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.