕЛ

1. Антонюк В., Миценко І. Війна в Україні як глобальний цивілізаційний конфлікт: причини та наслідки для економіки та людського розвитку. *Економіка і організація управління*. 2023. № 3(47). С. 4-17. DOI: https://doi.org/10.31558/2307-2318.2022.3.1.

2. Арістова І. В. Державна інформаційна політика: організаційно-правові аспекти : монографія / за заг. ред. О. М. Бандурки. Харків : Вид-во Ун-ту внутр. справ, 2000. 368 с.

3. Арістотель. Політика. Переклад з давньогр. О. Кислюка. К.: «Основи», 2000. 227 с.

4. Атестат відповідності КСЗІ. URL: https://vikisoft.kiev.ua/nhealth/atestat-vidpovidnosti-kszi/

5. Бебик В. М. Глобальне інформаційне суспільство: поняття, структура, комунікації. *Інформація і право*. 2011. № 1 (1). С. 41–49. DOI: https://doi.org/10.37750/2616-6798.2011.1(1).271458.

6. Боднар І. Р. Інформаційна безпека як основа національної безпеки. *Mechanism of Economic Regulation*. 2014. № 1. С. 68-75. URL: http://nbuv.gov.ua/UJRN/Mre_2014_1_8

7. Бойко В. Д., Василенко М. Д., Кухаренко С. В. Кібербезпека в ЄС та країнах-членах: генезис та проблеми її підвищення. *Інформаційна безпека людини, суспільства, держави*. 2019. № 3(27). С. 57–69. URL: https://journals.uran.ua/ispss/article/view/196117

8. Бондар М. І. Хмарні технології у публічному секторі: механізми безпекового контролю. *Електронне урядування*. 2024. Т. 8. № 1. С. 30–40

9. Вимоги до захисту інформації в інформаційних системах у воєнний час: роз’яснення Держспецзв’язку. URL: https://cip.gov.ua/ua/news/vimogi-do-zakhistu-informaciyi-v-informaciinikh-sistemakh-u-voyennii-chas-roz-yasnennya-derzhspeczv-yazku

10. Власюк О. С. Національна безпека України: еволюція проблем внутрішньої політики : вибр. наук. пр. Київ : НІСД, 2016. 528 с.

11. Воробець Н. Р. Інституційні особливості формування та

функціонування інформаційної безпеки в Україні: аналіз та перспективи розвитку. *Регіональні студії*. 2023. №34, с. 75–81 URL: http://regionalstudies.uzhnu.uz.ua/archive/34/12.pdf

12. Горбулін В. Актуальні проблеми системного забезпечення інформаційної безпеки України / В. Горбулін, М. Биченок, П. Копка. *Форми та методи забезпечення інформаційної безпеки держави* : зб. матеріалів наук.-практ. конф. (м. Київ, 13 березня 2008 р.). К. : Видавець Захаренко В. О., 2008. 216 с.

13. Дабіжа В. В., Некряч А. І. Державне регулювання інформаційної безпеки: проблеми та перспективи розвитку. *Herald of Khmelnytskyi National University*. Economic sciences. 2026. № 2. С. 84-91. DOI: https://doi.org/10.31891/2307-5740-2026-352-9.

14. Декларація принципів «Побудова інформаційного суспільства – глобальне завдання у новому тисячолітті»: Декларація Організації Об'єднаних Націй від 12.12.2003. URL: https://old.apitu.org.ua/wsis/dp

15. Державна служба спеціального зв'язку та захисту інформації України : офіційний вебпортал. URL: https://cip.gov.ua/

16. Державний науково-дослідний інститут технологій кібербезпеки та захисту інформації : вебсайт. URL: https://csi.cip.gov.ua/

17. Державний центр кіберзахисту : вебсайт. https://scpc.gov.ua/en

18. Дмитренко М. А. Системні проблеми забезпечення інформаційної безпеки України. *Інформація і право*. 2026. № 2(57), С.141-156. DOI: https://doi.org/10.37750/2616-6798.2026.2(57).364412

19. Дорошевич А. С. Гібридна війна в інформаційному суспільстві. *Вісник Національного університету «Юридична академія України імені Ярослава Мудрого*». 2015. № 2 (25). С. 21-28.

20. Дрига Д. А. Modern challenges to Ukraine's national security: a comprehensive approach to strengthening state resilience. *Modern Science: Research, Economy and Innovation* : proceedings of the 6-th International Scientific and Practical Conference. 2026. P. 162–166. DOI: https://doi.org/10.70286/ISU-02.09.2026.013.

21. Дрига Д. А. Аналіз правових механізмів забезпечення інформаційної

безпеки інформаційної інфраструктури європейського союзу. *Herald of Khmelnytskyi National University. Economic Sciences*. 2024. Вип. 334(5). С.46-51. DOI: https://doi.org/10.31891/2307-5740-2024-334-7.

22. Дрига Д. А. Державне регулювання інформаційної безпеки в Україні. *Координати державного управління*. 2026. С. 214-228. DOI: https://doi.org/10.62664/cpa.2026.01.11.

23. Дрига Д. А. Деякі актуалізовані підходи до оцінки класифікації загроз у інформаційній безпеці у сфері державного управління. *Сучасні аспекти модернізації науки в Україні: стан, проблеми, тенденції розвитку* : тези доп. V Міжнар. наук.-практ. конф. 2021. С. 32-35.

24. Дрига Д. А. Європейські підходи до державного регулювання інформаційної безпеки: сучасні механізми та перспективи імплементації в україні. *Herald of Khmelnytskyi National University. Economic Sciences*. 2026. Вип. 356(4), С.183-188. DOI: https://doi.org/10.31891/2307-5740-2026-356-25.

25. Дрига Д. А. Інформаційна безпека як складова національної безпеки в контексті досягнення цілей сталого розвитку. Цифрове наукове суспільство: соціально-економічні, правові та міжнародні аспекти : зб. наук. пр. з матеріалами VII Міжнар. наук. конф. (м. Харків, 31 лип. 2026 р.) / Міжнар. центр наук. досліджень. Вінниця : ТОВ «УКРЛОГОС Груп», 2026. С. 65–67.

26. Дрига Д. А. Інформаційна стійкість як опора національної безпеки: українська модель державного адміністрування. *Сучасний науковий журнал*. 2025. Вип. 10(4). С. 28-34. DOI : https://doi.org/10.36994/2786-9008-2025-10-3.

27. Дрига Д. А. Механізм формування важелів регулювання правових норм в умовах цифровізації. *Сучасний науковий журнал*. 2024. Вип. 3(1). С. 101-107. DOI: https://doi.org/10.36994/2786-9008-2024-3-13

28. Дрига Д. А. Особливості розуміння феномену інформаційної безпеки у сфері публічного управління. *Актуальні проблеми у сфері публічного управління*. 2023. Вип. 34. С. 108-111. DOI: https://doi.org/10.32782/pma2663-5240-2023.34.21

29. Дрига Д. А. Правовий механізм інформаційної безпеки як категорія публічного управління. *Публічне управління і адміністрування*. 2023. № 2 (80). С. 93-97. DOI: https://doi.org/10.32782/1813-3401.2023.2.17.

30. Дрига Д. А. Роль інформаційної безпеки у забезпеченні національної безпеки держави. *Актуальні питання сучасної стратегії розвитку України: виклики, пріоритети та прогнози*: тези доп. VI наук.-практ. онлайн-конф. студентів, аспірантів і молодих вчених (м. Київ, 14 трав. 2026 р.). Київ, 2026. С. 71–73. DOI: https://doi.org/10.36994/978-966-388-748-7-2026-223.

31. Дубов Д. В. Кіберпростір як новий вимір геополітичного суперництва : монографія. Київ : НІСД, 2014. 328 с.

32. Енциклопедичний словник з державного управління / уклад. : Ю. П. Сурмін, В. Д. Бакуменко, А. М. Михненко та ін. ; за ред. Ю. В. Ковбасюка, В. П. Трощинського, Ю. П. Сурміна. К. : НАДУ, 2010. 820 с. URL: https://duikt.edu.ua/uploads/l_168_62903572.pdf

33. За 4 місяці війни ІТ-армія атакувала понад 4200 російських онлайн-ресурсів : офіційне повідомлення Міністерства цифрової трансформації України. Telegram. 2022. 27 черв. URL: https://t.me/mstdigital/2645

34. Загородня А. С. Сутність та еволюція поняття «економічна безпека підприємства». *Український журнал прикладної економіки та техніки*. 2022. Том 7. № 3. С. 16-22.

35. Загородня А. С., Кулик А. В. Теоретичні засади інформаційної революції в контексті міжнародної політики та безпеки. *Modern scientific journal* (Сучасний науковий журнал). 2023. № 1(1). С. 57-63. DOI: https://doi.org/10.36994/2786-9008-2023-1-8.

36. Захаренко К. Міжнародний досвід інформаційної безпеки. Сучасне суспільство: політичні науки, соціологічні науки, культурологічні науки. 2019. №1. С.95–109. DOI: https://doi.org/10.34142/24130060.2019.17.1.09.

37. Золотар О. О. Інформаційна безпека людини: теорія і практика : монографія. Київ : Видавничий дім «АртЕк», 2018. 446 с.

38. Ісаков М. Г. Теоретичні основи державного регулювання підприємницької діяльності. *Актуальні проблеми права: теорія і практика*. Збірник наукових праць, 2012. № 23. Луганськ. URL: https://globus.ua/press/publ/item-43

39. Кадебська Е. В., Лопоха В. В. Національна безпека як правова

категорія. URL: https://www.spilnota.net.ua/ua/article/id-3144.

40. Колосовський Є. Ю., Круць Е. М. Сучасний стан кібербезпеки України в умовах воєнного періоду. *Юридичний науковий електронний журнал*. 2023. № 12. С. 402-405. URL: https://lsej.org.ua/12_2023/100.pdf

41. Конвенція про захист прав людини і основоположних свобод (з протоколами) (Європейська конвенція з прав людини): Міжнародний документ від 04.11.1950 року. URL: https://zakon.rada.gov.ua/laws/show/995_004#Text.

42. Конвенція про кіберзлочинність: Міжнародний документ від 23.11.2001 року. URL: https://zakon.rada.gov.ua/laws/show/994_575#Text.

43. Кононенко В. П, Новікова Л. В., Копицька П. О. Політика міжнародних організацій з питань інформаційної безпеки. *Науковий вісник Ужгородського національного університету.* Серія Право. 2021. № 65. Т. 1. С. 353–358. DOI: https://doi.org/10.24144/2307-3322.2021.65.64

44. Конституція України: Закон України від 28.06.1996 року № 254к/96-ВР. URL: https://zakon.rada.gov.ua/laws/show/254%D0%BA/96-%D0%B2%D1%80#Text.

45. Кормич Б. А. Інформаційна безпека: організаційно-правові основи : навч. посіб. Київ : Кондор, 2004. 384 с.

46. Кормич Б. А. Організаційно-правові засади політики інформаційної безпеки України : монографія. Одеса : Юридична література, 2003. 471 с.

47. Кормич Б. А. Організаційно-правові основи політики інформаційної безпеки України: автореф. дис. ... д-ра юрид. наук : 12.00.07. 2004. Харків. 43 с.

48. Корольов Д. С. Сучасні глобалізаційні процеси: особливості та вплив на діяльність та стабільність корпорацій. *Інвестиції практика та досвід*. 2025. № 2. С. 102–107. DOI: https://doi.org/10.32702/2306-6814.2025.2.102

49. Кохановська О. В. Інформація як нематеріальне благо та захист інформаційних прав згідно з Цивільним кодексом України. Вісник Верховного Суду України. 2005. № 11. С. 37–43.

50. Кохановська О. В. Теоретичні проблеми інформаційних відносин у цивільному праві : монографія. Київ : Київський університет, 2006. 463 с.

51. Кочубей Л. О., Некряч А. І. Державна інформаційна політика України

в умовах євроінтеграції. *Публічне управління і політика*. 2025. №4 (8). С. 2-9. DOI: https://doi.org/10.70651/3041-2498/2025.4.06.

52. Красноступ Г. М. Нова стратегія інформаційної безпеки: правова відповідь на російське інформаційне маніпулювання та втручання. *Інформація і право*. 2025. № 2(53). С. 136-146. DOI: https://doi.org/10.37750/2616-6798.2025.2(53).334149

53. Критерії і показники оцінки стану захищеності об'єктів критичної інфраструктури : Наказ Адміністрації Державної служби спеціального зв'язку та захисту інформації України. 14 січня 2025 року № 17. Документ z0376-25, чинний. URL: https://zakon.rada.gov.ua/laws/show/z0376-25#Text

54. Кукін І. В. Державне управління інформаційною безпекою особистості : монографія / І. В. Кукін [наук. ред. В. С. Нікіфоренко]. Київ : ВД «Дакор», 2023. 416 с.

55. Левченко О. В. Система забезпечення інформаційної безпеки держави у воєнній сфері: основи побудови та функціонування : монографія. Житомир : Видавець ПП «Євро-Волинь», 2021. 172 с. URL: https://sprotyvg7.com.ua/wp-content/uploads/2022/12/inform-bezpeka.pdf

56. Ліпкан В. А., Максименко Ю. Є., Желіховський В. М. Інформаційна безпека України в умовах євроінтеграції : навч. посіб. Київ : КНТ, 2006. 280 с.

57. Манокін Є. В. Сутність державного управління у сфері інформаційної безпеки органів охорони державного кордону України. *Інвестиції: практика та досвід* 2015. № 5. С. 120-126. URL: http://www.investplan.com.ua/pdf/5_2015/27.pdf

58. Марущак А. І. Дослідження проблем інформаційної безпеки у юридичній науці. *Правова інформатика*. 2010. № 3 (27). С. 17–21. URL: https://ippi.org.ua/ai-marushchak-doslidzhennya-problem-informatsiinoi-bezpeki-u-yuridichnii-nautsi

59. Міжнародний пакт про громадянські і політичні права: Міжнародний документ від 16.12.1966 року. URL: https://zakon.rada.gov.ua/laws /show/995_043#Text

60. Міністерство цифрової трансформації України. Офіційний сайт. URL:

https://thedigital.gov.ua/

61. Мохор В. В., Коробейніков Ф. О. Стійкість і резильєнтність у безпековому домені. *Реєстрація, зберігання і обробка даних*. 2024, Т. 26, № 1. С.113-120. DOI: https://doi.org/10.35681/1560-9189.2024.26.1.308655

62. Мужанова Т. М. Інформаційна безпека держави. Навчальний посібник. Київ, 2019. 131 с. URL: https://pdf.lib.vntu.edu.ua/books/2021/Muzhanova_2019_131.pdf

63. Національна стійкість України: стратегія відповіді на виклики та випередження гібридних загроз : національна доповідь / редкол.: С. І. Пирожков, О. М. Майборода, Н. В. Хамітов та ін. Київ : НАН України, 2022. URL: https://book.ipiend.gov.ua/index

64. Національний координаційний центр кібербезпеки. Український фонд безпекових досліджень. URL: https://ufss.com.ua/our-partners/natsional-nyy-koordynatsiynyy-tsentr-kiberbezpeky.html

65. Національний центр резервування державних інформаційних ресурсів / Національний репозиторій академічних текстів (NRAT). УкрІНТЕІ : вебсайт. URL: https://nrat.ukrintei.ua/naczionalnyj-czentr-rezervuvannya-derzhavnyh-informaczijnyh-resursiv/?pdf=10440

66. Некряч А. І. Державне управління використання штучного інтелекту в системі забезпечення інформаційної безпеки та підвищенні обороноздатності України. *Український журнал прикладної економіки та техніки*. 2026. Том 11. № 3. С. 331–336. DOI: https://doi.org/10.36887/2415-8453-2026-3-59

67. Некряч А. І. Резилієнтність територіальних громад в умовах воєнного стану: інноваційні механізми розвитку місцевого самоврядування в Україні. *Сучасний науковий журнал*. 2025. Вип. 10(4), С. 59–64. DOI: https://doi.org/10.36994/2786-9008-2025-10-7.

68. Некряч А. І., Кочубей Л. О. Міжнародне інформаційне співробітництво в контексті геополітичних викликів. *Координати публічного управління*. 2026. № 1 (6) С.478-493. DOI: https://doi.org/10.62664/cpa.2026.01.24.

69. Органи виконавчої влади. Урядовий портал. URL: https://www.kmu.gov.ua/catalog

70. Орлова Н. С., Яровой Т. С. Сучасні принципи та методи державної політики у сфері інформаційної безпеки. *Вісник Донецького державного університету управління*. Серія «Державне управління». 2019. № 3 (84). С. 5–14. DOI: https://doi.org/10.35340/2308-104x.2019.84-3-02

71. Оцінка стану захищеності. Державний центр кіберзахисту Держспецзв'язку : офіц. вебсайт. URL: https://scpc.gov.ua/uk/assessment

72. Панченко В. Управління інформаційною безпекою держави та підприємств: правові та організаційні аспекти. Актуальні проблеми правознавства. 2020, № 1 (21). С. 103-109. URL: https://api.dspace.wunu.edu.ua/api/core/bitstreams/4e36d332-0e27-4f6a-a46a-55347dfe4974/content

73. Пархоменко О. В. Інформація і знання: взаємозв'язок : монографія. Київ : ДІІВ, 2010. 267 с.

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

75. Перемога над фейками. Як фінські учні опановують майстерність медіаграмотності. URL: https://nus.org.ua/2020/03/04/peremoga-nad-fejkamy-yak-finski-uchni-opanovuyut-majsternist-mediagramotnosti/

76. Пирожков С. І., Хамітов Н. В. Реальна незалежність України: баланс цивілізаційної суб'єктності та національної безпеки. *Україна дипломатична*. 2021. Вип. XXII. С. 669-683. DOI: https://doi.org/10.37837/2707-7683-2021-34.

77. Пирожков С. І., Хамітов Н. В. Цивілізаційна суб'єктність України: від потенцій до нового світогляду і буття людини. Київ : Наукова думка, 2020. 255 с.

78. Питання Центру протидії дезінформації: Указ Президента України від 07.05.2021 р. № 187/2021. URL: https://zakon.rada.gov.ua/laws/show/187/2021#Text.

79. Платон. Держава. Пер. з давньогр. Д. Коваль. К.: Основи, 2000. 355 с.

80. Податковий кодекс України. Документ 2755-VI. Редакція від 31.05.2026. URL: https://zakon.rada.gov.ua/laws/show/2755-17#Text

81. Положення про Національний координаційний центр кібербезпеки. Документ 242/2016, чинний. Редакція від 16.09.2026. URL: https://zakon.rada.gov.ua/laws/show/242/2016#Text

82. Приходько В. П. Механізм державного регулювання та управління економічною безпекою. *Інвестиції: практика та досвід*. 2013. № 15. С.6-8. URL: http://www.investplan.com.ua/pdf/15_2013/3.pdf

83. Про Державну службу спеціального зв'язку та захисту інформації України : Закон України. Документ 3475-IV, чинний. Редакція від 20.04.2025. URL: https://zakon.rada.gov.ua/laws/show/3475-15#Text

84. Про державну службу. Закон України. Документ 889-VIII, чинний. Редакція від 12.04.2026. URL: https://zakon.rada.gov.ua/laws/show/889-19#Text

85. Про державну таємницю : Закон України. Документ 3855-XII, чинний. Редакція від 30.10.2024. URL: https://zakon.rada.gov.ua/laws/main/3855-12#Text

86. Про доступ до публічної інформації. Закон України. Документ 2939-VI, чинний. Редакція від 08.08.2025. https://zakon.rada.gov.ua/laws/show/2939-17#Text

87. Про електронні документи та електронний документообіг. Закон України. Відомості Верховної Ради (ВВР), 2003, № 36, ст. 275. Документ 851-IV, чинний. Редакція від 31.12.2023. URL: https://zakon.rada.gov.ua/laws/show/851-15#Text

88. Про затвердження Положення про Адміністрацію Державної служби спеціального зв'язку та захисту інформації України : Постанова Кабінету міністрів України. Документ 411-2014-п, чинний. Редакція від 26.06.2025. URL: https://zakon.rada.gov.ua/laws/show/411-2014-%D0%BF#Text

89. Про затвердження Положення про державну експертизу у сфері технічного захисту інформації. Адміністрація державної служби спеціального зв'язку та захисту інформації України. Наказ № 93. Документ z0820-07, чинний. Редакція від 19.05.2026. URL: https://zakon.rada.gov.ua/laws/show/z0820-07#Text

90. Про захист інформації в інформаційно-комунікаційних системах. Закон України. Документ 80/94-ВР, чинний. Редакція від 20.04.2025. URL: https://zakon.rada.gov.ua/laws/show/80/94-%D0%B2%D1%80#Text

91. Про захист персональних даних. Закон України. Документ 2297-VI,

чинний. Редакція від 14.06.2025. URL: https://zakon.rada.gov.ua/laws/show/2297-17#Text

92. Про інформацію : Закон України від 02.10.1992 № 2657-XII. База даних «Законодавство України». Верховна Рада України. URL: https://zakon.rada.gov.ua/go/2657-12

93. Про національну безпеку України : Закон України від 21.06.2018 № 2469-VIII. База даних «Законодавство України». Верховна Рада України. URL: https://zakon.rada.gov.ua/laws/show/2469-19

94. Про Національну програму інформатизації. Закон України. Відомості Верховної Ради (ВВР), 2023, № 51, ст.127. Документ 2807-IX, чинний, поточна редакція від 01.12.2022. URL: https://zakon.rada.gov.ua/laws/show/2807-20#Text

95. Про основні засади забезпечення кібербезпеки України Закон України. Документ 2163-VIII, чинний. Редакція від 20.04.2025. URL: https://zakon.rada.gov.ua/laws/show/2163-19#Text

96. Про Основні засади розвитку інформаційного суспільства в Україні на 2007-2015 роки : Закон України від 09.01.2007 № 537-V. Документ 537-V, чинний. URL: https://zakon.rada.gov.ua/laws/show/537-16

97. Про правотворчу діяльність. Закон України. Документ 3354-IX, чинний. Редакція від 19.04.2025. URL: https://zakon.rada.gov.ua/laws/show/3354-20#Text

98. Про Раду національної безпеки і оборони України. Закон України. Документ 183/98-ВР, чинний. Редакція від 08.03.2026. URL: https://zakon.rada.gov.ua/laws/show/183/98-%D0%B2%D1%80#Text

99. Про реалізацію експериментального проекту щодо функціонування Національного центру резервування державних інформаційних ресурсів: Постанова від 8.02.2021 р. № 94. URL: https://zakon.rada.gov.ua/laws/show/94-2021-%D0%BF#n8.

100. Про рішення Ради національної безпеки і оборони України від 14 вересня 2020 року «Про Стратегію національної безпеки України» : Указ Президента України від 14.09.2020. № 392/2020. База даних «Законодавство України». Верховна Рада України. URL:

https://zakon.rada.gov.ua/laws/show/392/2020.

101. Про рішення Ради національної безпеки і оборони України від 15 жовтня 2021 року «Про Стратегію інформаційної безпеки» : Указ Президента України від 28.12.2021 № 685/2021. База даних «Законодавство України». Верховна Рада України. URL: https://zakon.rada.gov.ua/laws/show/685/2021.

102. Про Службу безпеки України. Закон України. Документ 2229-XII, чинний. Редакція від 13.12.2025. URL: https://zakon.rada.gov.ua/laws/show/2229-12#Text

103. Про створення Центру протидії дезінформації. Рішення Ради національної безпеки і оборони України від 11 березня 2021 року. Документ n0015525-21, чинний. URL: https://zakon.rada.gov.ua/laws/show/n0015525-21#Text

104. Про стимулювання розвитку цифрової економіки в Україні. Закон України. Відомості Верховної Ради (ВВР), 2023, №№ 6-7, ст.18. Документ 1667-IX, чинний. Редакція від 28.08.2025. URL: https://zakon.rada.gov.ua/laws/show/1667-20#Text

105. Про утворення Національного центру оперативно-технічного управління мережами телекомунікацій. Розпорядження Кабінету Міністрів України від 27 березня 2019 р. № 177-р. Документ 177-2019-р, чинний. URL: https://zakon.rada.gov.ua/laws/show/177-2019-%D1%80#Text

106. Рада національної безпеки і оборони України. Офіційний вебсайт. URL: https://www.rnbo.gov.ua/

107. Резнік Н. П., Загородня А. С. Вплив цифровізації на інноваційне середовище суспільства. *Науковий журнал «Біоекономіка і аграрний бізнес»*. 2022. Том.13 №1. DOI: http://dx.doi.org/10.31548/bioeconomy13(1).2022.39-48

108. Рейтинг Кращих Компаній з Інформаційної Безпеки в Україні від Ukrainian Business Award. 2026. URL: https://uba.top/information-security-companies-in-ukraine-2/

109. Рудник Л. І. Дезінформація як прояв порушення права на доступ до інформації. *Вісник Національної академії правових наук України*. 2024. Т. 31. №3. С. 103–118. DOI: https://doi.org/10.31359/1993 0909 2024 31 3103

110. Рудник Л. І. Державне регулювання інформаційної безпеки в умовах

цифрових, кібернетичних і гібридних загроз. *Актуальні проблеми інноваційної економіки та права*. 2026. №3. 203-208 pp. DOI: https://doi.org/10.36887/2524-0455-2026-3-39

111. Рудник Л. І. Правові засади обмеження права на доступ до інформації в умовах воєнного стану. *Вісник Національного технічного університету України «Київський політехнічний інститут»*. Політологія. Соціологія. Право. 2023. №4 (60). С. 32-39. DOI : https://doi.org/10.20535/2308-5053.2023.4(60).296975

112. Семенець-Орлова І. А., Русинюк М. М. Інституційна резильєнтність органів державної влади як основа забезпечення стійкості та національної безпеки в умовах воєнного стану в Україні. *Електронне наукове видання «Публічне адміністрування та національна безпека»*, № 2 (67), 2026. С. 51-61. DOI : https://doi.org/10.25313/2617-572X-2026-2-11979.

113. Ситник Г. П. Державне управління у сфері національної безпеки (концептуальні та організаційно-правові засади): Підручник К.: НАДУ, 2012. 544 с.

114. Сіленко А. Соціально-політичні наслідки інформаційної революції. *Політичний менеджмент*. 2005. № 5 (14). С.61-74. URL: https://nbuv.gov.ua/UJRN/PoMe_2005_5_8

115. Сопільник Л. І., Микитюк М. А. Європейські стандарти в інформаційно-правовому забезпеченні електронного урядування. *Академічні візії*. Випуск 16, 2023. DOI: http://dx.doi.org/10.5281/zenodo.10077596

116. Сороківська О. А. Державне регулювання інформаційної безпеки в умовах розвитку інформаційного суспільства та сучасних воєнних загроз. Modeling the development of the economic systems. 2026. Вип. (3). С. 111–120. DOI: https://doi.org/10.31891/mdes/2026-21-14.

117. Соснін О. В. Національні інформаційні ресурси: проблеми визначення і розуміння. *Стратегічна панорама*. 2004. № 4. С. 141–146. URL: https://library.da.mfa.gov.ua/cgi-bin/irbis64r_11/cgiirbis_64.exe

118. Старостін О.Ю. Особливості забезпечення кібербезпеки в інформаційному просторі України в умовах воєнного стану. *Forum Prava*. 2025.

№ 81(1). С. 90-96. DOI: http://doi.org/10.5281/zenodo.13923457

119. Стратегія інформаційної безпеки. Документ 685/2021, чинний, поточна редакція. Прийняття від 28.12.2021. URL: https://zakon.rada.gov.ua/laws/show/685/2021#n2

120. Стратегія кібербезпеки України. Документ 447/2021, чинний. Прийняття від 26.08.2021. URL: https://zakon.rada.gov.ua/laws/show/447/2021#Text

121. Тарасенко Н. Доктрина інформаційної безпеки України в оцінках експертів. Центр досліджень соціальних комунікацій НБУВ. URL: http://nbuviap.gov.ua/index.php?option=com_content&view=article&id=2759:doktrina-informatsijnoji-bezpeki-yak-zasib-protidiji-informatsijnim-zagrozam&catid=8&Itemid=350.

122. Тихомиров О. О. Забезпечення інформаційної безпеки як функція сучасної держави : моногр. / О. О. Тихомиров ; заг. ред. Р. А. Калюжний. Центр навч.-наук. та наук.-практ. вид. НА СБ України, 2014. 196 с.

123. Управління інформаційною безпекою : навч. посіб. для здобувачів ступеня бакалавра за освіт. програмою «Системи, технології та математичні методи кібербезпеки» спец. F5 Кібербезпека та захист інформації / КПІ ім. Ігоря Сікорського; уклад.: С. О.Носок, М. В. Коломицев, І. В. Стьопочкіна. Електрон. текст. Київ: КПІ ім. Ігоря Сікорського, 2025. 88 с.

124. Федоренко Т. В., Лукацька Л. Г. Перспективи застосування штучного інтелекту в нотаріальному процесі України в умовах цифровізації. *Наукові перспективи*. Серія «Право». 2026. №3(69). С. 1330-1341. DOI: https://doi.org/10.52058/2708-7530-20263(69)-1330-1341.

125. Філіпенко Н., Харченко В., Лукашевич С. Еволюція безпекової політики Європейського союзу і контексті нових кіберзагроз: від директиви nis1 до директиви nis2 (оглядова стаття). *Пропілеї права та безпеки*. 2025. № 8. С. 34-42. DOI: https://doi.org/10.32620/pls.2025.8.03.

126. Форостовець А. С., Макєєв Д. В. Інформаційне суспільство та державна інформаційна політика: сучасні виклики і напрями розвитку. *Київський економічний науковий журнал*. 2026. Вип. 14. С. 220-225. DOI:

https://doi.org/10.32782/2786765X/2026-14-27.

127. Центр протидії дезінформації при Раді національної безпеки та оборони України. Офіційний сайт. URL: https://cpd.gov.ua.

128. Цибульник Н. Ю. Інформаційно-правова характеристика основних складових сектору безпеки держави. *Науковий вісник Ужгородського Національного Університету*. Серія ПРАВО. 2023. Випуск 80: частина 1. С. 607-612. DOI : https://doi.org/10.24144/2307-3322.2023.80.1.93

129. Цивілізаційна ідентичність українства: історія і сучасність / авт. кол.: О. Рафальський (кер.), Я. Калакура (наук. ред.), О. Калакура, М. Юрій ; НАН України, Інститут політичних і етнонаціональних досліджень ім. І. Ф. Кураса. Київ : ІПіЕНД ім. І. Ф. Кураса НАН України, 2022. 512 с.

130. Цивілізаційний вибір України: парадигма осмислення і стратегія дії: національна доповідь / редкол.: С.І. Пирожков, О.М. Майборода, Ю.Ж. Шайгородський та ін.; Інститут політичних і етнонаціональних досліджень ім. І.Ф. Кураса НАН України. К.: НАН України, 2016. 284 с.

131. Цивільний кодекс України. Документ 435-IV. Редакція від 28.06.2024. URL: https://zakon.rada.gov.ua/laws/show/435-15#Text

132. Цимбалюк В. С. Інформаційне право: визначення сутності та змісту як комплексної галузі права. *Правова інформатика*. 2005. № 2 (6). С. 5–12.

133. Цифрове десятиліття Європи: цифрові цілі до 2030 року. URL: https://commission.europa.eu/strategy-and-policy/priorities-2019-2024/europe-fitdigital-age/europes-digital-decade-digital-targets-2030_en

134. Чечель О. М. Принципи та механізм державного регулювання економіки. *Вісник АМСУ*. Серія: «Демократичне врядування». 2013. № 2 (9). С.103-111. URL: https://science.lpnu.ua/sites/default/files/journal-paper/2022/feb/26787/chechel.pdf

135. Чупрій Л. В. Цивілізаційна роль України у сучасному глобалізованому світі / Л. В. Чупрій, І. В. Богдановський, О. Г. Льовкіна. Регіональні студії. 2021. № 24. С. 170-175. URL: https://nbuv.gov.ua/UJRN/regst_2021_24_26

136. Шевчук М. О. Механізм забезпечення інформаційної безпеки фізичних осіб. *Електронне наукове видання «Аналітично-порівняльне*

правознавство». С.684-689. URL: https://dspace.uzhnu.edu.ua/bitstreams/a4bafcc5-dcae-4024-84f7-519840c641e7/download

137. Шемчук В. В. Механізм забезпечення інформаційної безпеки держави: теоретично-методологічні основи. *Філософські та методологічні проблеми права*. 2019. № 1 (17). С. 51-59. DOI: https://doi.org/10.33270/01191702.51

138. Шість років НЦУ: Голова Держспецзв'язку привітав фахівців Національного центру оперативно-технічного управління електронними комунікаційними мережами України. Державна служба спеціального зв'язку та захисту інформації України : вебсайт. URL: https://www.cip.gov.ua/ua/news/shist-rokiv-ncu-golova-derzhspeczv-yazku-privitav-fakhivciv-nacionalnogo-centru-operativno-tekhnichnogo-upravlinnya-elektronnimi-komunikaciinimi-merezhami-ukrayini

139. Як стандарт ISO/IEC 27001 допомагає розвиватися сучасному бізнесу. URL: https://my-itspecialist.com/standard-iso/iec-27001-for-business

140. Яровой Т. С. Завдання державної політики у сфері національної безпеки. *Теорія та практика державного управління*: зб. наук. пр. Харків: Вид-во ХарРІ НАДУ «Магістр». 2019. Вип. 4 (67). С. 188–196.

141. Яровой Т. С. Формування концепції громадянської безпеки держави. Вчені записки Університету «КРОК»: зб. наук. праць. Київ: *Вид-во Вищий навчальний заклад «Університет економіки та права «КРОК»*, 2018. С. 195–203.

142. Advancing responsible State behaviour in cyberspace in the context of international security : Resolution / adopted by the General Assembly on 12 December 2019 ; UN General Assembly (74th sess. : 2019–2020). Document A/RES/74/28. New York : UN, 2019. 4 p. URL: https://digitallibrary.un.org/record/3846397?utm_source=gemini&v=pdf

143. Bartelson J. Three Concepts of Globalization. Internetional sociology. 2000. № 2. Vol. 15. P. 180–196.

144. Bateson G. Steps to an Ecology of Mind: Collected Essays in Anthropology, Psychiatry, Evolution, and Epistemology. San Francisco : Chandler Publishing Company, 1972. 542 p.

145. Bell D. The Coming of Post-Industrial Society: A Venture in Social

Forecasting. New York : Basic Books, 1973. 507 p.

146. Bowden B. Civilizational Security. The Routledge Handbook of New Security Studies / ed. by J. Peter Burgess. New York : Routledge, 2010. P. 7–17. DOI: https://doi.org/10.4324/9780203859483-7.

147. Bowden B. Civilization and Its Consequences. Oxford Handbooks Online: Scholarly Research Reviews. Oxford : Oxford University Press, 2016. P. 1–13. URL: https://doi.org/10.1093/oxfordhb/9780199935307.013.30

148. Brzezinski Z. Between Two Ages: America's Role in the Technetronic Era. New York : The Viking Press, 1970. 334 p.

149. Buzan B. People, States and Fear: An Agenda for International Security Studies in the Post-Cold War Era. 2nd ed. Boulder, Colorado : Lynne Rienner Publishers, 1991. 393 p.

150. Castells M. The Information Age: Economy, Society and Culture. Vol. I: The Rise of the Network Society. Oxford : Blackwell Publishers, 1996. 556 p.

151. Castells M. The Rise of the Network Society. 2nd ed., with a new pref. Chichester : Wiley-Blackwell, 2010. 656 p. DOI: https://doi.org/10.1002/9781444319514

152. CERT-UA. Офіційний сайт. https://cert.gov.ua/

153. Cheng S. The Meaning of Information Civilization and Its Contemporary Value. Proceedings. 2017. Vol. 1, No. 3. Art. 118. DOI: https://doi.org/10.3390/IS4SI-2017-04053

154. Chmyr, Y., Nekryach, A., Kochybei, L., Dakal, A., Strelbytska, L. Postindustrial Society and Global Informational Space as Infrastructure Medium and Factor for Actualization of the State Informational. Security Contributions to Political Science, 2023, Part F1367, P. 61–73.

155. CISA. Cross-Sector Cybersecurity Performance Goals. URL: https://www.cisa.gov/cybersecurity-performance-goals

156. Communication from the Commission to the Council, the European Parliament, the European Economic and Social Committee and the Committee of the Regions – Network and Information Security: Proposal for A European Policy Approach. /* COM/2001/0298 final */. URL: https://eur-lex.europa.eu/legal-

content/EN/TXT/?uri=celex:52001DC0298#:~:text=Communication%20from%20the%20Commission%20to%20the%20Council%2C,European%20Policy%20Approach.%20%2F*%20COM%2F2001%2F0298%20final%20*%2F

157. Council Framework Decision 2005/222/JHA of 24 February 2005 on attacks against information systems: Framework decision of Council of the European Union. URL: https://eur-lex.europa.eu/legal-content/EN/ALL/?uri=celex:32005F0222.

158. Councilof Europe Conventionon Cybercrime (ETSNo.185). Budapest,23.XI.2001. URL: https://www.coe.int/en/web/conventions/full-list?module=treaty-detail&treatynum=185.

159. Cybersecurity Strategy of the European Union: An Open, Safe and Secure Cyberspace: adopted by the European Commission on 7 February 2013 / European Union. URL: https://ec.europa.eu/digital-singlemarket/ en/news/eu-cybersecurity-plan-protect-open-internetand-online-freedom-and-opportunity-cybersecurity

160. Developments in the field of information and telecommunications in the context of international security : resolution / adopted by the General Assembly. A/RES/53/70. URL: https://digitallibrary.un.org/record/265311?v=pdf

161. DigComp 2.2: The Digital Competence Framework for Citizens - With new examples of knowledge, skills and attitudes. URL: https://publications.jrc.ec.europa.eu/repository/handle/JRC128415

162. Directive (EU) 2022/2555 of 14 December 2022 (NIS2). URL: https://eur-lex.europa.eu/eli/dir/2022/2555/oj

163. Drucker P. F. Management Challenges for the 21st Century. New York : HarperBusiness, 1999. 207 p.

164. Early Computer Security Papers (1970–1985) // Proceedings of the 21st National Information Systems Security Conference (NISSC), Arlington, Virginia, October 5–8, 1998. National Institute of Standards and Technology. URL: https://csrc.nist.gov/files/pubs/conference/1998/10/08/proceedings-of-the-21st-nissc-1998/final/docs/early-cs-papers/early-cs-papers-1970-1985.pdf.

165. ENISA. ENISA Sectorial Threat Landscape – Public Administration. 2025. URL: https://www.enisa.europa.eu/publications/enisa-sectorial-threat-landscape-

public-administration

166. ENISA. ENISA Threat Landscape 2025. 2025. URL: https://www.enisa.europa.eu/publications/enisa-threat-landscape-2025

167. ENISA. ENISA Threat Landscape 2026. 22 September 2026. URL: https://www.enisa.europa.eu/topics/cyber-threats/threat-landscape

168. European Declaration on Digital Rights and Principles. URL: https://digital-strategy.ec.europa.eu/en/library/european-declaration-digital-rights-and-principles

169. Floridi L. Semantic Conceptions of Information. The Stanford Encyclopedia of Philosophy / ed. by E. N. Zalta. Stanford : Metaphysics Research Lab, Stanford University, 2005. URL: https://plato.stanford.edu/entries/information-semantic

170. Global Risks Report 2026. Global risks in-depth: anticipating tomorrow's challenges today. URL: https://www.weforum.org/publications/global-risks-report-2026/in-full/global-risks-report-2026-chapter-2.

171. Global Risks Report 2026. Key findings. URL: https://www.weforum.org/publications/global-risks-report-2026/in-full/global-risks-report-2026-key-findings

172. Global Risks Report 2026. URL: https://www.weforum.org/publications/global-risks-report-2026/digest.

173. Global Risks Report 2026/ Global Risks 2026-2036: The Age of Competition. URL: https://www.weforum.org/publications/global-risks-report-2026/in-full/global-risks-report-2026-chapter-1.

174. Global Risks Report 2026: Geopolitical and Economic Risks Rise in New Age of Competition. URL: https://www.weforum.org/media/global-risks-report-2026-geopolitical-and-economic-risks-rise-in-new-age-of-competition.

175. Guidelines for the governance of digital platforms. URL: https://www.unesco.org/en/articles/guidelines-governance-digital-platforms

176. Huntington S. P. The Clash of Civilizations? Foreign Affairs. 1993. Vol. 72, № 3. P. 22–49.

177. International Telecommunication Union. World Summit on the Information

Society: Geneva 2003 – Tunis 2005. Geneva : ITU. URL: https://www.itu.int/net/wsis.

178. International Telecommunication Union. WSIS Declaration of Principles: Building the Information Society: A Global Challenge in the New Millennium. Geneva : ITU, 2003. URL: https://www.itu.int/net/wsis/docs/geneva/official.

179. Lewicki G. Civilizational Security: Why the Russian Invasion of Ukraine Shows that 'National Security' is Not Enough to Understand Geopolitics. Comparative Civilizations Review. 2023. Vol. 89. Article 11. P. 121–140.

180. Lippmann W. U.S. Foreign Policy: Shield of the Republic. Boston : Little, Brown and Company, 1943. 177 p.

181. Luo Y. New OLI advantages in digital globalization. International Business Review. 2021. Vol. 30, no. 2. P. 101797. URL: https://doi.org/10.1016/j.ibusrev.2021.101797.

182. Machlup F. The Production and Distribution of Knowledge in the United States. Princeton, N.J. : Princeton University Press, 1962. 416 p.

183. Masuda Y. The Information Society as Post-Industrial Society. Tokyo : Institute for the Information Society, 1980. 178 p.

184. National Cybersecurity Strategy. The White House. Washington, D.C. 2023. URL: https://bidenwhitehouse.archives.gov/wp-content/uploads/2023/03/National-Cybersecurity-Strategy-2023.pdf

185. NATO. Cyber Defence. URL: https://www.nato.int/cps/en/natohq/topics_78170.htm

186. NATO. NATO's Approach to Counter Information Threats. 18 October 2024. URL: https://www.nato.int/en/about-us/official-texts-and-resources/official-texts/2024/10/18/natos-approach-to-counter-information-threats

187. NATO. Resilience and Article 3. URL: https://www.nato.int/cps/en/natohq/topics_132722.htm

188. NATO's Approach to Counter Information Threats : Public Summary. NATO, 18 October 2024. URL: https://www.nato.int/en/about-us/official-texts-and-resources/official-texts/2024/10/18/natos-approach-to-counter-information-threats.

189. NIST. The NIST Cybersecurity Framework (CSF) 2.0. 2024. DOI: https://doi.org/10.6028/NIST.CSWP.29

190. Norris P. A. Virtuous Circle. Political Communication in Postindustrial Societies. L. 2001. P. 17-18.

191. OECD. 2023 OECD Digital Government Index: Results and Key Findings. OECD Public Governance Policy Papers. 2024. No. 44. Paris : OECD Publishing. 37 p. DOI: https://doi.org/10.1787/1a89ed5e-en.

192. OECD. Facts not Fakes: Tackling Disinformation, Strengthening Information Integrity. Paris: OECD Publishing, 2024. DOI: https://doi.org/10.1787/d909ff7a-en

193. OECD. Going Digital: Shaping Policies, Improving Lives. Paris : OECD Publishing, 2019. 168 p. DOI: https://doi.org/10.1787/9789264312012-en.

194. OECD. Measuring the Digital Transformation: A Roadmap for the Future. Paris : OECD Publishing, 2019. 260 p. DOI: https://doi.org/10.1787/9789264311992-en/

195. Okinawa Charter on the Global Information Society. URL: https://g7g20-documents.org/database/document/2000-g7-japan-leaders-leaders-language-g8-communique-okinawa-2000

196. Oxford Advanced Learner's Dictionary. Security. Oxford University Press. URL: https://www.oxfordlearnersdictionaries.com/definition/english/security

197. Paulsen C., Byers R. Glossary of Key Information Security Terms. NISTIR 7298 Rev. 3. Gaithersburg, MD : National Institute of Standards and Technology, 2019. DOI: https://doi.org/10.6028/NIST.IR.7298r3.

198. Porat M. U. The Information Economy: Definition and Measurement. Washington, D.C. : U.S. Department of Commerce, Office of Telecommunications, 1977. 319 p. (Special Publication OT-SP-77-12 (1)).

199. Porat M. U. The Information Economy: Definition and Measurement. Vol. 1. Washington, D.C. : U.S. Government Printing Office, 1977. 250 p.

200. Prozorro відновлює програму Bug Bounty: як взяти участь та скільки платять. 2023. URL: https://ain.ua/2023/08/17/prozorro-vidnovlyuye-programu-bug-bounty/

201. Regulation (EU) 2022/2065 of 19 October 2022 (Digital Services Act). URL: https://eur-lex.europa.eu/eli/reg/2022/2065/oj

202. Regulation (EU) 2022/2065 of the European Parliament and of the Council of 19 October 2022 on a Single Market For Digital Services and amending Directive 2000/31/EC (Digital Services Act). URL: https://eur-lex.europa.eu/eli/reg/2022/2065

203. Regulation (EU) 2022/2065 of the European Parliament and of the Council of 19 October 2022 on a Single Market For Digital Services and amending Directive 2000/31/EC (Digital Services Act). URL: https://eur-lex.europa.eu/eli/reg/2022/2065

204. SCO, Agreement on Cooperation in the Field of International Information Security, June 16, 2009. URL: https://ccdcoe.org/sites/default/files/documents/SCO-090616-IISAgreement.pdf

205. Shannon C. E. A Mathematical Theory of Communication. Bell System Technical Journal. 1948. Vol. 27. P. 379-423, 623–656.

206. Shannon C. E. A Mathematical Theory of Communication. The Bell System Technical Journal. 1948. Vol. 27, № 3. P. 379–423. DOI: https://doi.org/10.1002/j.1538-7305.1948.tb01338.x.

207. Skrypniuk O., Falalieieva L., Chumak O., Buryk M., Rudnyk L. Safeguarding against cyber threats: legal measures for ensuring cybersecurity. Multidisciplinary Science Journal. 2024. Vol. 6. Article 2024ss0742. DOI: https://doi.org/10.31893/multiscience.2024ss0742

208. Toffler A. The Third Wave. New York : William Morrow and Company, 1980. 544 p.

209. U.S. Department of State. United States International Cyberspace & Digital Policy Strategy. URL: https://www.state.gov/united-states-international-cyberspace-and-digital-policy-strategy/

210. UNESCO. Information society. UNESCO Thesaurus. URL: https://vocabularies.unesco.org/en/

211. UNESCO. Recommendation on the Ethics of Artificial Intelligence. Paris : UNESCO, 2021. URL: https://www.unesco.org/en/legal-affairs/recommendation-ethics-artificial-intelligence

212. UNESCO. Towards Knowledge Societies: UNESCO World Report. Paris : UNESCO Publishing, 2005. 220 p.

213. Wiener N. Cybernetics or Control and Communication in the Animal and

the Machine. Cambridge, Mass. : The MIT Press, 2019. DOI: 10.7551/mitpress/11810.001.0001.

214. Wiener N. Cybernetics: Or Control and Communication in the Animal and the Machine. Paris : Hermann & Cie ; Cambridge, Mass. : The Technology Press ; New York : John Wiley & Sons, 1948. 194 p.

215. Wolfers A. “National Security” as an Ambiguous Symbol. Political Science Quarterly. 1952. Vol. 67, No. 4. P. 481–502.

216. World Economic Forum. The Global Risks Report 2026. URL: https://www.weforum.org/publications/global-risks-report-2026/

217. World Economic Forum. The Global Risks Report 2026. 21st ed. Geneva. URL: https://www.weforum.org/publications/global-risks-report-2026/in-ful

ДОДАТКИ

Додаток А

ПОСЛІДОВНІСТЬ ВПЛИВУ ЦИВІЛІЗАЦІЙНИХ ВИКЛИКІВ НА ІНФОРМАЦІЙНУ БЕЗПЕКУ ТА РОЛЬ ДЕРЖАВНОГО РЕГУЛЮВАННЯ

Джерело: розроблено автором на основі власних досліджень

Додаток Б

Взаємозв'язок сучасних цивілізаційних викликів, інформаційних вразливостей і загроз та їх міжсекторальних наслідків

Цивілізаційний виклик	Нові або посилені інформаційні вразливості	Інформаційні ризики та загрози	Міжсекторальні наслідки для національної безпеки
Трансформація міжнародного порядку та загострення геополітичного протиборства	зростання залежності держави від глобального інформаційного середовища; використання інформаційного простору як сфери міждержавного протиборства; підвищена вразливість суспільної свідомості в умовах конфлікту	дезінформація; інформаційні операції; зовнішній маніпулятивний вплив; дискредитація державних інституцій; викривлення інформації про внутрішні та міжнародні процеси	політична, воєнна, інформаційна, економічна та гуманітарна безпека
Глобалізація та транскордонність інформаційного простору	обмежені можливості держави контролювати транскордонне поширення інформації; залежність від зовнішніх інформаційних ресурсів і цифрової інфраструктури; швидкість глобального поширення контенту	транскордонне поширення дезінформації; зовнішній інформаційний вплив; втрата контролю над стратегічно значущими інформаційними потоками; поширення деструктивного контенту	інформаційна, політична, економічна, соціальна та гуманітарна безпека
Цифровізація та платформізація суспільних відносин	концентрація інформаційних потоків на глобальних цифрових платформах; алгоритмічне посередництво в доступі до інформації; залежність держави і суспільства від цифрової інфраструктури	алгоритмічне посилення маніпулятивного контенту; формування інформаційних «бульбашок»; непрозорість алгоритмічного ранжування; порушення інформаційних прав; зниження інформаційної автономії держави	інформаційна, політична, соціальна, економічна та технологічна безпека
Стрімкий розвиток штучного інтелекту та алгоритмічних систем	зниження бар'єрів для масового створення синтетичного контенту; складність встановлення автентичності інформації; непрозорість алгоритмічних рішень; залежність від автоматизованих систем	deepfake; автоматизована дезінформація; персоналізований маніпулятивний вплив; генерація неправдивого контенту; використання ШІ для масштабування інформаційних і кібероперацій	інформаційна, політична, воєнна, технологічна, економічна та соціальна безпека

Продовження Додатка Б

Цивілізаційний виклик	Нові або посилені інформаційні вразливості	Інформаційні ризики та загрози	Міжсекторальні наслідки для національної безпеки
Посилення технологічної взаємозалежності та технологічної залежності	залежність від іноземного програмного забезпечення, цифрових сервісів, хмарних технологій, критичних технологій та зовнішніх постачальників	порушення доступності інформаційних ресурсів; ризики несанкціонованого доступу до даних; зовнішній технологічний вплив; втрата контролю над критично важливими даними й інформаційними системами	технологічна, інформаційна, економічна, воєнна та енергетична безпека
Суспільна поляризація та трансформація моделей суспільної комунікації	фрагментація інформаційного простору; зниження довіри до державних інституцій та медіа; посилення емоційно орієнтованого споживання інформації	маніпулювання суспільними суперечностями; дезінформація; мова ворожнечі; радикалізація інформаційних середовищ; підрив суспільної довіри	соціальна, політична, інформаційна та гуманітарна безпека
Культурно-ціннісні та ідентифікаційні трансформації	вразливість історичної пам’яті, національної ідентичності та ціннісних орієнтирів до зовнішнього інформаційного впливу	маніпулювання історичними наративами; деструктивний вплив на національну ідентичність; інформаційне конструювання конфліктних ідентичностей; дискредитація національних цінностей	гуманітарна, інформаційна, соціальна та політична безпека
Кліматичні, екологічні та ресурсні трансформації	зростання суспільного запиту на оперативну інформацію в умовах криз; інформаційна невизначеність; залежність кризового управління від достовірності даних	дезінформація щодо причин і наслідків криз; маніпулювання екологічною проблематикою; поширення панічних повідомлень; порушення кризових комунікацій	екологічна, економічна, соціальна, енергетична та інформаційна безпека
Демографічні, міграційні та соціальні трансформації	загострення суспільних суперечностей; фрагментація інформаційних аудиторій; підвищена чутливість до маніпулювання соціальними проблемами	маніпулятивний контент щодо міграції та соціальних груп; дезінформація; розпалювання соціальної ворожнечі; інформаційне посилення суспільної поляризації	соціальна, гуманітарна, політична та інформаційна безпека

Джерело: систематизовано та сформовано автором на основі власних досліджень

Додаток В

Повноваження суб'єктів системи інституційного забезпечення інформаційної безпеки

Суб'єкт	Роль та компетенція у системі безпеки
Стратегічний рівень	
Кабінет Міністрів України	**Вища координація та нормативно-правове забезпечення**. Забезпечує проведення єдиної державної політики у сфері нацбезпеки, формування та реалізацію інформаційної політики держави, інформаційного суверенітету, фінансування програм, пов'язаних з інформаційною безпекою, спрямовує та координує роботу міністерств, інших органів виконавчої влади у цій сфері.
Оперативно-силовий рівень	
Міністерство оборони України	**Військова та воєнно-інформаційна безпека**. Забезпечує моніторинг інформаційного простору, прогнозування та виявлення інформаційних загроз національній безпеці держави у воєнній сфері; захист військової інформаційної інфраструктури; протидію воєнній дезінформації; розвиток стратегічних комунікацій; оборону держави, стримування збройної агресії.
Міністерство внутрішніх справ України	**Внутрішня безпека, кіберправопорядки та реєстри**. Забезпечує комплексну протидію інформаційно-психологічним операціям (ІПСО), кіберзлочинності та гібридним загрозам; захист публічного порядку, безпеку критичних державних баз даних/реєстрів та протидію внутрішнім інформаційно-психологічним загрозам.
Міністерство юстиції України	**Правова безпека та правовий фронт.** Здійснює юридичний захист інтересів держави у міжнародних судах, правову оцінка загроз, підготовку санкційних механізмів, захист державних реєстрів.
Технологічно-інфраструктурний рівень	
Міністерство цифрової трансформації України	**Кіберзахист, цифрова стійкість та ІТ-інфраструктура**. Формує політику у сфері цифровизації, захисту критичної інформаційної інфраструктури, координує цифрову трансформацію країни, впроваджує електронне урядування та інструменти цифрової безпеки; пропонує та впроваджує інноваційні рішення у сферах кіберзахисту й Defense-Tech; вибудовує архітектуру цифрового захисту країни; забезпечує збереження цілісності даних, впровадження AI-інструментів у сфері безпеки; розробляє стандартизовані вимоги до захисту державних реєстрів та електронних сервісів; забезпечує впровадження принципів кібергігієни та просвітництва; реалізує національні проєкти з підвищення цифрової грамотності населення, що знижує вразливість громадян до методів соціальної інженерії.
Міністерство з відновлення, інфраструктури та транспорту України	**Захист критичної інфраструктури.** Здійснює фізичний та цифровий захист об'єктів транспорту, логістики, зв'язку, захист критичних мереж перевезень та управління відбудовою; регулювання та стандартізацію муніципальних систем відеоспостереження, ситуаційних центрів та розсудливого використання інтернет-речей (IoT) для уникнення витоку даних про переміщення сил і засобів.

Суб'єкт	Роль та компетенція у системі безпеки
Зовнішній рівень	
Міністерство закордонних справ України	**Зовнішньоінформаційна та дипломатична безпека.** Забезпечує популяризацію та формування позитивного іміджу України у світових інформаційних ресурсах та національних інформаційних ресурсах іноземних держав з метою захисту її політичних, економічних та соціально-культурних інтересів, зміцнення національної безпеки і відновлення територіальної цілісності України. Проводить публічну та цифрову дипломатію, бере участь у розбудові міжнародних безпекових альянсів. Протидіє російським дезінформаційним наративам на міжнародній арені, розвиває мережу стратегічних комунікацій із партнерами щодо відповідальної поведінки держав у кіберпросторі.
Рівень ресурсної, макроекономічної та екологічної безпеки	
Міністерство фінансів України	**Фінансова та ресурсна безпека.** Забезпечує фінансування сектору оборони та безпеки, моніторинг фінансових потоків, залучення міжнародної допомоги, протидію фінансуванню тероризму.
Міністерство економіки та довкілля України	**Економічна та екологічна безпека.** Забезпечує протидію економічному тиску, релокацію підприємств, бронювання кадрів, захист від екологічного тероризму.
Міністерство енергетики України	**Енергетична безпека.** Здійснює захист та оперативне відновлення енергосистеми, протидію кібератакам на енергомережі, гарантує підтримку стійкості в умовах блекаутів; впроваджує жорсткі протоколи безпеки для автоматизованих систем управління технологічними процесами на об'єктах електроенергетики та нафтогазового комплексу; створює та координує роботу галузевих команд реагування на комп'ютерні надзвичайні події для оперативного обміну інформацією про інциденти між енергокомпаніями.
Міністерство аграрної політики та продовольства України	**Продовольча безпека.** Забезпечує продовольчу стійкість країни та світового ринку, захист логістики експорту агропродукції.
Рівень соціально-демографічної стійкості	
Міністерство у справах громад, територій та ВПО України	**Регіональна стійкість та інфо-вплив на деокуповані території.** Забезпечує соціальну адаптація ВПО, проводить інформаційну роботу з громадами на лінії зіткнення, здійснює підготовку до деокупації.
Міністерство соціальної політики, сім'ї та єдності України	**Соціальна безпека та стійкість.** Соціальний захист населення, підтримка вразливих категорій, збереження єдності суспільства та зв'язку з діаспорою.
Міністерство охорони здоров'я України	**Біобезпека та медична стійкість.** Протидіє біологічним загрозам, здійснює психологічна реабілітація громадян, забезпечує стійкість медичної системи у кризових умовах.
Міністерство у справах ветеранів України	**Соціально-психологічна безпека.** Забезпечує реінтеграцію ветеранів, запобігає дестабілізації суспільства через невирішені соціальні проблеми захисників.

Суб'єкт	Роль та компетенція у системі безпеки
Гуманітарно-освітній та когнітивний рівень	
Міністерство культури України	**Гуманітарна та когнітивна безпека.** Забезпечує формування та реалізацію державної політики у сферах інформаційної безпеки, захисту інформаційного суверенітету, культури, державної мовної політики, державного іномовлення та популяризації України у світі, а також здійснює нормативно-правове регулювання й визначає пріоритетні напрями розвитку цих сфер.
Міністерство освіти і науки України	**Академічна, наукова та когнітивна безпека.** Забезпечує протидію ворожим фейкам в освіті, здійснює патріотичне виховання, підготовку фахівців з безпеки/кібербезпеки, організовує та координує реалізацію проєктів у сфері медіаграмотності; забезпечує включення модулів із кібергігієни та академічної доброчесності до навчальних програм, здійснює підтримку університетських наукових досліджень у сфері криптографії та захисту інформації.
Міністерство молоді та спорту України	**Молодіжна стійкість.** Забезпечує протидію вербуванню молоді ворожими спецслужбами, здійснює національно-патріотичне виховання; впроваджує заходи щодо протидії дезінформації, ворожим маніпуляціям та деструктивним інформаційним впливам у молодіжному середовищі.

Створено автором на основі [69]

Додаток Г

СПИСОК ОПУБЛІКОВАНИХ ПРАЦЬ ЗДОБУВАЧА ЗА ТЕМОЮ ДИСЕРТАЦІЇ

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

1. Дрига Д. А. Правовий механізм інформаційної безпеки як категорія публічного управління. *Публічне управління і адміністрування.* 2023. № 2 (80). С. 93-97. DOI: https://doi.org/10.32782/1813-3401.2023.2.17.

2. Дрига Д.А. Особливості розуміння феномену інформаційної безпеки у сфері публічного управління. *Актуальні проблеми у сфері публічного управління.* 2023. Вип. 34. С. 108-111. DOI: https://doi.org/10.32782/pma2663-5240-2023.34.21.

3. Дрига Д.А. Аналіз правових механізмів забезпечення інформаційної безпеки інформаційної інфраструктури Європейського союзу. *Herald of Khmelnytskyi National University. Economic Sciences.* 2024. Вип. 334(5). С.46-51. DOI: https://doi.org/10.31891/2307-5740-2024-334-7.

4. Дрига Д.А. Державне регулювання інформаційної безпеки в Україні. *Координати державного управління*. 2026. № 1(6). С. 214-228. DOI: https://doi.org/10.62664/cpa.2026.01.11.

5. Дрига Д.А. Європейські підходи до державного регулювання інформаційної безпеки: сучасні механізми та перспективи імплементації в Україні. *Herald of Khmelnytskyi National University. Economic Sciences.* 2026. Вип. 356(4). С.183-188. DOI: https://doi.org/10.31891/2307-5740-2026-356-25.

Статті в інших виданнях

6. Дрига Д. А. Механізм формування важелів регулювання правових норм в умовах цифровізації. *Сучасний науковий журнал.* 2024. Вип. 3(1). С. 101-107. DOI: https://doi.org/10.36994/2786-9008-2024-3-13.

7. Дрига Д. А. Інформаційна стійкість як опора національної безпеки: українська модель державного адміністрування. *Сучасний науковий журнал*. 2025. Вип. 10(4). С. 28-34. DOI: https://doi.org/10.36994/2786-9008-2025-10-3.

Тези наукових доповідей

8. Дрига Д. А. Деякі актуалізовані підходи до оцінки класифікації загроз у інформаційній безпеці у сфері державного управління. *Сучасні аспекти модернізації науки в Україні: стан, проблеми, тенденції розвитку* : V Міжнародна науково-практична онлайн-конференція, м. Венеція, Італія, 7 січня 2021 року : тези доповіді. Венеція, 2021. С. 32-35.

9. Дрига Д. А. Роль інформаційної безпеки у забезпеченні національної безпеки держави. *Актуальні питання сучасної стратегії розвитку України: виклики, пріоритети та прогнози* : VI Науково-практична онлайн-конференція студентів, аспірантів і молодих вчених, м. Київ, 14 травня 2026 року : тези доповіді. Київ, 2026. С. 71-73.

10. Дрига Д. А. Інформаційна безпека як складова національної безпеки в контексті досягнення цілей сталого розвитку. *Цифрове наукове суспільство: соціально-економічні, правові та міжнародні аспекти* : VII Міжнародна наукова конференція, м. Харків, 31 липня 2026 року : тези доповіді. Харків, 2026. С. 65-67.

11. Dryha D. A. Modern challenges to Ukraine’s national security: a comprehensive approach to strengthening state resilience. *Modern Science: Research, Economy and Innovation* : 6th International Scientific and Practical Conference, Zagreb, Croatia, September 2-4, 2026 : conference paper. Zagreb, 2026. P. 162-166.

Додаток Д

Заклад вищої освіти
"Відкритий
міжнародний УНІВЕРСИТЕТ
розвитку людини
"УКРАЇНА"

Higher Education Institution
"Open
International UNIVERSITY
of Human Development
"UKRAINE"

Україна, 03115, м. Київ, вул. Львівська, 23, тел.: 044-409-27-69, 067-406-53-92, 067-328-28-22
e-mail: office@uu.edu.ua; viddilorgrobotu@ukr.net сайт: http://uu.edu.ua

№ 13/23-268 від 30.09.2026 р.

Довідка
про впровадження
результатів наукового дослідження у навчальний процес

видана Дризі Дмитру Андрійовичу про те, що результати його дисертаційного дослідження на здобуття наукового ступеня доктора філософії на тему «**Державне регулювання інформаційної безпеки в умовах сучасних цивілізаційних викликів**» за спеціальністю 281 «Публічне управління та адміністрування» були використані при розробці робочої програми і викладанні навчальної дисципліни «Теорія державного управління» за програмою підготовки фахівців освітнього рівня «бакалавр».

Завідувач кафедри міжнародних відносин
та політичного консалтингу
Інституту права та суспільних відносин
ЗВО «Відкритий міжнародний університет
розвитку людини «Україна»
к.пол.н., доцент **Тетяна КАДЛУБОВИЧ**

Додаток Е

Заклад вищої освіти
"Відкритий
міжнародний УНІВЕРСИТЕТ
розвитку людини
"УКРАЇНА"

Higher Education Institution
"Open
International UNIVERSITY
of Human Development
"UKRAINE"

Україна, 03115, м. Київ, вул. Львівська, 23, тел.: 044-409-27-69, 067-406-53-92, 067-328-28-22
e-mail: office@uu.edu.ua; viddilorgrobotu@ukr.net сайт: http://uu.edu.ua

№ 13/2366 від 30 вересня 2026р.

ДОВІДКА

Видана здобувачу **Дризі Дмитру Андрійовичу** про те, що він у ході виконання дисертаційної роботи на тему «**Державне регулювання інформаційної безпеки в умовах сучасних цивілізаційних викликів**» приймав участь у виконанні науково-дослідної теми кафедри міжнародних відносин та політичного консалтингу «Воєнно-стратегічний розвиток сучасної України: міжнародно-політичні виклики, державні інтереси, безпека» (№ державної реєстрації 0124U000322).

Директор Інституту права та суспільних відносин **Тетяна ФЕДОРЕНКО**

Додаток Є

Український Інститут політики
Ukrainian Institute of Politics | Украинский Институт политики

02068, м. Київ, вул.Вірменська, 6, оф. 474

Телефони: +38 063 789 32 57; +38 093 757 7565
E-mail: uiamp2012@gmail.com
http://uiamp.org.ua/

№ 519 01.10 2026р.

Довідка
про впровадження
результатів наукового дослідження у
експертно-аналітичної розробки Українського Інституту Політики

Цією довідкою підтверджується, що результати дисертаційного дослідження Дриги Дмитра Андрійовича на здобуття наукового ступеня доктора філософії на тему: «Державне регулювання інформаційної безпеки в умовах сучасних цивілізаційних викликів» за спеціальністю 281 «Публічне управління та адміністрування» були використані у практичній діяльності Аналітичного центру «Український Інститут Політики», зокрема під час розробки аналітичних матеріалів, експертних рекомендацій та проведення прикладних досліджень з питань інформаційної безпеки та державного управління.

Впровадження результатів дослідження Дриги Д. А. дозволило підвищити якість аналітичного забезпечення управлінських рішень та поглибити практичну складову навчально-методичних матеріалів у сфері державного регулювання інформаційної безпеки.

Директор
Українсько Інституту Політики **Руслан БОРТНІК**

Додаток Ж

НАЦІОНАЛЬНА
ПОЛІЦІЯ УКРАЇНИ
ДЕПАРТАМЕНТ КІБЕРПОЛІЦІЇ
Управління протидії кіберзлочинам в місті Києві
просп. Лобановського Валерія, 51, м. Київ, 03110, тел. (044) 363-19-00
kyiv@cyberpolice.gov.ua
01.10.2026 № 1325/38/100-2026
На № _____ від _____

Відкритий міжнародний університет розвитку людини "Україна"
М. Київ, вул. Львівська 23, 03115

Довідка

про впровадження результатів наукового дослідження у діяльність Управління кіберполіції

видано здобувачу наукового ступеня доктора філософії Дризі Дмитру Андрійовичу про те, що результати його дисертаційного дослідження на тему: «Державне регулювання інформаційної безпеки в умовах сучасних цивілізаційних викликів» за спеціальністю 281 «Публічне управління та адміністрування» були використані у практичній діяльності Управління кіберполіції, зокрема під час розробки аналітичних матеріалів, експертних рекомендацій та проведення прикладних досліджень з питань інформаційної безпеки та державного управління.

Практичне впровадження наукових розробок Дриги Д. А., дало змогу оптимізувати організаційно-управлінські процеси в діяльності підрозділу, підвищити якість опрацювання аналітичних матеріалів та розширити прикладний інструментарій забезпечення інформаційної безпеки.

Заступник начальника
УПК в м. Києві
ДКП НП України
полковник поліції **Юрій ЧУПРИНА**

УПРАВЛІННЯ ПРОТИДІЇ КІБЕРЗЛОЧИНАМ В МІСТІ КИЄВІ ДЕПАРТАМЕНТУ КІБЕРПОЛІЦІЇ НАЦІОНАЛЬНОЇ ПОЛІЦІЇ УКРАЇНИ
ДЛЯ ДОВІДОК