МІНІСТЕРСТВО ОСВІТИ І НАУКИ УКРАЇНИ
ДЕРЖАВНЕ НЕКОМЕРЦІЙНЕ ПІДПРИЄМСТВО
ДЕРЖАВНИЙ УНІВЕРСИТЕТ
«КИЇВСЬКИЙ АВІАЦІЙНИЙ ІНСТИТУТ»

Кваліфікаційна наукова праця
на правах рукопису

КАЛЕТНІК ВАСИЛЬ ВАСИЛЬОВИЧ

УДК 342.9:351.862.4(477)

ДИСЕРТАЦІЯ

АДМІНІСТРАТИВНО-ПРАВОВИЙ МЕХАНІЗМ ЗАБЕЗПЕЧЕННЯ ІНФОРМАЦІЙНОЇ БЕЗПЕКИ УКРАЇНИ

12.00.07 – адміністративне право і процес;
фінансове право; інформаційне право
Спеціальність 081 – Право
Галузь знань 08 – Право

Подається на здобуття наукового ступеня доктора філософії
Дисертація містить результати власних досліджень. Використання ідей, результатів і текстів інших авторів мають посилання на відповідне джерело

_____ В.В. Калетнік
(підпис здобувача)

Науковий керівник: **Головко Катерина Володимирівна**,
доктор юридичних наук, професор

Київ – 2026

АНОТАЦІЯ

Калетнік В.В. **– Адміністративно-правовий механізм забезпечення інформаційної безпеки України.** – Кваліфікаційна наукова праця на правах рукопису.

Дисертація на здобуття наукового ступеня доктора філософії зі спеціальності 081 «Право». – Державне некомерційне підприємство «Державний університет «Київський авіаційний інститут»», Київ, 2026.

Дисертацію присвячено комплексному дослідженню адміністративно-правового механізму забезпечення інформаційної безпеки України в аспекті протидії зовнішньому впливу на публічне управління. Розкрито теоретико-методологічні засади, структуру та функції цього механізму, а також визначено напрями його подальшого вдосконалення.

На основі міждисциплінарного аналізу уточнено сутність інформаційної безпеки як багатовимірного феномену, що поєднує технологічні, політичні, правові, ціннісні та культурні аспекти. Визначено її місце та функціональне навантаження в системі національної безпеки держави, обґрунтовано інтегральний характер інформаційної безпеки як умови стабільності держави й суспільства. Систематизовано існуючі концептуальні підходи до трактування інформаційної безпеки: *за спільними ознаками:* системний, статичний, процесний (діяльнісний), комплексний підходи; *за трансдисциплінарною природою:* технічний, гуманітарний, нормативний, психологічний, комплексний підходи. Запропоновано, в рамках комплексного підходу, розглядати інформаційну безпеку держави як нормативно закріплений стан захищеності національного інформаційного простору, за якого забезпечується: стійкість інформаційної інфраструктури та цілісність інформаційних ресурсів; стабільність інформаційних процесів і захист прав суб’єктів інформаційних відносин; збереження національної ідентичності; реалізація національних інтересів і досягнення стратегічних цілей в

інформаційній сфері; створення умов для сталого розвитку інформаційного суспільства.

За результатами наукового осмислення сутності феномену «адміністративно-правовий механізм забезпечення інформаційної безпеки держави» виокремлено низку підходів до його розуміння: системний, структурно-функціональний, діяльнісний та комплексний. Саме з точки зору комплексного підходу запропоновано розглядати адміністративно-правовий механізм забезпечення інформаційної безпеки держави як підсистему державного управління, що через норми права, діяльність уповноважених інституцій та застосування адміністративних інструментів (дозвільних, реєстраційних, контрольних, примусових) забезпечує захист від внутрішніх і зовнішніх загроз та створює умови для сталого розвитку національного інформаційного простору. Наголошено, що така підсистема є цілісною, динамічною та інтегрує взаємопов'язані компоненти (нормативно-правовий, інституційно-координаційний, процедурно-функціональний, інформаційно-аналітичний, комунікаційно-превентивний), які функціонують у взаємодії із зовнішніми та внутрішніми факторами та умовами.

Розкрито теоретико-правову природу зовнішнього впливу на публічне управління як специфічну загрозу суверенітету публічного управління та інформаційній безпеці держави, що має опосередкований, прихований і кумулятивний характер та реалізується переважно поза межами формалізованих владно-розпорядчих процедур. Уточнено розуміння публічного управління як діяльності суб'єктів державного управління, місцевого самоврядування та інших залучених інституцій щодо формування та реалізації публічної політики в інтересах суспільства та держави. Наголошено на тому, що в структурному аспекті публічне управління є складною багаторівневою соціально-правовою системою, у межах якої поєднуються вертикальний (ієрархічний, владний) та горизонтальний (мережевий, комунікативний) виміри, взаємодія яких забезпечує ефективність управління та соціальну легітимацію управлінських рішень.

Обґрунтовано, що саме горизонтальний вимір публічного управління, який охоплює інститути громадянського суспільства, експертні, аналітичні та медійні середовища, є найбільш вразливим до зовнішнього впливу внаслідок відкритості, інклюзивності, плюралістичності та активного використання формальних і неформальних інформаційно-комунікаційних каналів. Доведено, що в сучасних умовах зовнішній вплив трансформується з форм прямого втручання у приховані механізми деформації управлінських процесів, спрямовані на спотворення інформаційного, смислового та процедурного середовища ухвалення управлінських рішень.

Запропоновано під зовнішнім впливом на публічне управління розуміти цілеспрямовану діяльність іноземного чи афілійованого з ним суб'єкта, що полягає у прихованому або позапроцесуальному втручанні у процеси формування, обігу та інтерпретації інформації, прийняття управлінських рішень чи визначення порядку денного публічної політики, з метою зміни її змісту або результатів на користь іноземних суб'єктів. Деталізовано функціональну роль адміністративно-правового механізму забезпечення інформаційної безпеки держави в частині протидії зовнішньому впливу як системи процедурних фільтрів (ідентифікації та ризик-скорингу, адміністративної перевірки, судового контролю). Наголошено на необхідності подальшої конкретизації адміністративно-правового механізму забезпечення інформаційної безпеки держави, зокрема шляхом розробки спеціалізованих процедур ідентифікації афілійованості.

У ході дослідження встановлено, що нормативно-правове забезпечення інформаційної безпеки України у частині протидії зовнішньому впливу на публічне управління характеризується фрагментарністю та концептуальною незавершеністю. Попри наявність значного масиву законодавчих і стратегічних актів у сфері національної безпеки, інформаційної політики та публічного управління, чинне правове регулювання не формує цілісної моделі реагування на опосередковані й приховані впливи на управлінські процеси та фактично ігнорує вразливості горизонтального виміру публічного управління.

Визначено, що системними обмеженнями ефективності правового регулювання є відсутність законодавчо закріпленого понятійно-категоріального апарату у сфері протидії зовнішньому впливу, застарілість окремих нормативно-правових актів, а також брак спеціалізованих реєстраційних, наглядових і контрольних механізмів, адаптованих до латентного, нефронтального характеру сучасних інформаційних загроз. Унаслідок цього нормативно-правове забезпечення набуває переважно реактивного й декларативного характеру та не забезпечує превентивного управління ризиками в системі публічного управління.

З'ясовано, що еволюція національних нормативних ініціатив у цій сфері відзначається непослідовністю та коливанням між надмірно жорсткими, потенційно репресивними моделями і формально-декларативними підходами, позбавленими ефективних механізмів імплементації. Доведено, що така нормативна нестійкість створює правову невизначеність, підвищує ризики політизації правозастосування та перешкоджає формуванню прозорої та легітимної системи протидії зовнішньому впливу. У зв'язку з цим обґрунтовано необхідність запровадження спеціального законодавчого регулювання у формі закону України «Про протидію зовнішньому впливу на публічне управління», побудованого на засадах законності, пропорційності, прозорості та судового контролю.

Систематизовано уявлення про суб'єктний склад забезпечення інформаційної безпеки України в аспекті протидії зовнішньому впливу на публічне управління та виявлено його концептуальну неузгодженість у чинних стратегічних і нормативно-правових актах. Встановлено, що значна частина наявних підходів до визначення суб'єктів забезпечення інформаційної безпеки ґрунтується на застарілих моделях, сформованих до початку повномасштабної збройної агресії російської федерації проти України, та не відображає змін архітектури загроз і появу нових інституційних акторів.

Запропоновано функціональну модель системи суб'єктів забезпечення інформаційної безпеки, побудовану як сукупність взаємопов'язаних

підсистем: стратегічно-координаційної, операційно-виконавчої, контрольно-аналітичної, гуманітарно-комунікаційної та громадсько-експертної. Обґрунтовано, що ефективність такої системи стримується відсутністю єдиного міжвідомчого алгоритму реагування на загрози, фрагментацією інформаційних ресурсів і реєстрів, недостатнім рівнем горизонтальної взаємодії між суб'єктами, низькою цифровою інтегрованістю та ризиками політизації управлінських рішень.

З метою підвищення інституційної спроможності інституційно-координаційного блоку адміністративно-правового механізму забезпечення інформаційної безпеки наголошено на необхідності створення спеціалізованого уповноваженого органу – Центру протидії зовнішньому впливу з протидії зовнішньому впливу, запровадження єдиної цифрової платформи міжвідомчого обміну даними – Системи інтегрованого моніторингу афілійованості та розвитку прозорих механізмів звітності, суспільної взаємодії й громадського контролю як чинників підвищення довіри до державної політики у сфері інформаційної безпеки.

Порівняльно-правовий аналіз досвіду іноземних держав (Сполучених Штатів Америки, Канади, Сполученого Королівства Великої Британії та Північної Ірландії, Австралійського Союзу, Французької Республіки, Литовської Республіки, Фінляндської Республіки, Республіки Польща, Угорщини) у сфері протидії зовнішньому впливу на публічне управління засвідчив наявність різнотипних правових моделей – від репресивно-реєстраційних до аналітико-превентивних, сформованих під впливом історичних, політичних та інституційних особливостей відповідних держав. Встановлено, що ефективні практики не зводяться до ізольованих обмежувальних заходів, а базуються на поєднанні спеціального законодавства, обов'язкового декларування зв'язків з іноземними суб'єктами, міжвідомчої координації, прозорої публічної комунікації та дієвих механізмів громадського і судового контролю.

Обґрунтовано, що використання інструментів протидії зовнішньому впливу поза межами принципів верховенства права трансформує відповідні механізми у засоби політичного тиску й обмеження громадянських свобод, що наочно демонструє російська модель правового регулювання. Показано, що жодна з проаналізованих моделей не є універсальною та не може бути безпосередньо імплементована в український правопорядок без урахування національного контексту, дотримання конституційних гарантій прав і свобод людини та громадянина.

З урахуванням результатів порівняльно-правового аналізу запропоновано гібридну модель протидії зовнішньому впливу на публічне управління, адаптовану до умов України, яка поєднує: реєстраційні механізми та санкції за недекларування (Сполучені Штати Америки, Сполучене Королівство Великої Британії та Північної Ірландії, Канада); контроль фінансування стратегічно чутливих сфер (Французька Республіка, Литовська Республіка); інституційні механізми міжвідомчого моніторингу з процедурними гарантіями незалежності (Сполучене Королівство Великої Британії та Північної Ірландії, частково Угорщина – з істотними правовими обмеженнями); превентивні, освітні та репутаційні інструменти (Фінляндська Республіка); спеціальний режим підвищеної відповідальності в умовах воєнного стану без стигматизації громадянського суспільства.

На основі теоретико-правового аналізу та практики зарубіжних держав розроблено та науково обґрунтовано формалізований алгоритм адміністративно-правової ідентифікації афілійованості та ризиків зовнішнього впливу на публічне управління, побудований на ризик-орієнтованій і процесно-управлінській логіці та інтегрований із системою критеріїв адміністративно-правової значущості й індикаторами доказової ваги, що забезпечує перехід від оціночних підходів до формалізованого ризик-скорингу. Сформовано матричну модель оцінки рівнів ризику зовнішнього впливу, яка дозволяє диференціювати адміністративні режими реагування без автоматичного настання правових наслідків і розглядає ідентифікацію

зовнішнього впливу як інструмент превентивного управління ризиками, що відповідає принципам пропорційності, верховенства права та європейським стандартам демократичної стійкості.

Обґрунтовано наукові та нормативно-правові підходи до вдосконалення адміністративно-правового механізму забезпечення інформаційної безпеки України в аспекті протидії зовнішньому впливу на публічне управління, який поєднує нормативно-правовий, інституційно-координаційний, інформаційно-аналітичний, процедурно-контрольний та комунікаційно-превентивний компоненти в єдину функціональну систему. Підкреслено судоцентричний характер застосування управлінсько-превентивних правових наслідків, які є строковими, індивідуалізованими та застосовуються виключно за рішенням суду, без каральної природи. Доведено доцільність створення спеціалізованого уповноваженого органу з протидії зовнішньому впливу як центрального органу виконавчої влади, що здійснює адміністративно-аналітичну діяльність без репресивних повноважень. Показано, що така модель переводить протидію зовнішньому впливу з фрагментарної, політизованої площини у процесуально захищену адміністративно-правову систему, яка забезпечує баланс між потребами національної та інформаційної безпеки і гарантіями прав і свобод людини, формуючи основу для впровадження спеціального Закону України «Про протидію зовнішньому впливу на публічне управління» з інтеграцією превентивної аналітики, інституційної координації та судового контролю.

Ключові слова: *інформація, національна безпека, інформаційна безпека, забезпечення інформаційної безпеки, адміністративно-правовий механізм, зовнішній вплив, публічне управління, інформаційні права, захист персональних даних, Європейський суд з прав людини.*

ABSTRACT

Kaletnik V.V. – **Administrative and legal mechanism for Ensuring Information Security of Ukraine.** – Qualifying scientific work as a manuscript.

Dissertation for the degree of Doctor of Philosophy in the specialty 081 «Law». – Non-Profit Enterprise «State University «Kyiv Aviation Institute»», Kyiv, 2026.

The dissertation is devoted to a comprehensive study of the administrative-legal mechanism for ensuring information security of Ukraine in the context of counteracting external influence on public administration. The research reveals the theoretical and methodological foundations, structure and functions of this mechanism and identifies directions for its further improvement.

Based on an interdisciplinary analysis, the essence of information security is clarified as a multidimensional phenomenon combining technological, political, legal, value-based and cultural aspects. Its place and functional role within the system of national security of the state are determined, and the integral nature of information security as a condition for the stability of both the state and society is substantiated. Existing conceptual approaches to the interpretation of information security are systematized: according to shared methodological features – systemic, static, process-oriented (activity-based) and comprehensive approaches; according to their transdisciplinary nature – technical, humanitarian, normative, psychological and integrated approaches. Within the framework of the comprehensive approach, information security of the state is proposed to be understood as a legally defined condition of protection of the national information space that ensures: resilience of information infrastructure and integrity of information resources; stability of information processes and protection of the rights of participants in information relations; preservation of national identity; realization of national interests and achievement of strategic objectives in the information sphere; and the creation of conditions for sustainable development of the information society.

As a result of a theoretical analysis of the phenomenon of the administrative-legal mechanism for ensuring information security of the state, several approaches to its interpretation are identified: systemic, structural-functional, activity-based, and comprehensive. From the standpoint of the comprehensive approach, this mechanism is proposed to be understood as a subsystem of public administration which, through legal norms, the activities of authorized institutions, and the application of administrative instruments (permitting, registration, supervisory, and coercive), ensures protection against internal and external threats and creates conditions for the sustainable development of the national information space. It is emphasized that this subsystem is holistic and dynamic and integrates interconnected components – regulatory-legal, institutional-coordination, procedural-functional, information-analytical, and communication-preventive – operating in interaction with internal and external factors and conditions.

The theoretical and legal nature of external influence on public administration is revealed as a specific threat to the sovereignty of public administration and to the information security of the state. Such influence is characterized by an indirect, concealed and cumulative nature and is implemented mainly outside formalized administrative decision-making procedures. Public administration is clarified as the activity of state authorities, local self-government bodies and other involved institutions aimed at the formulation and implementation of public policy in the interests of society and the state. Structurally, public administration is considered a complex multi-level socio-legal system that combines vertical (hierarchical and authoritative) and horizontal (network-based and communicative) dimensions, the interaction of which ensures the effectiveness of governance and the social legitimacy of managerial decisions.

It is substantiated that the horizontal dimension of public administration, encompassing civil society institutions, expert and analytical communities, and media environments, is the most vulnerable to external influence due to its openness, inclusiveness, pluralism and active use of formal and informal information-communication channels. It is demonstrated that in contemporary conditions

external influence is transforming from forms of direct interference into hidden mechanisms of distortion of governance processes aimed at manipulating the informational, semantic and procedural environment of decision-making.

External influence on public administration is defined as purposeful activity of a foreign actor or an entity affiliated with it, involving covert or extra-procedural interference in the processes of formation, circulation and interpretation of information, decision-making processes, or the setting of the public policy agenda, with the aim of altering its content or outcomes in favor of foreign actors. The functional role of the administrative-legal mechanism for ensuring information security in countering such influence is specified as a system of procedural filters (identification and risk-scoring, administrative verification, and judicial review). The necessity of further specification of this mechanism is emphasized, in particular through the development of specialized procedures for identifying affiliation with foreign actors.

The research establishes that the regulatory and legal framework for information security in Ukraine, particularly with regard to countering external influence on public administration, is characterized by fragmentation and conceptual incompleteness. Despite the existence of a considerable body of legislative and strategic acts in the spheres of national security, information policy and public administration, the current legal regulation does not form a coherent model for responding to indirect and covert influence on governance processes and largely ignores vulnerabilities inherent in the horizontal dimension of public administration.

It is determined that systemic limitations of legal regulation include the absence of a legislatively established conceptual and categorical framework for countering external influence, the obsolescence of certain regulatory acts, and the lack of specialized registration, supervisory and control mechanisms adapted to the latent and non-confrontational nature of modern information threats. As a result, the regulatory framework acquires predominantly reactive and declarative characteristics and fails to ensure preventive risk management within the public administration system.

The evolution of national regulatory initiatives in this field is shown to be inconsistent, oscillating between excessively restrictive and potentially repressive models and purely declarative approaches lacking effective implementation mechanisms. Such normative instability creates legal uncertainty, increases the risks of politicization in law enforcement, and impedes the formation of a transparent and legitimate system for countering external influence. Accordingly, the need is substantiated for the introduction of a special legislative act – the Law of Ukraine «On Counteracting External Influence on Public Administration» – based on the principles of legality, proportionality, transparency and judicial oversight.

The system of actors responsible for ensuring information security in Ukraine in the context of countering external influence on public administration is analyzed and its conceptual inconsistency in existing strategic and regulatory acts is identified. It is established that many existing approaches rely on outdated institutional models formed prior to the beginning of the full-scale armed aggression of the Russian Federation against Ukraine and do not reflect the transformed architecture of threats or the emergence of new institutional actors.

A functional model of the system of actors responsible for ensuring information security is proposed, structured as a set of interconnected subsystems: strategic-coordination, operational-executive, control-analytical, humanitarian-communication, and public-expert. It is substantiated that the effectiveness of this system is limited by the absence of a unified inter-agency response algorithm to threats, fragmentation of information resources and registers, insufficient horizontal interaction among actors, low levels of digital integration, and risks of politicization of administrative decision-making.

To enhance the institutional capacity of the institutional-coordination component of the administrative-legal mechanism, the establishment of a specialized authorized body – the Center for Countering External Influence – is proposed, along with the creation of a unified digital inter-agency data-exchange platform, the Integrated Affiliation Monitoring System, and the development of transparent mechanisms for

reporting, public interaction and civic oversight as factors for increasing public trust in state policy in the field of information security.

A comparative legal analysis of the experience of foreign states – the United States of America, Canada, the United Kingdom of Great Britain and Northern Ireland, Australia, the French Republic, the Republic of Lithuania, the Republic of Finland, the Republic of Poland and Hungary – demonstrates the existence of diverse legal models for countering external influence on public administration, ranging from registration-based regulatory regimes to analytical and preventive frameworks shaped by historical, political and institutional factors. Effective practices are shown to rely not on isolated restrictive measures but on a combination of special legislation, mandatory disclosure of links with foreign actors, inter-agency coordination, transparent public communication, and effective mechanisms of public and judicial oversight.

It is argued that the use of instruments for countering external influence outside the framework of the rule of law transforms them into instruments of political pressure and restrictions on civil liberties, as demonstrated by the Russian regulatory model. None of the analyzed models is universal or directly transferable to the Ukrainian legal order without consideration of the national context and constitutional guarantees of human rights and freedoms.

Taking into account the results of the comparative legal analysis, a hybrid model for countering external influence on public administration adapted to the conditions of Ukraine is proposed. It combines: registration mechanisms and sanctions for non-disclosure (United States, United Kingdom, Canada); oversight of financing in strategically sensitive sectors (France, Lithuania); institutional mechanisms of inter-agency monitoring with procedural guarantees of independence (United Kingdom and partially Hungary, with significant legal limitations); preventive, educational and reputational instruments (Finland); and a special regime of increased responsibility under martial law without stigmatization of civil society.

Based on theoretical legal analysis and the practice of foreign states, a formalized algorithm for administrative-legal identification of affiliation and risks

of external influence on public administration is developed. The algorithm is built on a risk-oriented and process-management logic and is integrated with a system of criteria for administrative-legal relevance and indicators of evidentiary weight, enabling the transition from discretionary assessments to formalized risk scoring. A matrix model for assessing levels of risk of external influence is proposed, allowing differentiated administrative response regimes without automatic legal consequences and treating identification of external influence as an instrument of preventive risk management consistent with the principles of proportionality, the rule of law and European standards of democratic resilience.

The dissertation substantiates scientific and normative approaches to improving the administrative-legal mechanism for ensuring information security of Ukraine in the context of countering external influence on public administration. This mechanism integrates regulatory-legal, institutional-coordination, information-analytical, procedural-control and communication-preventive components into a unified functional system. The court-centered nature of the application of preventive administrative measures is emphasized: such measures are temporary, individualized and applied exclusively by judicial decision and do not possess a punitive character. The expediency of establishing a specialized authorized body for countering external influence as a central executive authority performing analytical and administrative functions without repressive powers is demonstrated. Such a model shifts counteraction to external influence from a fragmented and politicized domain into a procedurally protected administrative-legal system that ensures a balance between the requirements of national and information security and the guarantees of human rights and freedoms, thereby creating the institutional and legal basis for the adoption of the Law of Ukraine «On Counteracting External Influence on Public Administration».

Keywords: *information; national security; information security; ensuring information security; administrative-legal mechanism; external influence; public administration; information rights; personal data protection, European Court of Human Rights.*

СПИСОК ПРАЦЬ, ОПУБЛІКОВАНИХ ЗА ТЕМОЮ ДИСЕРТАЦІЇ

у наукових фахових виданнях України:

1. Калетнік В. В. Теоретичні аспекти удосконалення національного законодавства в контексті протидії деструктивній діяльності агентів впливу. *Наукові праці Національного авіаційного університету. Серія: Юридичний вісник «Повітряне і космічне право»*. 2020. Вип. 56 (№ 3). С. 81–88. URL: https://doi.org/10.18372/2307-9061.56.14895.

2. Калетнік В. В. Сучасний стан адміністративно-правового забезпечення інформаційної безпеки в Україні: теоретико-правовий аналіз. *Наукові праці Національного авіаційного університету. Серія: Юридичний вісник «Повітряне і космічне право»*. 2021. Вип. 59 (№ 2). С. 70–77. URL: https://doi.org/10.18372/2307-9061.59.15597.

3. Калетнік В. В. Інформаційна безпека як система суспільних відносин і об’єкт правової охорони. *Наукові праці Національного авіаційного університету. Серія: Юридичний вісник «Повітряне і космічне право»*. 2022. Вип. 65 (№ 4). С. 72–79. URL: https://doi.org/10.18372/2307-9061.65.17042.

4. Калетнік В. В. Аналіз національного законодавства в контексті протидії діяльності агентів впливу як одного з методів прихованого лобіювання. *Науковий вісник Ужгородського національного університету. Серія: Право.* 2024. Вип. 84 (№ 3). С. 115–124. URL: https://doi.org/10.24144/2307-3322.2024.84.3.18.

в інших наукових виданнях України:

5. Калетнік В. В. Проблема правового забезпечення в контексті протидії «активним заходам». *Гілея: науковий вісник.* 2020. Вип. 154 (№ 3). С. 269–275. URL: http://gileya.org/index.php?ng=library&cont=long&id=222

6. Калетнік В. В. Проблеми юридичної кваліфікації діяльності агентів впливу. *Гілея: науковий вісник.* 2020. Вип. 155 (№ 4). С. 236–241. URL: http://gileya.org/index.php?ng=library&cont=long&id=223.

7. Калетнік В. В., Калетнік Н. В. Інформаційна безпека і кіберзахист як сучасна інтелектуальна зброя. *Молодий вчений.* 2021. Вип. 93 (№ 5). С. 305–311. URL: https://doi.org/10.32839/2304-5809/2021-5-93-58.

8. Калетнік В. В., Калетнік Н. В. Кібератаки як ключові елементи «інформаційної війни» Російської Федерації. *Молодий вчений*. 2022. Вип. 101 (№ 1). С. 37–42. URL: https://doi.org/10.32839/2304-5809/2022-1-101-8.

у наукових виданнях інших країн:

9. Калетнік В. В. Аналіз законодавства іноземних країн та національного законодавства України в аспекті напрацювання механізмів регулювання діяльності агентів впливу. *Visegrad Journal on Human Rights*. 2021. № 5. С. 50–58. ISSN 1339-7915. URL: https://journal-vjhr.sk/wp-content/uploads/2021/12/VJHR_5_2021.pdf.

у колективній монографії:

10. Калетнік В. В. Аналіз та шляхи вдосконалення нормативно-правового поля України в контексті забезпечення правових основ протидії агентам впливу. *Theoretical foundations of state and law* : монографія. Бондар В., Кузьменко І., Рудніченко С. та ін. Бостон, 2022. С. 28–33. URL: https://doi.org/10.46299/isg.2022.mono.legal.1.1.3.

наукові праці, які засвідчують апробацію дисертації:

11. Калетнік В. В. Захист прав, свобод і безпеки людини в умовах діджиталізації. *Права людини в епоху цифрових трансформацій* : матеріали XII Міжнар. наук.-практ. конф., м. Київ, 25 лют. 2022 р. / Нац. авіац. ун-т. Київ, 2022. С. 166–169. URL: https://ocs.nau.edu.ua/index.php/TL/conference/paper/view/10998/8634.

12. Калетнік В. В. Аналіз деструктивної діяльності агентів впливу в умовах широкомасштабної збройної агресії Російської Федерації проти України. *Development of Scientific Space in the Context of Global Changes* : матеріали Міжнар. наук. конф., м. Рига (Латвія), 25–26 лист. 2022 р. / Publishing House «Baltija Publishing». Рига, 2022. С. 10–13. URL: https://doi.org/10.30525/978-9934-26-256-2-3.

13. Калетнік В. В. Вплив деструктивної діяльності агентів впливу на національну безпеку держави. *Modern Science: Global Trends, Technologies and Innovations* : тези доп. Міжнар. наук. конф., м. Рига (Латвія), 20–21 жовт. 2023 р. / Publishing House «Baltija Publishing». Рига, 2023. С. 15–19. URL: https://doi.org/10.30525/978-9934-26-354-5-5.

14. Калетнік В. В. Поняття і характеристика адміністративно-правового механізму забезпечення інформаційної безпеки України. *Забезпечення стійкості системи публічної влади та управління в умовах спеціальних адміністративно-правових режимів та відновлення України* : матеріали II Міжнар. наук.-практ. конф., м. Одеса, 17 трав. 2024 р. / Одеська політехніка. Одеса, 2024. С. 480–483. URL: https://op.edu.ua/sites/default/files/publicFiles/studolympconf/mizh_nauk_prak_konf_17.05.2024.pdf.

15. Калетнік В. В. Заходи антиукраїнського інформаційного впливу Російської Федерації: механізми, наративи, протидія. *Science in the context of current challenges: from theory to practice* : тези доп. Міжнар. наук. конф., м. Рига (Латвія), 9-10 трав. 2025 р. / Publishing House «Baltija Publishing». Рига, 2025. С. 88–92. URL: https://doi.org/10.30525/978-9934-26-568-6-25.

ЗМІСТ

ПЕРЕЛІК УМОВНИХ СКОРОЧЕНЬ …… 20

ВСТУП …… 22

РОЗДІЛ 1. ТЕОРЕТИКО-ПРАВОВІ ЗАСАДИ ФОРМУВАННЯ АДМІНІСТРАТИВНО-ПРАВОВОГО МЕХАНІЗМУ ЗАБЕЗПЕЧЕННЯ ІНФОРМАЦІЙНОЇ БЕЗПЕКИ ДЕРЖАВИ …… 35

1.1. Інформаційна безпека держави як предмет адміністративно-правового регулювання …… 35

1.2. Адміністративно-правовий механізм забезпечення інформаційної безпеки держави: сутність та структура …… 50

1.3. Зовнішній вплив на публічне управління як загроза інформаційній безпеці держави …… 70

Висновки до розділу 1 …… 88

РОЗДІЛ 2. АДМІНІСТРАТИВНО-ПРАВОВИЙ МЕХАНІЗМ ЗАБЕЗПЕЧЕННЯ ІНФОРМАЦІЙНОЇ БЕЗПЕКИ УКРАЇНИ: ПРАКТИЧНА СКЛАДОВА …… 92

2.1. Стан нормативно-правового забезпечення інформаційної безпеки України в аспекті протидії зовнішньому впливу на публічне управління …… 92

2.1.1. Загальна характеристика чинної нормативно-правової бази у сфері інформаційної безпеки та публічного управління …… 92

2.1.2. Нормативні ініціативи та спроби конкретизації законодавства щодо протидії зовнішньому впливу на публічне управління …… 102

2.2. Система суб'єктів забезпечення інформаційної безпеки України в аспекті протидії зовнішньому впливу на публічне управління …… 108

2.3. Аналіз досвіду іноземних країн з протидії зовнішньому впливу та можливі шляхи його запозичення в Україні …… 123

Висновки до розділу 2 …… 140

РОЗДІЛ 3. НАПРЯМИ ВДОСКОНАЛЕННЯ АДМІНІСТРАТИВНО-ПРАВОВОГО МЕХАНІЗМУ ЗАБЕЗПЕЧЕННЯ ІНФОРМАЦІЙНОЇ БЕЗПЕКИ УКРАЇНИ ……. 143

3.1. Особливості адміністративно-правової ідентифікації афілійованості та ризиків зовнішнього впливу на публічне управління ….. 143

3.2. Пропозиції щодо удосконалення адміністративно-правового механізму забезпечення інформаційної безпеки України в аспекті протидії зовнішньому впливу на публічне управління …… 149

Висновки до розділу 3 ……. 159

ВИСНОВКИ ……... 162

СПИСОК ВИКОРИСТАНИХ ДЖЕРЕЛ ……... 169

ДОДАТКИ ……. 193

ПЕРЕЛІК УМОВНИХ СКОРОЧЕНЬ

ВРУ – Верховна Рада України

ГШ ЗСУ – Генеральний штаб Збройних Сил України

ГУР – Головне управління розвідки

Держкіно – Державне агентство з питань кіно

Держкомтелерадіо – Державний комітет телебачення і радіомовлення України

Держспецзв'язку – Державна служба спеціального зв'язку та захисту інформації України

Держфінмоніторинг – Державна служба фінансового моніторингу України

ДМС – Державна митна служба України

ДПС – Державна податкова служба України

ЄС – Європейський Союз

ЄСПЛ – Європейський суд з прав людини

ЗМІ – засоби масової інформації

ЗСУ – Збройні Сили України

ІГС – інститути громадянського суспільства

КМУ, Кабмін – Кабінет Міністрів України

КНР – Китайська Народна Республіка

КУпАП – Кодекс України про адміністративні правопорушення

МЗС – Міністерство закордонних справ України

Мінцифри – Міністерством цифрової трансформації України

МОН – Міністерством освіти і науки України

МОУ – Міністерство оборони України

Мінкультури – Міністерство культури України

Мін'юст – Міністерство юстиції України

НАДС – Національне агентство України з питань державної служби

НАЗК – Національне агентство з питань запобігання корупції

НАТО – Організація Північноатлантичного договору

Нацрада – Національна рада України з питань телебачення і радіомовлення

НБУ – Національний банк України

НІСД – Національний інститут стратегічних досліджень

НКЕК – Національна комісія, що здійснює державне регулювання у сферах електронних комунікацій, радіочастотного спектра та надання послуг поштового зв`язку

НКЦК – Національний координаційний центр кібербезпеки

НПУ – Національна поліція України

НУО – неурядова організація (неурядові організації)

РНБО – Рада національної безпеки і оборони України

рф – російська федерація

СБУ – Служба безпеки України

СЗР – Служба зовнішньої розвідки України

СІМА – Система інтегрованого моніторингу афілійованості

США – Сполучені Штати Америки

ЦОВВ – центральний орган виконавчої влади (центральні органи виконавчої влади)

ЦПД – Центр протидії дезінформації

ЦПЗВ – Центр протидії зовнішньому впливу

FARA – Foreign Agents Registration Act

FITS – Foreign Influence Transparency Scheme Act

FIRS – Foreign Influence Registration Scheme

FITAA – Foreign Influence Transparency and Accountability Act

SPO – Sovereignty Protection Office

ВСТУП

Актуальність теми дослідження. В умовах трансформації сучасного світового порядку та загострення глобальних і регіональних протистоянь особливого значення набуває проблема захисту національних інтересів від деструктивних зовнішніх впливів. Поширення інформаційної експансії та агресії, активне застосування технологій гібридної війни, використання кіберпростору як середовища маніпуляцій та підривної діяльності зумовлюють необхідність переосмислення та посилення адміністративно-правових засад інформаційної безпеки України. Однією з ключових загроз національній безпеці в цілому, а також інформаційній безпеці України зокрема, є зовнішній вплив на публічне управління, спрямований на підрив демократичних інститутів, легітимності державних рішень та довіри суспільства до органів влади.

Особливої актуальності дослідження набуває в умовах Війни за Незалежність України, що супроводжується масштабними інформаційно-психологічними операціями, спрямованими на підрив національної єдності, делегітимізацію органів державної влади, маніпуляцію громадською думкою та формування вигідних агресору політичних рішень. Саме в такому контексті питання ідентифікації, правового визначення та протидії зовнішньому впливу на публічне управління постає як першочергове завдання державної політики у сфері національної та інформаційної безпеки.

Поняття зовнішнього впливу на публічне управління на сьогодні залишається новим і недостатньо розробленим у вітчизняній правовій доктрині. Воно охоплює форми та способи опосередкованого втручання у процеси вироблення, ухвалення й реалізації управлінських рішень, що здійснюються під впливом іноземного суб’єкта та створюють ризики для суверенітету України в публічному управлінні, інформаційної безпеки та державного суверенітету загалом. За цих умов постає необхідність у створенні ефективного адміністративно-правового механізму виявлення, верифікації,

декларування та усунення зовнішніх політичних, організаційних, фінансових та інформаційних впливів на процеси вироблення та прийняття управлінських рішень, а також формування порядку денного.

Зазначене вимагає від політиків, науковців, правників, громадських діячів, суспільства загалом пошуку принципово нових підходів до удосконалення адміністративно-правового механізму забезпечення інформаційної безпеки України в аспекті протидії зовнішньому впливу на публічне управління відповідно до викликів та загроз сьогодення.

Різні аспекти національної безпеки загалом та інформаційної безпеки зокрема, окремих її складових, питання адміністративно-правового регулювання та забезпечення інформаційної безпеки досліджували вчені-юристи, серед яких П. Д. Біленчук, В. Т. Білоус, Р. В. Бондаренко, В. І. Гурковський, Л. О. Євдоченко, О. С. Зозуля, Л. О. Кочубей, С. І. Крук, Ю. Д. Кунєв, В. А. Ліпкан, А. М. Лисеюк, Ю. П. Лісовська, О. В. Логінов, А. Ф. Мельник, Ю. Є. Максименко, Л. Р. Наливайко, Н. Р. Нижник, О. Ю. Оболенський, А. Й. Присяжнюк, О. В. Радченко, Г. П. Ситник, О. О. Тихомиров, Т. Ю. Ткачук, Л. С. Харченко, П. В. Цимбал, В. В. Шемчук, І. М. Шопіна, О. О. Шумейко та інші. Їхні праці заклали методологічне підґрунтя досліджень у сфері інформаційної безпеки та стали базою для подальших наукових пошуків.

Особливе місце посідають дослідження, присвячені осмисленню феномену зовнішнього впливу, а також проблемам виявлення та протидії такій діяльності. Ці питання аналізували Д. В. Дубов, Е. А. Гугнін, І. В. Корецька, І. В. Матвєєнко, Р. В. Шутов, а також зарубіжні дослідники – М. Діккаш, К. Мішель та інші.

Окремий блок наукових напрацювань, що має безпосереднє значення для цього дослідження, становлять праці вчених у сфері державного та публічного управління. Зокрема, ці питання досліджували О. Ф. Константінов, В. С. Куйбіда, В. В. Мамонова, О. А. Машков, А. Ф. Мельник, Р. С. Мельник, Б. Б. Мельниченко, О. В. Михайловська, Н. Р. Нижник, О. Ю. Оболенський,

Н. І. Обушна, Н. В. Філіпова, І. І. Фуртак, Л. С. Ладонько, а також зарубіжні науковці К. Поллітт, Г. Букарт та інші. Їхні праці дали змогу поглянути на публічне управління як на складну багаторівневу систему, що поєднує вертикальні владно-ієрархічні та горизонтальні мережеві взаємодії, у межах якої відбувається формування та реалізація управлінських рішень.

Теоретико-правову основу дисертаційного дослідження становлять праці вчених із теорії держави і права, конституційного та адміністративного права: В. Б. Авер'янов, Ю. П. Битяк, В. В. Галунько, О. В. Зайчук, Є. В. Кобко, А. М. Колодій, Ю. Д. Кунєв, Н. М. Крестовська, Л. Г. Матвєєва, О. І. Остапенко, О. Ф. Скакун. Їхні напрацювання формують фундаментальні засади для розкриття адміністративно-правового механізму забезпечення інформаційної безпеки України.

Узагальнюючи, можна констатувати, що наукова література відображає багатогранність досліджуваної проблематики: від загальнотеоретичних підходів до інформаційної безпеки та публічного управління до практичних аспектів протидії зовнішньому впливу на публічне управління.

Водночас наявні напрацювання не забезпечують комплексного наукового осмислення адміністративно-правового механізму забезпечення інформаційної безпеки у контексті протидії зовнішньому впливу на публічне управління, що зумовлює актуальність цього дисертаційного дослідження.

Зв'язок роботи з науковими програмами, планами, темами. Дисертацію виконано відповідно до Закону України «Про пріоритетні напрями розвитку науки і техніки», Переліку пріоритетних тематичних напрямів наукових досліджень і науково-технічних розробок на період до 2023 року, затверджених постановою Кабінету Міністрів України від 7 вересня 2011 р. № 942; Плану законодавчого забезпечення реформ в Україні, схваленого Постановою Верховної Ради України від 04 червня 2015 р. № 509-VII.

Проблематика дисертації виходить з положень Указу Президента України «Про Цілі сталого розвитку України на період до 2030 року» від 30 вересня 2019 р. № 722, постанови Кабінету Міністрів України «Про

затвердження Державної стратегії регіонального розвитку на 2021–2027 рр.» від 5 серпня 2020 р. № 695.

Дисертацію виконано в межах Держбюджетних (кафедральних) науково-дослідних робіт:

№ 71 / 13.01.02 за темою: «Забезпечення конституційних прав громадян в контексті конвенційних зобов'язань України» (державний реєстраційний номер 011U103091);

№ 53-2022 / 13.01.02 за темою: «Людиноцентричність публічного права України» (державний реєстраційний номер 0124U003363).

Мета і завдання дослідження. *Метою дисертаційного дослідження* є обґрунтування теоретичних положень і методологічних підходів, вироблення практичних пропозицій щодо вдосконалення адміністративно-правового механізму забезпечення інформаційної безпеки України в аспекті протидії зовнішньому впливу на публічне управління.

Досягнення поставленої мети зумовило необхідність вирішення низки взаємопов'язаних завдань, структурованих відповідно до логіки дисертаційного дослідження.

У першому розділі:

проаналізувати та систематизувати наукові підходи до розуміння інформаційної безпеки держави;

розкрити сутність та структуру адміністративно-правового механізму забезпечення інформаційної безпеки держави;

дослідити теоретико-правову природу зовнішнього впливу на публічне управління як специфічної загрози інформаційній безпеці держави.

У другому розділі:

проаналізувати сучасний стан нормативно-правового забезпечення інформаційної безпеки України в аспекті протидії зовнішньому впливу на публічне управління;

дослідити систему суб'єктів забезпечення інформаційної безпеки України в аспекті протидії зовнішньому впливу на публічне управління;

здійснити порівняльно-правовий аналіз досвіду іноземних держав щодо протидії зовнішньому впливу на публічне управління та виокремити релевантні елементи для можливого нормативного та інституційного запозичення в Україні.

У третьому розділі:

розробити та науково обґрунтувати формалізований адміністративно-правовий алгоритм ідентифікації афілійованості та ризиків зовнішнього впливу на публічне управління;

обґрунтувати наукові та нормативно-правові підходи до вдосконалення адміністративно-правового механізму забезпечення інформаційної безпеки України в аспекті протидії зовнішньому впливу на публічне управління.

Об'єкт дослідження – публічно-правові відносини у сфері забезпечення інформаційної безпеки України.

Предмет дослідження – адміністративно-правовий механізм забезпечення інформаційної безпеки України.

Методи дослідження. Методологічну основу дослідження становлять загальнофілософські, загальнонаукові, спеціально-юридичні та міждисциплінарні методи пізнання, використання яких зумовлене метою та завданнями дисертаційної роботи.

Загальнофілософським підґрунтям виступає *діалектичний метод* (1.1, 1.3), що забезпечило дослідження інформаційної безпеки як динамічної системи та дало змогу виявити закономірності трансформації зовнішнього впливу у приховані механізми деформації управлінських процесів. *Принцип системності* (1.2, 2.2, 3.2) використано для обґрунтування п'ятикомпонентної структури адміністративно-правового механізму як цілісної підсистеми державного управління. *Принцип сходження від абстрактного до конкретного* (1.3, 3.1) застосовано для розкриття змісту феномену «зовнішнього впливу» та розробки формалізованого алгоритму його ідентифікації.

Серед загальнонаукових методів застосовано: *гносеологічний* (1.1, 1.2, 1.3) – для формування авторських дефініцій «інформаційна безпека держави», «забезпечення інформаційної безпеки держави», «адміністративно-правовий механізм забезпечення інформаційної безпеки держави», «публічне управління», «система публічного управління», «інституційно-процедурна деформація управлінських процесів», «суверенітет публічного управління», «іноземний суб'єкт» та «афілійований суб'єкт»; *аналіз та синтез* (2.1, 3.2) – для виявлення дефектів нормативного регулювання та розробки положень спеціального Закону України «Про протидію зовнішньому впливу на публічне управління»; *індукцію та дедукцію* (усі розділи) – для переходу від аналізу вразливості «горизонтального виміру» управління до теоретичних узагальнень щодо загроз суверенітету України в публічному управлінні; *структурно-функціональний метод* (2.2) – для диференціації суб'єктів забезпечення інформаційної безпеки на п'ять взаємопов'язаних функціональних підсистем.

До спеціально-юридичних методів віднесено: *формально-юридичний* (2.1, 3.1) – для аналізу змісту правових норм та побудови матричної моделі ризик-скорингу на основі індикаторів афілійованості; *метод юридичної інтерпретації* (1.2, 2.2) – для з'ясування обсягу компетенції суб'єктів забезпечення інформаційної безпеки у межах їхнього адміністративно-правового статусу; *порівняльно-правовий метод* (2.3) – для критичного аналізу іноземного досвіду та обґрунтування гібридної моделі протидії зовнішньому впливу, релевантної для України.

Серед міждисциплінарних методів застосовано: *історико-правовий* (2.1) – для дослідження еволюції національних нормативних ініціатив та причин їхньої попередньої неефективності; *математичне моделювання та експертне оцінювання* (3.1) – для розрахунку інтегрального показника ризику *(IR)* та визначення вагових коефіцієнтів критеріїв значущості зовнішнього впливу із застосуванням коефіцієнта конкордації Кендалла.

Комплексне застосування зазначених методів забезпечило досягнення поставленої мети та вирішення завдань дослідження у їх логічній та структурній взаємопов'язаності.

Нормативну основу роботи становлять Конституція України, закони України, акти Президента України та Кабінету Міністрів України, інші підзаконні нормативно-правові акти, що регулюють питання інформаційної безпеки держави та публічного управління. Обґрунтування авторських висновків щодо напрямків удосконалення адміністративно-правового механізму забезпечення інформаційної безпеки України в аспекті протидії зовнішньому впливу на публічне управління здійснено із застосуванням практики законодавчого врегулювання такої діяльності у таких зарубіжних державах, як: Сполучені Штати Америки, Канада, Сполучене Королівство Великої Британії та Північної Ірландії, Австралійський Союз, Французька Республіка, Литовська Республіка, Фінляндська Республіка, Республіка Польща, Угорщина.

Емпіричну базу дослідження становлять матеріали науково-практичних конференцій, дані офіційних сайтів, аналітичні матеріали, результати опитування представників інститутів громадянського суспільства.

Наукова новизна одержаних результатів полягає в тому, що дисертація є одним із перших комплексних наукових досліджень у вітчизняній адміністративно-правовій науці, в якому системно досліджено адміністративно-правовий механізм забезпечення інформаційної безпеки держави в аспекті протидії зовнішньому впливу на публічне управління. У результаті дослідження сформульовано низку нових наукових положень, рекомендацій і висновків, зокрема:

уперше:

обґрунтовано зовнішній вплив на публічне управління як самостійну адміністративно-правову категорію, що становить специфічну загрозу інформаційній безпеці держави та реалізується через інституційно-процедурну деформацію управлінських процесів, яка створює перешкоди для

реалізації незалежної адміністративної дискреції та призводить до підміни публічного інтересу інтересами іноземних суб'єктів;

введено та теоретично обґрунтовано поняття:

«інституційно-процедурна деформація управлінських процесів», що дає змогу відмежувати динаміку зовнішнього впливу від його юридично значущих наслідків, які мають системний характер і не зводяться до разових порушень законності;

«суверенітет публічного управління», що розкриває здатність системи публічного управління до автономного формування порядку денного та реалізації рішень відповідно до публічних інтересів у межах установлених правових процедур;

запропоновано п'ятикомпонентну структуру адміністративно-правового механізму забезпечення інформаційної безпеки держави, яка, на відміну від традиційних трикомпонентних моделей, включає нормативно-правовий, інституційно-координаційний, інформаційно-аналітичний, процедурно-контрольний та комунікаційно-превентивний блоки як взаємопов'язані процедурні фільтри ідентифікації загроз;

розроблено авторську концептуальну модель адміністративно-правового механізму забезпечення інформаційної безпеки України в аспекті протидії зовнішньому впливу, що ґрунтується на концепції демократичної стійкості (*democratic resilience*) та трансформує реагування на латентні безпекові загрози з площини політичної доцільності у сферу чітко регламентованих адміністративних процедур;

обґрунтовано використання алгоритму адміністративно-правової ідентифікації прихованої афілійованості, побудованого на методі ризик-скорингу. Сутність алгоритму полягає у розрахунку інтегрального показника ризику *(IR)* шляхом математичного синтезу параметрів значущості впливу та показників афілійованості, що забезпечує перехід від суб'єктивних оцінок до об'єктивної матричної моделі визначення рівнів безпекових загроз;

сформульовано та запропоновано авторські визначення категорій і понять, що раніше були відсутні в національному законодавстві і науковому дискурсі: «зовнішній вплив на публічне управління», «іноземний суб'єкт», «афілійований суб'єкт», що забезпечило чіткий понятійно-категоріальний апарат для подальшого законодавчого та адміністративно-правового регулювання;

удосконалено:

методологічні підходи до розуміння та класифікації концепцій інформаційної безпеки шляхом виокремлення комплексного (комбінованого) підходу, що інтегрує правові, технічні та соціально-психологічні виміри;

теоретичні підходи до розуміння забезпечення інформаційної безпеки як проактивної управлінської діяльності, в якій правовий компонент виступає не лише як обмежувач, а як механізм формування резистентності системи публічного управління до зовнішніх впливів;

порівняльно-правовий аналіз іноземних моделей протидії зовнішньому впливу через їх функціональну диференціацію за реєстраційним, інституційним, превентивним і репресивним векторами. Це дало змогу обґрунтувати авторську концепцію гібридної моделі для України, що синтезує досвід провідних демократичних держав, зокрема Французької Республіки (у частині цифрового моніторингу), Сполученого Королівства Великої Британії та Північної Ірландії (щодо рівнів реєстрації), а також Канади, Литви та Фінляндії (у частині інституційної стійкості та прозорості), забезпечуючи баланс між національною стійкістю та демократичними стандартами;

теоретичне узагальнення ролі судового контролю як невід'ємного елементу адміністративно-правового механізму забезпечення інформаційної безпеки, що визначає судоцентричний характер застосування правових наслідків. Це дозволяє трансформувати заходи реагування з каральних у превентивні та забезпечити їх індивідуалізацію;

дістали подальшого розвитку:

теоретичне обґрунтування архітектоніки системи публічного управління в безпекознавчому контексті як дуалістичної структури, що поєднує

вертикальне ієрархічне ядро та горизонтальний мережевий контур, що дозволило розглядати публічне управління як складний об’єкт забезпечення інформаційної безпеки;

наукові положення щодо проявів інституційно-процедурної деформації управлінських процесів як результату зовнішнього впливу, що дало змогу виявити системні дефіцити чинного законодавства, зокрема феномени «процедурного вакууму» та «регуляторної сліпоти»;

класифікація суб’єктів забезпечення інформаційної безпеки України в аспекті протидії зовнішньому впливу на публічне управління, диференційована за п’ятьма функціональними підсистемами, що дозволило інтегрувати ключові органи фінансового, кадрового та антикорупційного контролю в єдиний адміністративно-координаційний контур протидії зовнішньому впливу;

теоретичне обґрунтування створення спеціалізованого уповноваженого органу – Центру протидії зовнішньому впливу як інституційного гаранта захисту суверенітету публічного управління, наділеного повноваженнями з адміністративної верифікації ризиків афілійованості, координації реагування та ведення Реєстру афілійованих суб’єктів на засадах прозорості та обов’язкового судового контролю;

науково обґрунтовані положення щодо вдосконалення адміністративно-правового регулювання протидії зовнішньому впливу, що знайшли відображення у розробленому в межах дисертації авторському законопроєкті Закону України «Про протидію зовнішньому впливу на публічне управління», який:

- формалізує процедурно-правовий режим адміністративної верифікації афілійованості, долаючи виявлену «регуляторну сліпоту» чинного законодавства щодо латентних каналів впливу;

- запроваджує ризик-орієнтований моніторинг і ідентифікацію зовнішнього впливу як інструмент нейтралізації інституційно-процедурної деформації управлінських процесів;

- встановлює чіткі алгоритми адміністративного регулювання для подолання «процедурного вакууму» у діяльності суб'єктів владних повноважень;

- закріплює механізми адміністративної відповідальності та судоцентричний характер застосування превентивних заходів, що забезпечує баланс між національною стійкістю та захистом прав і свобод людини;

- становить науково обґрунтовану основу для системного правового реагування на гібридні виклики суверенітету України в публічному управлінні.

Практичне значення одержаних результатів полягає у можливості безпосереднього використання сформульованих у дисертаційному дослідженні висновків, методичних підходів та розроблених моделей у нормотворчій, правозастосовній та експертно-аналітичній діяльності державних органів у сфері забезпечення інформаційної безпеки та публічного управління.

По-перше, теоретичні положення дисертації можуть стати основою для розробки навчальних програм з курсів і спецкурсів у циклі правових дисциплін.

По-друге, практична цінність дослідження полягає в адаптації розробленої моделі до потреб органів державної влади та правоохоронних інституцій, зокрема для:

розроблення адміністративно-правових інструментів протидії зовнішньому впливу на публічне управління;

забезпечення комплексної інформаційної безпеки держави в умовах сучасних викликів та загроз.

По-третє, отримані напрацювання можуть бути використані у законотворчій діяльності Верховної Ради України, Міністерства юстиції України та інших органів виконавчої влади, а також у підготовці підзаконних актів, методичних рекомендацій та стратегічних документів щодо протидії зовнішньому впливу.

По-четверте, запропонований у роботі адміністративно-правовий механізм забезпечення інформаційної безпеки України має прикладне значення для експертного середовища, освітніх та наукових установ, які займаються питаннями правового забезпечення інформаційної безпеки.

По-п'яте, окремі наукові та практичні положення дисертації було використано під час розробки у 2025 році проєкту Доктрини "Інформаційні операції" (акт про впровадження результатів дисертаційного дослідження № 304/9 від 01.01.2026).

По-шосте, отримані результати впроваджено в навчальний процес кафедри військового права Військово-юридичного інституту Національного юридичного університету імені Ярослава Мудрого протягом 2025–2026 н. р. при викладанні дисципліни «Правові основи інформаційної безпеки у воєнній сфері» (довідка від 23.02.2026).

Особистий внесок здобувача. Дисертаційне дослідження виконано здобувачем самостійно з використанням теоретичних напрацювань вітчизняних і зарубіжних учених у сфері адміністративного права, національної (інформаційної) безпеки та державного управління. Наукові положення, висновки й пропозиції ґрунтуються на власних результатах автора. На всі використані в роботі ідеї та результати інших дослідників здійснено належні посилання.

Апробація результатів дисертації. Основні положення та результати дослідження були оприлюднені на міжнародних наукових і науково-практичних конференціях, зокрема: «Права людини в епоху цифрових трансформацій» (м. Київ, 25 лютого 2022 року), «Development of Scientific Space in the Context of Global Changes» (м. Рига, Латвія, 25–26 листопада 2022 року), «Modern Science: Global Trends, Technologies and Innovations» (м. Рига, Латвія, 20–21 жовтня 2023 року), «Забезпечення стійкості системи публічної влади та управління в умовах спеціальних адміністративно-правових режимів та відновлення України» (м. Одеса, 17 травня 2024 року), «Science in the context of current challenges: from theory to practice» (м. Рига,

Латвія, 9–10 травня 2025 року); а також під час наукових і науково-методичних семінарів – «Інформаційні війни: перспективи правової протидії» (м. Київ, 15 квітня 2021 року), «Правове забезпечення інформаційної безпеки: стан та перспективи розвитку» (м. Київ, 2 листопада 2021 року), і в межах науково-практичної дискусії «Верховенство права: теорія і практика в умовах сучасних світових викликів» (м. Київ, 1 грудня 2025 року).

Публікації. Результати дослідження викладено у 15 публікаціях. Основні наукові результати дисертації висвітлено у 10 наукових працях, з яких: 1 – розділ у колективній монографії; 9 – наукові статті, з них 4 – у фахових виданнях України з юридичних наук та 5 – у інших наукових виданнях (4 – у наукових виданнях України, 1 – у зарубіжному науковому виданні).

Додатково результати дисертації відображено у 5 публікаціях (тези доповідей на міжнародних наукових і науково-практичних конференціях), що підтверджують апробацію результатів дослідження.

Таким чином, апробація результатів підтвердила наукову й практичну значущість положень дисертації та їхню придатність для подальшого використання у нормотворчій та правозастосовній діяльності.

Структура та обсяг дисертації. Дисертація складається із вступу, трьох розділів, що містять вісім підрозділів, висновків, списку використаних джерел та додатків. Матеріали додатків містять перелік опублікованих праць (Додаток А), глосарій термінів (Додаток Б), інструментарій та результати експертного оцінювання (Додатки В–Д), проєкт Закону України (Додаток Е), а також акт та довідку про впровадження результатів дослідження (Додатки Є, Ж). Загальний обсяг дисертації становить 232 сторінки, у тому числі основного тексту – 147 сторінок. Список використаних джерел налічує 200 найменувань – 24 сторінки, додатки – 40 сторінок.

РОЗДІЛ 1
ТЕОРЕТИКО-ПРАВОВІ ЗАСАДИ ФОРМУВАННЯ АДМІНІСТРАТИВНО-ПРАВОВОГО МЕХАНІЗМУ ЗАБЕЗПЕЧЕННЯ ІНФОРМАЦІЙНОЇ БЕЗПЕКИ ДЕРЖАВИ

1.1. Інформаційна безпека держави як предмет адміністративно-правового регулювання

На початку XXI століття інформація для будь-якої держави набуває значення стратегічного ресурсу, від ефективності використання якого безпосередньо залежать рівень національної безпеки та перспективи формування демократичного суспільства, у якому забезпечується реалізація конституційних прав і свобод людини та громадянина, зокрема права на вільний пошук, отримання, передавання й поширення інформації всіма законними способами.

Розвиток засобів масової інформації (далі – ЗМІ) та інформаційно-комунікаційних технологій зумовив залучення суспільства до глобальних інформаційних систем, у межах яких воно постає не лише споживачем, а й активним суб'єктом інформаційних процесів. Соціальні умови життя населення значною мірою визначаються рівнем розвитку інформаційних технологій. У політичній площині пріоритет зміщується від силових важелів впливу до інформаційних детермінант. Водночас у господарському секторі ми спостерігаємо процес глибокого впровадження інтелектуальних продуктів та інформаційних ресурсів у систему ринкових відносин. Унаслідок глобальних процесів інформатизації стався якісний перехід у механізмах управління на всіх щаблях публічної влади.

Водночас тенденція до зростання відкритості суспільства та широке впровадження інформаційно-комунікаційних технологій формують передумови для протиправних посягань на інформацію, її користувачів та інформаційні

системи зв’язку, що, своєю чергою, призводить до послаблення системних механізмів гарантування інформаційної безпеки на державному рівні.

Інформаційна безпека є важливою невід’ємною складовою забезпечення національної безпеки держави. Визначальним фактором стабільного соціального поступу та утвердження суб’єктності держави у глобальному середовищі є формування високотехнологічного й захищеного інформаційного простору, здатного забезпечувати належний рівень захисту інформаційних ресурсів і комунікаційних систем. Завдяки впровадженню дієвого механізму захисту інформаційних інтересів особистості, соціуму та владних інститутів стає можливим оперативне детектування й нівелювання потенційних і фактичних деструктивних впливів, що загрожують національним пріоритетам, а також запобігання регресивним процесам в економіці та соціальній сфері.

Стабільність інформаційної безпеки детермінується сукупністю внутрішніх та екзогенних чинників, серед яких визначальними є геополітична кон’юнктура, а також рівень технологічного й соціоекономічного базису держави. В інтенсифікації розвитку цього сегмента солідарно зацікавлені як представники приватного сектору, що інтегрують інноваційні рішення, так і органи державної влади, для яких питання кібернетичної та інформаційної стійкості мають стратегічний пріоритет.

Особливий статус захисту інформаційного суверенітету закріплено на найвищому законодавчому рівні. Згідно з положеннями ст. 17 Конституції України, гарантування національної безпеки визначено одним із засадничих обов’язків держави. Зокрема, Основний Закон імперативно закріплює, що захист суверенітету, територіальної цілісності, а також забезпечення економічної та інформаційної стійкості є найважливішими державними функціями та справою всього Українського народу [1]. Таким чином, розбудова надійної системи інформаційної безпеки виступає одним із базисних елементів життєдіяльності сучасної держави, що зумовлює необхідність ґрунтовного наукового дослідження цієї категорії.

Перед розглядом змісту поняття «інформаційна безпека» та її місця в системі національної безпеки України методологічно доцільно звернутися до аналізу базових категорій «інформація», «безпека» та «небезпека».

Етимологічне коріння категорії «інформація» сягає латинського першоджерела «informatio», що традиційно трактується як процес роз'яснення, представлення або формування цілісного уявлення про об'єкт пізнання [2]. Широке впровадження даного конструкту в науковий обіг припадає на XX століття, що зумовило появу різнопланових теоретико-методологічних концепцій. У межах сучасного наукового знання домінують дві фундаментальні парадигми: атрибутивна, де інформація постає як іманентна властивість матерії та притаманна будь-яким об'єктам реальності, та функціональна, згідно з якою вона розглядається як динамічний компонент процесів управління та комунікативної взаємодії в складних системах.

Слід зазначити, що першим дослідником інформатики як науки вважають Н. Вінера. У своїх наукових доробках Н. Вінер характеризував категорію інформації як специфічне відображення змісту, що надходить із довкілля в процесі адаптації до нього людини та її сенсорного сприйняття. Дослідник акцентував увагу на онтологічній самостійності цього явища, зазначаючи, що інформація не є ані матерією, ані енергією, а виступає автономною сутністю. На переконання вченого, механізми отримання та оперування даними є невід'ємною частиною життєдіяльності суб'єкта та його пристосування до мінливості зовнішніх обставин [3, с. 17]. З наведеної концепції можна зробити висновок, що абстрактні відомості трансформуються в інформацію лише в момент їхньої активної взаємодії з адресатом чи суб'єктом пізнання.

Подальший розвиток кібернетичної думки сприяв поглибленню цього поняття. Інформацію почали трактувати як сукупність отриманих із зовнішнього простору сигналів, що фіксуються в пам'яті та підлягають подальшій обробці за допомогою когнітивних зусиль людини або технічного інструментарію. У такому контексті вона постає як ресурс, що передається

комунікативними мережами задля забезпечення інформування, стимулювання певних дій чи корекції соціальної поведінки.

Варто зауважити, що кібернетичний підхід до інформації вимагав її філософського осмислення, адже саме філософському знанню належить роль у визначенні методологічного фундаменту будь-якої наукової галузі. Зокрема, український академік В. М. Глушков розглядає інформацію крізь призму фізичної субстанції. На думку вченого, вона є показником неоднорідності розподілу енергії та матерії у просторово-часовому вимірі, а також мірою тих трансформацій, якими супроводжується динаміка будь-яких світових процесів [4, с. 32].

У науковому доробку В. Г. Іванова, С. М. Іванова та В. В. Карасюка інформація трактується крізь призму гносеологічного підходу як сукупність даних про об’єкт пізнання, які суб’єкт здатен виокремити у процесі його інтелектуального відображення [5, с. 17]. Натомість С. О. Телешун та І. В. Рейтерович пропонують інший вектор аналізу, акцентуючи увагу на комунікативній природі явища та розглядаючи його як масив відомостей, що циркулюють між учасниками інформаційного обміну. Такий підхід дозволяє змістити фокус із вивчення статичних параметрів даних на процесуальну складову – безпосередній акт трансляції знань у соціальному просторі [6, с. 9].

У контексті сучасних процесів інформатизації саме категорія «дані» найбільш адекватно передає специфіку об’єктів інформаційних правовідносин, оскільки охоплює сукупність відомостей, зафіксованих як фактичні обставини, що відображають різні виміри людської діяльності та існування.

Нормативно-правове визначення поняття «інформація» закріплене у Законі України «Про інформацію». Згідно з положеннями Закону, під цією категорією слід розуміти сукупність будь-яких відомостей або даних, незалежно від форми їхнього представлення – чи то фіксація на фізичних (матеріальних) носіях, чи то відображення у цифровому (електронному) форматі [7]. Аналогічне визначення можна знайти і у ч. 1 ст. 200 Цивільного кодексу України [8]. У межах зазначеного нормативного акта також

виокремлюється категорія науково-технічної інформації. Під нею розуміють сукупність даних або відомостей про здобутки у сферах науки, промисловості та техніки (як вітчизняні, так і іноземні), що були отримані в результаті проектно-технологічної, науково-дослідної, виробничої чи громадської діяльності. Така інформація може фіксуватися на фізичних носіях або існувати в електронному (цифровому) форматі [7].

Більш детальну інтерпретацію поняття «інформація» подано в Законі України «Про захист економічної конкуренції». Відповідно до цього акта, інформацією вважаються відомості, представлені в будь-якій об'єктивній формі та закріплені на різноманітних носіях. До них належать, зокрема, документація та листування, друковані видання, схематичні зображення (карти, діаграми, органіграми), аудіовізуальні матеріали (фотографії, кіноплівки, відеозаписи, голограми), а також бази даних інформаційних систем та особисті пояснення осіб чи інші форми публічного або документованого оприлюднення відомостей [9].

Виходячи з наведених підходів, інформацію доцільно розуміти як дані, залучені до процесу комунікації, а посягання на неї – як порушення як змісту відомостей, так і можливості їх вільної передачі. Оскільки за своєю суттю інформація детермінована на активне розповсюдження та практичне застосування, її функціонування поза межами трансляції та сприйняття адресатом є лише умовною абстракцією. Це зумовлює сучасний науковий підхід до трактування інформації через її операційну здатність – можливість суб'єкта оперувати певними відомостями.

У практичному вимірі інформація постає як повідомлення, спрямоване на передання знань про ідеї, події або стан справ, адже у статичному вигляді вона втрачає функціональну цінність і зводиться до простого масиву даних. Відтак інформацію слід розглядати комплексно – як поєднання відомостей і даних, процесів їх комунікації та суб'єктивного сприйняття.

З правової позиції інформація є особливою нематеріальною субстанцією, що формує соціально-правові відносини щодо володіння,

використання, поширення й передачі відомостей, які підлягають правовій охороні. У цьому сенсі захист інформації охоплює розроблення та застосування правових норм, спрямованих на забезпечення інформаційних прав і законних інтересів держави, фізичних та юридичних осіб, а також інститутів громадянського суспільства (далі – ІГС).

У словнику Б. Д. Грінченка «безпека» визначена як «стан, коли кому-, чому-небудь ніщо не загрожує» [10, с. 101]. Д. О. Беззубов виокремлює низку універсальних ознак поняття «безпека», що розкривають її сутнісні характеристики, зокрема сталість, системність, структурованість, альтернативність, визначеність, орієнтацію на досягнення конкретного результату, результативність, статичність, індивідуальну та колективну спрямованість, а також прогнозованість [11, с. 60].

Характер безпеки варіюється залежно від її типу, що вимагає розробки складної термінологічної системи для їх опису [12, с. 115] Різноманіття проявів безпеки об’єктивно потребує їх систематизації за відповідними критеріями, оскільки окремі види тісно взаємопов’язані та здатні трансформуватися. Л. М. Стрельбицька, М. П. Стрельбицький класифікують види безпеки за сферами [12, с. 116]: військова, економічна, інформаційна, політична, соціальна, духовна, ідеологічна, гуманітарна, фізична, моральна, майнова, психологічна, екологічна, техногенна, транспортна, виробнича, трудова, правова та інші, серед яких ключову роль у цьому дослідженні відіграє інформаційна безпека.

Водночас у науковій літературі, попри значну кількість дефініцій інформаційної безпеки, відсутній єдиний узгоджений підхід до розуміння її змісту, що зумовило формування різних концептуальних позицій. Найбільш розгорнуту класифікацію таких підходів запропонував В. А. Ліпкан, узагальнивши їх у три основні групи: розуміння інформаційної безпеки як сталого явища (статичний підхід), як динамічного процесу (процесний підхід) та як складової ширшої системи (системний підхід) [13, с. 25–30].

У межах традиційного статичного підходу дослідники акцентують увагу на стані захищеності різних сегментів інформаційної сфери. Зокрема, Ю. Д. Кунєв пов'язує інформаційну безпеку з якісними характеристиками систем обігу інформації, що дозволяють ефективно задовольняти потреби суб'єктів [14, с. 96]. Своєю чергою, О. А. Ніщименко та Л. О. Кочубей розглядають цю категорію через призму захисту національних інтересів України від деструктивних впливів, які можуть перешкоджати стабільному прогресу особистості й держави [15, с 19; 16, с. 221–222]. Б. А. Кормич доповнює ці погляди акцентом на правовій складовій, визначаючи безпеку як стан дотримання законодавчих норм, що регулюють інформаційні відносини [17, с. 142].

В. Т. Шатун, О. В. Гладун та О. П. Баранов пропонують деталізований перелік чинників, від яких має бути захищений інформаційний простір. До них вони відносять не лише несанкціоноване використання даних, а й такі загрози, як неактуальність, недостовірність або неповнота відомостей, що разом із негативними технологічними наслідками можуть зашкодити національним інтересам [18, с. 175; 19, с. 60–62]. Натомість Н. Р. Нижник та співавтори зосереджуються на інституційному аспекті, трактуючи безпеку як систему правових інститутів, що гарантують наявність стратегічно важливих даних [20, с. 21].

С. С. Єсімов та О. Г. Ярема аргументують статус інформаційної безпеки як автономного правового явища, структура якого охоплює механізми доступу до обмеженої інформації, ліцензування захисної діяльності та юридичну відповідальність за порушення у цій царині [21, с. 247–248]. К .І. Бєляков посилює цю тезу, наголошуючи, що захищеність сфери має бути не лише технічною, а насамперед правовою [22, с. 255].

Аналізуючи правову природу досліджуваного явища, особливої уваги заслуговує позиція О. О. Заярного. Автор обґрунтовує пріоритетність захисту інформаційних прав особи, що набуває критичного значення в умовах цифрової трансформації та правового режиму воєнного стану. Досліджуючи практику, яку формує Європейський суд з прав людини (далі – ЄСПЛ), вчений акцентує на

необхідності дотримання балансу між вимогами національної безпеки та фундаментальними гарантіями приватності й доступу до даних [23, с. 94].

Такий підхід формує сучасний вектор розвитку наукової думки, зміщуючи акцент із суто охоронної моделі на правозахисну парадигму, де інформаційна безпека виступає дієвим інструментом забезпечення конституційних свобод.

Законодавче закріплення поняття «інформаційна безпека» еволюціонувало від розуміння її як стану захищеності інтересів від технічних і змістовних загроз (згідно із Законом України «Про Основні засади розвитку інформаційного суспільства в Україні на 2007-2015 роки» [24]) до більш комплексного трактування в чинній Стратегії інформаційної безпеки. В останній вона розглядається як невід'ємна складова нацбезпеки, що гарантує суверенітет, територіальну цілісність та конституційні права громадян на об'єктивну інформацію, водночас забезпечуючи стійкість перед деструктивною пропагандою та ворожими інформаційними операціями [25].

В межах другого концептуального напряму (процесного підходу) інформаційна безпека інтерпретується не як статичний стан, а як динамічна система суспільних відносин та безперервний процес протидії загрозам. Зокрема, А. В. Бабінська та В. С. Цимбалюк акцентують увагу на нормативному регулюванні балансу прав і обов'язків суб'єктів інформаційного простору в контексті захисту їхнього суверенітету [26, с. 28]. Схожої позиції дотримується В. І. Гурковський, який розглядає інформаційну безпеку як фундамент для збереження соціокультурних цінностей нації та прогресивного державотворення [27, с. 74]. Р. А. Калюжний розширює це розуміння, визначаючи її як специфічний вид правовідносин, що виникають у процесі створення, обігу та охорони інформації [28, с. 18–19], тоді як В. А. Ліпкан із співавторами фокусують увагу на управлінському аспекті – діяльності інституцій щодо нівелювання небезпек [13, с. 75].

Третій концептуальний вектор (системний підхід) позиціонує інформаційну безпеку як стратегічну функцію держави та органічну складову

загальної архітектури національної безпеки [13, с. 25–30]. Ця позиція корелює із приписами ст. 17 Конституції України, де гарантування інформаційної стійкості визначено серед пріоритетних завдань всього суспільства та владних інституцій [1]. В такому контексті категорія, що досліджується, постає результатом скоординованого державного управління, спрямованого на реалізацію національних пріоритетів в інформаційній сфері. Даний підхід також імплементовано в положеннях профільних законів, зокрема «Про національну безпеку України» та Концепції Національної програми інформатизації, де інформаційна безпека розглядається в нерозривній єдності з політичною, економічною та оборонною стабільністю [29; 30].

Розвиваючи системне бачення, І. В. Бондар пропонує багаторівневу структуру безпеки, що інтегрує персональний, публічний, корпоративний та державний сектори [31, с. 72]. П. В. Цимбал та А. М. Лисеюк доповнюють цей аналіз через категорію балансу: на їхню думку, держава має одночасно забезпечувати відкритість якісної інформації для громадян та захищати національний медіапростір від зовнішніх маніпуляцій і ведення інформаційної війни [32, с. 25].

Сучасний етап розвитку наукової думки характеризується переходом до четвертої групи – комплексного (комбінованого) підходу. Т. Ю. Ткачук обґрунтовує доцільність об’єднання статичних і динамічних ознак, трактуючи безпеку як стан, що гарантує самозбереження інфраструктури та ресурсів в умовах постійного впливу реальних загроз [33, с. 77–78]. О. О. Золотар також наголошує на недоцільності вузького тлумачення, пропонуючи аналізувати інформаційну безпеку як багатовимірне явище, що враховує постійну трансформацію соціальних систем [34, с. 145]. Критичний перегляд традиційної парадигми пропонує І. Ф. Корж, який закликає відійти від виключно «охоронного» розуміння («захищеності») на користь моделі «збалансованого функціонування», де пріоритетом є розвиток інформаційного простору в інтересах особи та суспільства [35, с. 38].

Таким чином, еволюція наукових поглядів дозволяє доповнити класичну трикомпонентну класифікацію В. А. Ліпкана четвертим, інтегральним підходом. Це відображає складну природу інформаційної безпеки як комплексного державно-правового феномену, що поєднує в собі стан, процес і функцію. Систематизацію цих підходів за їхніми ключовими характеристиками відображено в табл. 1.1.1.

Таблиця 1.1.1

Основні сучасні підходи до визначення дефініцій поняття «інформаційна безпека» (за спільними ознаками)

№ з/п	Концептуальні підходи	Основні ідеї	Представники / джерела
1.	Статичний	Розгляд безпеки як стабільного стану захищеності інформаційної сфери, національних інтересів та законодавчо визначених правил здійснення інформаційних процесів	Ю.Д. Кунєв [14], О.А. Ніщименко [15], Л.О. Кочубей [16], Б.А. Кормич [17], О.П. Баранов [19]; ЗУ від 09.01.2007 № 537-V [24], Стратегія інформаційної безпеки [25].
2.	Процесний	Трактування безпеки як динамічної системи відносин та безперервної діяльності (процесу) щодо відсічі загрозам задля збереження інформаційного суверенітету	А.В. Бабінська, В.С. Цимбалюк [26], В.І. Гурковський [27], Р.А. Калюжний [28], В.А. Ліпкан [13]
3.	Системний	Розуміння безпеки як стратегічної функції держави та невід'ємного елемента загальної архітектури національної безпеки (у єдності з політичною та економічною сферами)	І.В. Бондар [31], П.В. Цимбал, А.М. Лисеюк [32]; Конституція України [1], ЗУ від 21.06.2018 № 2469-VIII [29], ЗУ від 04.02.1998 № 75/98-ВР [30]
4.	Комплексний	Інтегральний підхід, що поєднує ознаки стану, процесу та функції для забезпечення сталого розвитку інформаційної сфери та правозахисного виміру безпеки	Т.Ю. Ткачук [33], О.О. Золотар [34], І.Ф. Корж [35], О.О. Заярний [23]

Джерело: складено автором на основі аналізу [13–35].

Водночас узагальнена класифікація концептуальних підходів до розуміння інформаційної безпеки, навіть із урахуванням її доповнення комбінованим (комплексним) підходом, не вичерпує всієї методологічної багатоманітності наукових інтерпретацій цієї категорії. З огляду на

міжгалузевий характер інформаційних процесів і багатовимірність загроз інформаційній сфері, у сучасній науці сформувалися більш деталізовані методологічні підходи, що дають змогу глибше розкрити окремі аспекти інформаційної безпеки.

У цьому контексті особливої уваги заслуговує підхід І. М. Шопіної, яка, виходячи з трансдисциплінарної природи інформаційної безпеки, представляє розгалужену матрицю методологічних орієнтирів для аналізу даного феномену [36, с. 137]. Такий підхід не лише деталізує загальні концептуальні моделі, а й дає змогу простежити, як інформаційна безпека постає одночасно як стан, процес, вид правовідносин, інструмент публічного управління та елемент суб'єктивного сприйняття. Узагальнений перелік відповідних методологічних підходів подано в таблиці 1.1.2.

Таблиця 1.1.2

Методологічні підходи до розуміння сутності інформаційної безпеки

(за І. М. Шопіною [36])

№ з/п	Підходи	Розуміння інформаційної безпеки
1.	Статусний	Характеризує поточну кондицію інформаційних ресурсів або ступінь їхньої захищеності від деструктивних чинників
2.	Диференційний	Передбачає розмежування ступенів безпеки залежно від специфіки суб'єкта та часових параметрів через систему процедурних дій
3.	Реляціоналістський	Специфічна категорія суспільних відносин у медіапросторі, що регулюються нормами права задля досягнення стабільності системи
4.	Інструментальний	Сукупність прикладних засобів та методів, що дозволяють реалізувати цілі управлінського впливу в інформаційній сфері
5.	Протекціоністський	Комплексна безпека програмно-апаратного базису та операційних процесів з метою підтримки цілісності та конфіденційності даних
6.	Збережувально-забезпечувальний	Фокусується на підтримці фундаментальних властивостей інформації: від її автентичності до безвідмовності доступу
7.	Процесуальний	Динамічна послідовність процесів у соціальних структурах, що забезпечують виконання функцій публічного управління
8.	Концептуальний	Визначає здатність інформаційних систем зберігати функціональність під тиском внутрішніх чи зовнішніх загроз
9.	Діяльнісний	Інтерпретує безпеку через активну практику маніпулювання інформаційними ресурсами або їх цілеспрямований захист
10.	Екзистенційний	Аналізує внутрішній психологічний стан та суб'єктивне сприйняття рівня захищеності конкретною особою

Аналіз наведених наукових підходів до трактування поняття «інформаційна безпека» дає підстави розглядати її як складне та багатовимірне явище, визначення якого ускладнюється низкою чинників. Передусім це пов’язано з умовами її формування, що детермінуються суспільним розвитком та процесами інформатизації. Попри динамічний характер останніх, вони залишаються недостатньо осмисленими в контексті сучасних глобальних викликів. Водночас українська специфіка забезпечення інформаційної безпеки значною мірою визначається впливом російсько-української війни, що проявляється у кібератаках, інформаційно-пропагандистських кампаніях та поширенні дезінформації з метою дестабілізації суспільних процесів.

Різноманіття наукових підходів зумовлене трансдисциплінарним характером цього явища, яке перебуває на перетині технічних, правових, соціокультурних і психологічних досліджень. Це, своєю чергою, ускладнює формування єдиного узгодженого підходу до його визначення.

З огляду на це, для цілей даного дослідження доцільно узагальнити основні підходи до розуміння інформаційної безпеки, що склалися у сучасній науковій думці [2–36]:

технічний підхід, який акцентує увагу на застосуванні інженерно-технологічних рішень для запобігання, виявлення та нейтралізації інформаційних загроз;

гуманітарний підхід, що орієнтований на захист суспільних цінностей і конституційних прав, а також формування відповідних світоглядних і методологічних засад;

нормативний підхід, у межах якого ключова увага приділяється правовому регулюванню та закріпленню механізмів захисту інформаційного простору;

психологічний підхід, який зосереджується на забезпеченні захисту психіки людини від деструктивних інформаційних впливів.

Запропонована авторська систематизація наукових підходів дає змогу розмежувати концепції розуміння інформаційної безпеки держави за двома ключовими напрямами: за сутнісними характеристиками (статичний,

системний, процесно-діяльнісний і комплексний), що відображено на рис. 1.1.1; а також за трансдисциплінарною основою (технічний, гуманітарний, нормативний і психологічний), як показано на рис. 1.1.2.

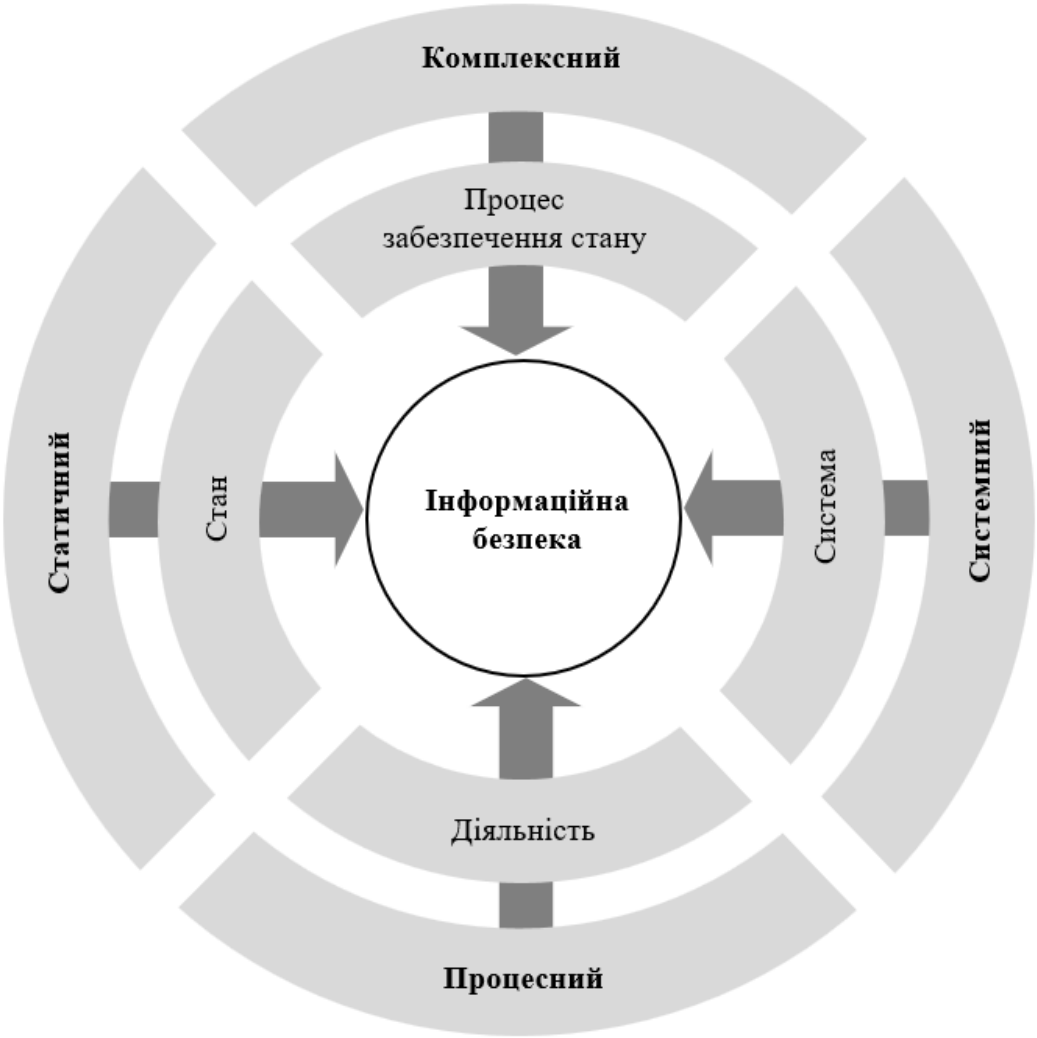


Рис. 1.1.1. Підходи до визначення дефініцій поняття «інформаційна безпека» (за сутнісними ознаками)

На наше переконання, найбільш релевантним для сучасних реалій є саме комплексний підхід. У першому випадку він виступає синтезом статичного та діяльнісного елементів (рис. 1.1.1), а у другому – постає як цілісна парадигма, що гармонізує правові, технологічні та соціально-психологічні аспекти захисту національного інформаційного простору (рис. 1.1.2). Саме такий багатовимірний погляд дозволяє нам сформулювати авторську дефініцію інформаційної безпеки.

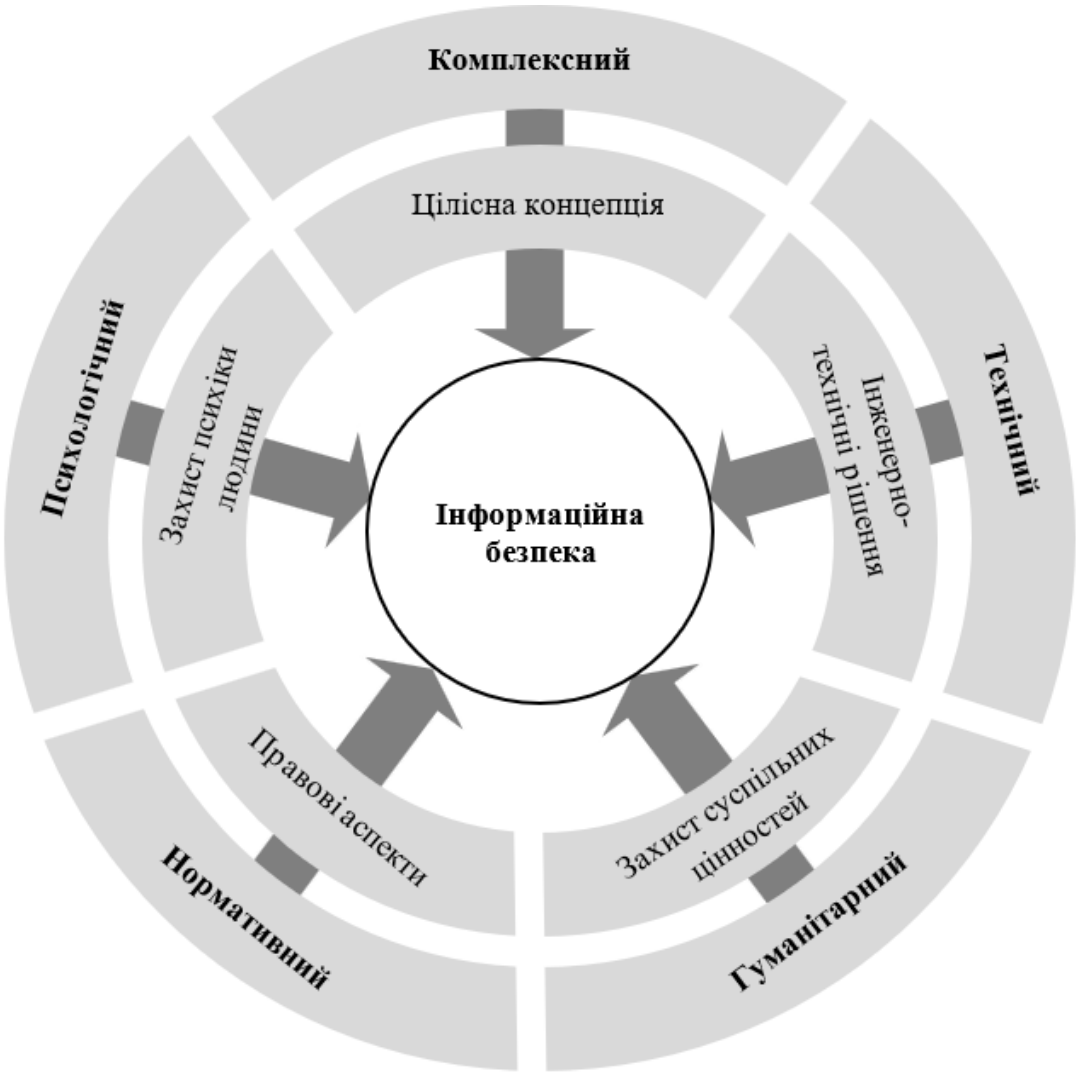


Рис. 1.1.2. Підходи до визначення дефініцій поняття «інформаційна безпека» (за трансдисциплінарною природою)

Саме з точки зору комплексного підходу вбачається за доцільне інформаційну безпеку держави розглядати як нормативно закріплений стан захищеності національного інформаційного простору, за якого забезпечується: стійкість інформаційної інфраструктури та цілісність інформаційних ресурсів; стабільність інформаційних процесів і захист прав суб’єктів інформаційних відносин; збереження національної ідентичності; реалізація національних інтересів і досягнення стратегічних цілей в інформаційній сфері; створення умов для сталого розвитку інформаційного суспільства.

Використання конструкції «нормативно закріплений стан» акцентує увагу на домінантній ролі правового компонента у структурі інформаційної безпеки. Останній виражається через розгалужену систему юридичних норм та дієвих механізмів їх імплементації в межах охоронної та регулятивної функцій держави під час здійснення інформаційної діяльності [14, с. 98].

Оскільки інформаційна діяльність постає фундаментальним видом соціальної активності, вона об’єктивно потребує цілеспрямованого правового впорядкування, виступаючи при цьому безпосереднім об’єктом регулятивного впливу [37, с. 16].

У свою чергу, правове забезпечення безпеки інформаційної сфери доцільно розглядати як невід’ємну частину предмета інформаційного права, що функціонує в системі адміністративно-правової галузі [14, с. 98]. По суті, заходи із гарантування інформаційної безпеки інтегровані в інформаційну діяльність на всіх її ієрархічних рівнях. Відповідно, норми, що регламентують цей процес, входять до складу адміністративного права (зокрема, його інформаційно-адміністративного підмасиву), що забезпечує нормативне регулювання відносин, пов’язаних із підтриманням належного рівня безпеки в державі [14, с. 99].

Враховуючи вищезазначене, а також запропонований підхід до розуміння інформаційної безпеки держави, в основу якого покладено принцип активного захисту, який виходить за межі пасивних оборонних стратегій, під забезпеченням інформаційної безпеки держави слід розуміти складову інформаційної діяльності на всіх рівнях і сферах, що реалізується як постійний процес організованої діяльності державних інституцій та суспільства, спрямований на проактивне виявлення, запобігання та нейтралізацію реальних і потенційних загроз шляхом вжиття комплексних заходів інформаційного впливу та захисту, створення ефективної системи моніторингу, контролю та управління ризиками, що забезпечує стабільне функціонування національного інформаційного простору у довгостроковій перспективі [11, с. 98–99; 46, с. 16].

З’ясування доктринальних підходів до розуміння інформаційної безпеки держави, її сутнісних ознак та місця в системі національної безпеки створює необхідне теоретико-методологічне підґрунтя для подальшого дослідження правових засобів її забезпечення. У зв’язку з цим подальше дослідження доцільно зосередити на з’ясуванні сутності та структури адміністративно-правового механізму забезпечення інформаційної безпеки держави як ключового інструменту реалізації відповідної державної політики та трансформації нормативних приписів у практичну діяльність.

Забезпечення інформаційної безпеки держави реалізується за допомогою адміністративно-правових засобів у процесі здійснення публічної владної діяльності, що зумовлює необхідність подальшого аналізу відповідного механізму.

1.2. Адміністративно-правовий механізм забезпечення інформаційної безпеки держави: сутність та структура

Забезпечення інформаційної безпеки держави як складової національної безпеки не зводиться виключно до формування доктринальних підходів чи нормативного закріплення відповідних дефініцій. Реалізація задекларованих у цій сфері цілей потребує функціонування цілісного механізму, здатного забезпечити практичне втілення державної політики, узгодженість дій суб’єктів публічного управління, а також ефективну протидію реальним і потенційним загрозам національному інформаційному простору.

У сучасних умовах провідна роль у забезпеченні інформаційної безпеки належить адміністративно-правовому механізму, оскільки основний обсяг повноважень щодо формування, реалізації та контролю державної політики в інформаційній сфері зосереджений у системі органів публічної влади. Саме адміністративно-правові засоби визначають порядок діяльності відповідних суб’єктів, встановлюють правові режими функціонування інформаційної інфраструктури, регламентують процедури управлінського впливу та

забезпечують юридичну відповідальність за порушення вимог інформаційної безпеки.

Разом з тим, сучасний науковий дискурс характеризується поліаспектністю трактувань природи адміністративно-правового механізму забезпечення інформаційної безпеки держави. Наукові розвідки демонструють широкий спектр інтерпретацій: від нормативного розуміння механізму як масиву правових приписів до його сприйняття крізь призму архітектури суб'єктів владних повноважень чи функціонально-процесуального алгоритму втілення державних пріоритетів. Така різноманітність підходів зумовлює необхідність комплексного адміністративно-правового аналізу зазначеного механізму, з'ясування його структурних елементів і функціонального призначення.

Перш ніж перейти до розгляду сутності та структури адміністративно-правового механізму забезпечення інформаційної безпеки держави, а також визначення його місця в ієрархічній системі державного управління, доцільно уточнити термінологічний апарат дослідження, зокрема такі базові поняття, як: «забезпечення», «забезпечення інформаційної безпеки», «система», «система забезпечення інформаційної безпеки», «механізм», «механізм держави», «механізм державного управління», «адміністративно-правовий механізм». Аналіз зазначених категорій є необхідною передумовою методологічно коректного дослідження.

З метою окреслення особливостей розуміння поняття «забезпечення інформаційної безпеки» у межах даного дослідження доцільно насамперед звернутися до тлумачення категорії «забезпечення» в загальномовному значенні.

У тлумачних словниках поняття «забезпечення» розкривається через кілька взаємопов'язаних значень, а саме: акумулювання необхідних ресурсів задля задоволення конкретних суспільних запитів; формування стабільного підґрунтя для реалізації визначених видів активності; гарантування

досягнення цільових орієнтирів та захист від потенційних деструктивних чинників [38, с. 375].

Дослідження понятійного апарату в юридичній та економічній площинах, у змісті яких використовується категорія «забезпечення», дозволяє констатувати дещо відмінні підходи до її тлумачення. По-перше, забезпечення розглядається як комплекс заходів і засобів, спрямованих на створення умов для належного функціонування певної системи та/або належного перебігу відповідних процесів. По-друге, забезпечення трактується як діяльність, пов'язана зі створенням необхідних засобів і застосуванням сукупності заходів та інструментів для досягнення визначеної мети.

У межах академічного дискурсу домінує інклюзивне бачення цієї категорії, що інтегрує згадані підходи з акцентом на активній, діяльнісній природі гарантування безпеки. Такий методологічний висновок має фундаментальне значення для подальшої декомпозиції адміністративно-правового інструментарію забезпечення інформаційної безпеки держави.

Розкриваючи сутність безпекових процесів, В. А. Предборський зазначає, що активність у цій царині є особливим соціальним феноменом. Її поява обумовлена прагненням нівелювати суперечності між актуальними загрозами та базовими інтересами особи, суспільства й державних інституцій. Науковець акцентує, що практична реалізація подібних заходів спирається на стратегії превентивного впливу, локалізації та нейтралізації деструктивних факторів [39, с. 13].

Подальшого розвитку діяльнісний підхід набуває у запропонованій В. А. Предборським концепції двомірності забезпечення безпеки. Відповідно до неї діяльність у цій сфері має два взаємопов'язані та взаємообумовлені виміри. Горизонтальний вимір охоплює забезпечення безпеки особи, підприємств, установ, держав і регіонів, тоді як вертикальний вимір пов'язаний із забезпеченням окремих видів безпеки – політичної, військової, інформаційної, економічної, науково-технічної тощо [39, с. 14].

Варто наголосити, що попри первинне формулювання наведених дедуктивних висновків у межах вивчення проблем економічної безпеки України, вони мають універсальний характер. Методологічно виправданим є їх екстраполяція на сферу інформаційної безпеки, адже зазначені положення відображають фундаментальні закономірності та ідентичні за своєю природою механізми функціонування базових елементів, що формують цілісну систему національної безпеки держави

У цьому контексті показовою є позиція П. Д. Біленчука, Л. В. Борисової, І. М. Неклонського та В. О. Собини, які пропонують розглядати процес забезпечення державної безпеки як специфічну форму активності у системі національної безпеки. Дослідники акцентують увагу на тому, що така діяльність реалізується через розгалужену архітектуру владних інституцій та військових формувань із залученням широкого інструментарію: від правових та організаційних засобів до спеціальних режимних, розвідувальних, оперативно-технічних та службово-бойових заходів, спрямованого на захист об’єктів державної безпеки [40, с. 14]. Запропоноване визначення ґрунтується на поширеному в науці підході до розуміння забезпечення як особливого виду діяльності, однак у чинному законодавстві України воно не отримало прямого нормативного закріплення.

У свою чергу, О. О. Тихомиров, розвиваючи діяльнісний підхід, пропонує інтерпретувати державне забезпечення інформаційної безпеки як сукупність встановлених державою гарантій в інформаційній сфері, що прямо або опосередковано випливають із базових законодавчих актів, покликаних регулювати суспільні відносини в інформаційній сфері [41, с. 72]. Запропоноване визначення акцентує увагу на нормативно-гарантійному характері діяльності держави у сфері інформаційної безпеки.

Схожі погляди поділяють В. А. Ліпкан, Ю. Є. Максименко та В. М. Желіховський, які акцентують увагу на тому, що забезпечення інформаційної безпеки є результатом усвідомленої та цілеспрямованої діяльності органів державного управління. На думку авторів, така діяльність

спрямована на превенцію можливого порушення їх функціонування внаслідок дії деструктивних факторів [42, с. 161]. У цьому контексті забезпечення інформаційної безпеки трактується як постійний управлінський процес, інтегрований у систему державного управління.

А. Ю. Нашинець-Наумова, залишаючись у межах діяльнісної парадигми, під забезпеченням інформаційної безпеки розуміє «сукупність заходів, орієнтованих на захист інформаційних інтересів людини, суспільства та держави». Головною метою такої активності дослідниця визначає «гарантування інформаційного суверенітету України та захист її інформаційної системи від внутрішніх та зовнішніх загроз» [43, с. 50]. Такий підхід підкреслює стратегічний вимір забезпечення інформаційної безпеки та її зв’язок із суверенітетом держави.

У межах дослідження правового забезпечення інформаційної безпеки в умовах євроінтеграції України Т. Ю. Ткачук зазначає, що забезпечення інформаційної безпеки України варто розглядати як багатогранну та комплексну категорію. Вона інтегрує у собі сукупність динамічних процесів, спрямованих на нейтралізацію викликів і загроз безпеці національних інтересів в інформаційній сфері [33, с. 114].

Подальшого розвитку комплексно-діяльнісний підхід набуває у працях Т. С. Перуна. Дослідник інтерпретує забезпечення інформаційної безпеки як специфічний за своєю природою соціально-правовий механізм. Його функціонування полягає у виробленні та впровадженні державної стратегії, що має на меті підтримку необхідного ступеня захисту об’єктів безпеки. Це досягається через реалізацію цілісної системи заходів – від нормативного регулювання та організаційного впливу до управлінських та інших інструментів, що відповідають актуальним загрозам життєво важливим інтересам особи, суспільства та держави в інформаційній сфері [44, с. 52].

Зі свого боку, Р. В. Бондаренко акцентує увагу на інституційно-інструментальному вимірі забезпечення інформаційної безпеки. Дослідник підкреслює, що відповідна діяльність реалізується через узгоджене

функціонування різних гілок державної влади – зокрема законодавчої, правоохоронної, судової та контрольної – у тісній взаємодії з органами місцевого самоврядування, а також іншими суб'єктами, включаючи організації та громадян [45, с. 98]. При цьому механізм забезпечення інформаційної безпеки держави, за позицією автора, ґрунтується на використанні органами виконавчої влади комплексу адміністративно-правових інструментів. Йдеться, передусім, про дозвільні процедури, що охоплюють надання дозволів на здійснення діяльності, пов'язаної з державною таємницею, а також застосування стандартизації, ліцензування і легалізації. Окреме місце займають реєстраційні механізми, зокрема оформлення ЗМІ та ведення державних реєстрів персональних даних. Водночас важливою складовою виступають заходи адміністративного примусу, включаючи застосування юридичної відповідальності адміністративного характеру [45, с. 98].

Аналіз вітчизняного правового поля свідчить про те, що попри інтенсивне оперування категорією «забезпечення інформаційної безпеки», її нормативна детермінація залишається фрагментарною та позбавленою належної деталізації. Зокрема, Стратегія національної безпеки України, окреслюючи фундаментальні засади захисту в інформаційній сфері, протидії викликам та захист персональних даних, фактично не пропонує дефінітивного розкриття самого терміна «забезпечення» [46].

Аналогічна ситуація простежується і в інших стратегічних актах. Так, Доктрина інформаційної безпеки України (пп. 5, 6) згадує про цей процес крізь призму пріоритетних векторів державної активності, проте утримується від його термінологічного формулювання [47]. Понад те, навіть у профільній Стратегії інформаційної безпеки, де вказана діяльність позиціонується як одна з ключових функцій держави, чітке нормативне визначення поняття так і не було закріплено [25].

Варто зазначити, що аналіз такої категорії, як « інформаційна безпека» у попередньому підрозділі (1.1) створив методологічні передумови для формування авторського підходу до розуміння її забезпечення.

З урахуванням наведеного, забезпечення інформаційної безпеки держави – це складова інформаційної діяльності на всіх рівнях і сферах, що реалізується як постійний процес організованої діяльності державних інституцій та суспільства, спрямований на проактивне виявлення, запобігання та нейтралізацію реальних і потенційних загроз шляхом вжиття комплексних заходів інформаційного впливу та захисту, створення ефективної системи моніторингу, контролю та управління ризиками, що забезпечує стабільне функціонування національного інформаційного простору у довгостроковій перспективі.

Запропоноване визначення відображає комплексне бачення забезпечення інформаційної безпеки як безперервної управлінської діяльності та може бути використане як базове у подальшому дослідженні адміністративно-правового механізму.

Перехід до безпосереднього аналізу змістовних параметрів адміністративно-правового механізму забезпечення інформаційної безпеки держави потребує попереднього методологічного уточнення ряду вихідних дефініцій. Зокрема, логічно виправданим вбачається з’ясування природи таких категорій, як «механізм», «механізм держави» та «механізм державного управління», що складають основу досліджуваного явища.

Поняття «механізм» відзначається високим ступенем міждисциплінарної затребуваності, що спричинило формування вагомого теоретичного доробку, присвяченого його багатоаспектному тлумаченню. В узагальненому філософському трактуванні під механізмом розуміють цілісну систему структурних компонентів, що перебувають у безперервному функціональному взаємозв’язку та динамічній взаємодії [49, с. 377].

Згідно з фундаментальними лексикографічними джерелами, поняття «механізм» розкривається через систему внутрішньої будови об’єкта або

сукупність процесів, які формують певне явище (фізичного чи соціального характеру) [38, с. 398]. Як слушно зауважує О. М. Литвинов, попри технічне походження цього терміну, де він асоціюється з динамічним з'єднанням частин для виконання заданого руху, у правовій площині він трансформується у систему функціональних зв'язків із чітко детермінованими параметрами управлінського впливу [49, с. 93–94].

Дистанціюючись від виключно технічного сприйняття даної категорії, С. І. Крук акцентує на тому, що в межах політико-правового дискурсу механізми слід розглядати не як фізичну даність, а як складну архітектуру прав, обов'язків та легітимних процедур. Автор акцентує, що специфіка такого механізму базується на державній владі, орієнтуючись на її поділ та систему стримувань і противаг задля запобігання узурпації владних повноважень [50, с. 9]. Подібну логіку простежуємо у працях І. І. Фуртак, яка трактує механізм як природну систему з обов'язковою послідовністю вхідних та вихідних явищ [51, с. 203].

Більш деталізований перелік ознак пропонує О. В. Радченко, вказуючи, що будь-який механізм є продуктом свідомої організації, має чітку векторну спрямованість, характеризується жорстким взаємозв'язком елементів та в ідеалі прагне до автоматизму у функціонуванні [52, с. 10]. Таким чином, юридичний механізм постає не просто як сукупність засобів, а як динамічна конструкція, що конвертує ресурси у конкретний управлінський ефект.

Цей підхід знаходить своє відображення в теорії публічного управління. Зокрема, Н. Р. Нижник та О. А. Машкова визначають управлінський механізм як невід'ємну частину системи, що забезпечує цілеспрямований вплив на внутрішні та зовнішні фактори діяльності об'єкта [53, с. 37, 49]. Своєю чергою, С. В. Петрова пропонує розрізняти статичний аспект (механізм як інструментарій) та динамічний аспект (механізм як безпосереднє функціонування) управлінських процесів [54, с. 16].

В юридичній доктрині категорія «механізм» найчастіше корелює з процесами правового регулювання. О. Ф. Скакун інтерпретує його як консолідовану систему правових форм і методів, за допомогою яких нормативні

приписи трансформуються в упорядкованість суспільного життя [55, с. 498–499]. Цю думку розвивають О. В. Зайчук та Н. М. Оніщенко, наголошуючи, що саме через механізм правового регулювання забезпечується соціальний компроміс та розв'язання конфліктів у правовій сфері [56, с. 114–115]. Отже, у правовій теорії механізм виступає головним транслятором «права на папері» у реальну соціальну практику.

Традиційні підходи, запропоновані В. В. Копейчиковою, акцентували увагу на організаційно-структурній стороні, розглядаючи механізм як систему державних інституцій, підприємств та установ, що реалізують функції держави [57, с. 212]. Проте сучасні дослідники, як-от А. В. Рубан та В. О. Шведун, зміщують фокус на функціонально-діяльнісну складову, визначаючи механізм у сфері безпеки як систему превентивних заходів організаційного та правового характеру [58, с. 23].

Синтез цих моделей простежується у працях В. А. Ліпкана, Ю. Є. Максименка та В. М. Желіховського, які трактують державно-правовий механізм як узгоджену ієрархію інституцій, створених для реалізації інформаційної політики [42, с. 137]. Більш розгорнуту трикомпонентну модель пропонує Б. А. Кормич, виокремлюючи: інституціональний блок (державні структури); функціональний блок (ролі, форми та методи діяльності); правовий блок (ієрархія норм і принципів) [59, с. 132-133].

Інтегрований підхід підтримує і В. П. Приходько, розглядаючи механізм як складну систему «знарядь-процесів», що призначена для практичного втілення управлінських цілей [60, с. 61]. У цьому контексті Н. М. Ткачова справедливо додає, що до структури комплексного механізму мають входити економічний, мотиваційний, політичний та правовий підмеханізми [61, с. 14].

У сфері безпекознавства А. В. Кулінська та О. С. Зозуля визначають механізм як сукупність дій суб'єктів, спрямованих на залучення матеріальних та людських ресурсів задля захисту національних інтересів [62; 63]. При цьому В. В. Шемчук робить акцент на регламентації такої діяльності законодавством, що надає механізму легітимного характеру [64, с. 56].

На основі проведеного наукового аналізу ми пропонуємо власне трактування: механізм забезпечення інформаційної безпеки держави слід розглядати як системно впорядковану сукупність правових, організаційних, технічних та соціальних засобів, за допомогою яких уповноважені суб'єкти реалізують цілеспрямовану діяльність з: охорони інформаційного суверенітету (захист критичної інфраструктури, державних інформаційних ресурсів); протидії загрозам (кібератаки, дезінформація, зовнішній вплив, шпигунство); управління ризиками (моніторинг, прогнозування, адаптація до нових викликів); забезпечення стабільності інформаційного середовища.

Саме така дефініція слугуватиме методологічним підґрунтям для подальшого розкриття архітектоніки адміністративно-правового механізму в межах нашого дисертаційного дослідження.

Категорія «механізм забезпечення інформаційної безпеки» перебуває у тісному гносеологічному зв'язку із поняттям «система забезпечення інформаційної безпеки», проте ці дефініції не є тотожними. В науковому дискурсі інформаційна безпека нерідко аналізується саме крізь призму її структурної декомпозиції на окремі елементи.

Етимологічно термін «система», що має грецьке коріння, позначає інтегровану сукупність частин, об'єднаних у монолітне ціле. У філософському вимірі ця категорія відображає цілісність, яка формується завдяки стійким зв'язкам та організації різнорідних елементів чи процесів. При цьому властивості системи як цілісного утворення якісно відрізняються від простої суми характеристик її компонентів. Системоутворюючі зв'язки, зумовлені об'єктивними закономірностями, формують внутрішню архітектуру (структуру) системи, забезпечуючи її стабільне функціонування [65, с. 26–27].

Розглядаючи прикладні аспекти, В. А. Ліпкан, Ю. Є. Максименко та В. М. Желіховський трактують систему забезпечення інформаційної безпеки як комплекс адміністративно-правових, організаційних та спеціальних заходів, що мають на меті гарантування сталого розвитку об'єктів безпеки та відповідної інфраструктури [42, с. 158]. Своєю чергою, А. Ю. Нашинець-

Наумова робить акцент на внутрішній впорядкованості та диференціації складових цієї системи (суб'єктів, об'єктів, загроз), хоча й залишає певну термінологічну незавершеність щодо сутності самої структури [43, с. 142].

На наше переконання, система забезпечення інформаційної безпеки постає як більш широка категорія. Вона охоплює сукупність взаємопов'язаних елементів, які, попри автономність, активно взаємодіють із зовнішнім середовищем для реалізації специфічних безпекових завдань.

У цьому контексті механізм забезпечення інформаційної безпеки доцільно інтерпретувати як функціонально-динамічну складову зазначеної системи. Якщо система характеризує статичну архітектуру (хто і що?), то механізм відображає інструментальний спосіб її життєдіяльності (як саме?). Він консолідує методи, процедури та адміністративно-правові інструменти, завдяки яким здійснюється практичний вплив на об'єкт захисту.

Подібну логіку співвідношення простежуємо у працях Л. О. Євдоченка, який розглядає державну систему безпеки як багатокомпонентний апарат реалізації національних інтересів [66, с. 5]. Ю. П. Лісовська також підкреслює, що фундаментом такої системи є конституційні норми, а її «двигуном» – органи та засоби, що забезпечують стабільність державного управління через адміністративно-правові та аналітичні заходи [67, с. 11].

Цікавим є комплексний погляд О. С. Зозулі, яка включає до системи не лише державні інституції, а й структури громадянського суспільства, об'єднані спільними правовими та технологічними механізмами захисту [63, с. 44].

Підсумовуючи, у межах нашого дослідження під системою забезпечення інформаційної безпеки держави ми розуміємо інтегровану сукупність суб'єктів, об'єктів та взаємопов'язаних правових, організаційних і технічних механізмів, спрямовану на захист життєво важливих інтересів держави, суспільства та людини в інформаційному просторі.

Забезпечення інформаційної безпеки доцільно розглядати як один із напрямів державного управління, у межах якого реалізуються функції держави в інформаційній сфері. У цьому контексті державно-правовий механізм постає

як складне системне утворення, ключовими елементами якого виступають категорії «право» та «державний механізм» [68, с. 248–249]. Право відіграє визначальну роль у впорядкуванні суспільних відносин у державі. Саме через систему правових норм і встановлених державою правил організовується взаємодія суб'єктів соціальної системи, що забезпечує захист їхніх прав, свобод та законних інтересів як у межах окремих сфер суспільного життя, так і на рівні суспільства загалом. Водночас механізм держави забезпечує практичну реалізацію її функцій у різних сферах суспільного розвитку та на різних рівнях публічного управління. Через нього визначаються компетенція органів влади, правові засади їх діяльності, матеріально-організаційна основа функціонування, а також стратегічні орієнтири й пріоритети державної політики. На цьому наголошують і провідні дослідники адміністративного права. Зокрема, В. Б. Авер'янов, Ю. П. Битяк, В. М. Гаращук, О. В. Дьяченко та В. Я. Малиновський зазначають, що держава та її ключовий атрибут – державна влада – органічно пов'язані з процесами державного управління і становлять підґрунтя виникнення та функціонування відповідного механізму, через який реалізуються управлінські повноваження [69, с. 12; 70, с. 15, 25; 71, с. 6]. З огляду на те, що інформаційна безпека є складовою загальної системи безпеки держави та перебуває з нею у тісному взаємозв'язку, поняття «адміністративно-правовий механізм забезпечення інформаційної безпеки держави» обґрунтовано можна розглядати як спеціалізований прояв ширших категорій – «механізму держави» та «механізму державного управління» [69, с. 12, 18, 20]. Відповідно, функціонування системи забезпечення інформаційної безпеки, так само як і механізму її реалізації, є похідним від існування держави та відображає здійснення однієї з її базових функцій – інформаційної, спрямованої на захист національного інформаційного простору та стабільність інформаційних відносин у суспільстві [72, с. 95].

Так, К. Т. Томашкова зазначає, що «механізм державного управління системою економічної безпеки особистості полягає у впливі одного суб'єкта управління – держави – на інші (суспільство, особистість)» [73, с. 18].

Аналогічної позиції дотримується В. Р. Котковський, підкреслюючи, що державне регулювання економічної безпеки є специфічним видом державного управління, який охоплює соціально-економічну, політичну та інші сфери суспільного життя [74, с. 15]. Поділяючи цю наукову позицію, вважаємо за доцільне зазначити, що вона повною мірою застосовна й до сфери інформаційної безпеки. Водночас слід наголосити, що управлінський вплив і прийняття відповідних рішень здійснює не держава як абстрактний суб'єкт, а уповноважені органи державної влади [71, с. 299–300].

Підсумовуючи наведені міркування, логічним видається твердження, що будь-які інструментальні утворення, які мають публічну природу та покликані забезпечувати впорядкування соціально значущих сфер, знаходять своє практичне втілення через систему правових важелів у межах діяльності владних інституцій. У цьому контексті слушно зазначається, що втілення державної влади в практичну діяльність органів держави відбувається через функціонування державного механізму [75, с. 73].

Проведений теоретико-правовий аналіз дозволяє окреслити сукупність характерних рис адміністративно-правового механізму забезпечення інформаційної безпеки держави:

бере свій початок від державно-владних інституцій та визначається потребою в ефективному виконанні управлінських функцій в інформаційній сфері;

постає дієвим інструментом реалізації державної волі, що безпосередньо зумовлює його чітку спрямованість на здійснення публічного управління;

знаходить своє практичне втілення виключно через активність уповноважених органів та структур, що належать до державного апарату;

функціонує як цілісна архітектура взаємопов'язаних засобів, що дістають своє юридичне вираження в нормах чинного права;

має на меті впорядкування та гармонізацію соціальних зв'язків і відносин, що виникають в інформаційному середовищі;

фокусується на інформаційній безпеці як на автономній категорії суспільного буття та фундаментальному аспекті діяльності сучасної держави.

Для формування цілісного розуміння сутності та структури цього явища «адміністративно-правовий механізм забезпечення інформаційної безпеки держави» доцільно здійснити його філософсько-правове осмислення на основі синтезу наявних наукових підходів. Такий підхід дозволяє вийти за рамки вузькогалузевого аналізу й виробити узагальнене розуміння зазначеного явища.

Корисними у цьому контексті є висновки, сформульовані А. Й. Присяжнюком і С. І. Лекарем у межах досліджень адміністративно-правового механізму забезпечення економічної безпеки держави.

Ґрунтовний аналіз сутності відповідного інструментарію представлений у наукових розвідках А. Й. Присяжнюка. Автор пропонує розглядати цей механізм як інтегровану систему юридичних засобів, покликаних забезпечувати державне управління в межах економічного сектору. Ключовим вектором такої діяльності визначено нормативне впорядкування суспільних відносин, що виникають під час підтримання економічної стабільності держави, а функція безпосередньої реалізації зазначених завдань покладається на уповноважені державні органи [76, с. 810].

До структури цього механізму дослідник включає такі блоки:

нормативно-правовий (сукупність норм права, нормативно-правових актів, юридичних фактів);

інституційно-організаційний (система уповноважених органів управління у сфері забезпечення економічної безпеки);

процедурно-функціональний (принципи, інструменти, методи регулювання, процедури й алгоритми реалізації діяльності, зокрема управлінські техніки й технології);

забезпечувальний (кадрове, інформаційне, матеріально-технічне та інші види забезпечення);

інформаційно-аналітичний (аналіз стану розвитку та функціонування об’єкта забезпечення) [76, с. 811–812].

Схожих поглядів дотримується і С. І. Лекарь. У своїх працях дослідник розглядає адміністративно-правовий механізм забезпечення економічної безпеки держави як упорядковану сукупність правових інструментів. Саме через них здійснюється державний вплив на суспільні відносини під час реалізації державної економічної політики. Автор наголошує, що кінцевим орієнтиром такої активності є приведення існуючих відносин у відповідність до цілей забезпечення економічної безпеки держави, що покладаються на уповноважені державні органи [77, с. 17].

Безпосередньо до питань інформаційної безпеки звертається Б. О. Мельник. Він стверджує, що адміністративно-правовий механізм забезпечення інформаційної безпеки держави постає невід'ємною складовою національної безпеки держави. До його складу вчений включає взаємопов'язані правові норми, організаційні компоненти та комплекс заходів, що в сукупності забезпечують захист інформаційного простору держави. Дослідник також підкреслює, що в умовах глобалізації даний напрям безпеки трансформується у базову функцію державного управління [78, с. 37].

Л. Ю. Веселова, досліджуючи правову природу кібернетичного захисту, визначає механізм адміністративно-правового забезпечення кібербезпеки як цілісну систему нормативних інструментів та практичних методів. Саме завдяки їх застосуванню створюються умови для стабільної взаємодії та поступального розвитку суб'єктів, що формують національну мережу кібербезпеки. До структури вказаного явища дослідниця відносить норми адміністративного права, адміністративно-правові відносини, а також юридичні акти, що фіксують реалізацію прав та обов'язків учасників цієї сфери [79, с. 43].

Своєю чергою, Є. В. Кобко пропонує узагальнюючий погляд, згідно з яким під механізмом адміністративно-правового забезпечення національної безпеки України варто розуміти інтегрований комплекс правових, фінансових та організаційних засобів. Держава використовує цей інструментарій як важіль цілеспрямованого впливу та впорядкування суспільних відносин,

забезпечуючи необхідні умови для їх належного функціонування у безпековій царині [80, с. 43].

Структуру цього механізму автор розглядає як сукупність взаємопов'язаних елементів, серед яких [80, с. 44]:

нормативно-правові елементи (норми, принципи, юридичні факти, гарантії);

інституційні елементи (суб'єкти та об'єкти забезпечення національної безпеки);

організаційно-функціональні елементи (форми й методи адміністративно-правового впливу, а також матеріально-технічне, фінансове, кадрове та інформаційне забезпечення).

Своєю чергою, Ю. П. Лісовська розглядає адміністративно-правове регулювання інформаційної безпеки держави як цілісну систему заходів законодавчого та управлінського спрямування. Метою такої діяльності є встановлення стійкого правопорядку та законності в інформаційному просторі, а також гарантування інтересів кожного учасника інформаційних відносин. На переконання дослідниці, вказаний інструментарій включає:

нормотворчий вектор, представлений сукупністю законодавчих актів, що проголошують право на безперешкодне отримання інформації та детермінують правовий статус суб'єктів у цій галузі;

адміністративно-виконавчий вектор, що реалізується через компетенційну діяльність органів виконавчої влади, чиї зусилля спрямовані на підтримання захищеності суспільства від неправомірних посягань [67, с. 13].

Окрім того, авторка акцентує увагу на доцільності тлумачення адміністративно-правового забезпечення інформаційної безпеки як системи випереджальних заходів багатоаспектного (економічного, технологічного, політичного та юридичного) характеру. Такі дії мають на меті своєчасне виявлення, превенцію та нейтралізацію небезпек, що загрожують фундаментальним інтересам людини, громади та владних інституцій в інформаційній сфері [67, с. 11].

Л. Г. Чистоклетов та О. Л. Хитра інтерпретують категорію адміністративно-правового забезпечення крізь призму нормативного підґрунтя, через яке суб'єкти владних повноважень впливають на суспільні зв'язки в царині публічного управління. На переконання авторів, це поняття також охоплює активність зазначених суб'єктів із розробки, застосування та модернізації вказаного базису задля досягнення фундаментальних цілей адміністративного права [81, с. 178]. Водночас дослідники пропонують розглядати цей механізм як динамічну систему, суб'єктний склад якої представлений юридичними та фізичними особами. Саме завдяки їхнім цілеспрямованим діям відбувається становлення, функціонування та подальша оптимізація відповідного забезпечення. Структура такого механізму, за позицією вчених, інтегрує правові принципи, інструментальні методи, форми регулювання, а також сучасні технології державного управління [81, с. 178].

Підсумовуючи теоретичний аналіз сутності категорійного апарату, що описує адміністративно-правовий механізм забезпечення інформаційної безпеки держави, доцільно систематизувати наявні в доктрині погляди та згрупувати їх за ключовими методологічними підходами:

системний, що розглядає механізм як цілісну систему з елементами (суб'єкти, об'єкти, норми), зв'язками (координація, підпорядкування) та системними властивостями (синергія, адаптивність), з акцентом на взаємозалежність усіх компонентів;

структурно-функціональний, який передбачає виділення організаційних структур (органи влади, установи) та функцій (превенція, контроль, реагування) з акцентом на відповідність структур їх функціональному призначенню;

діяльнісний, що аналізує механізм через призму процесів (адміністративні процедури, алгоритми дій), ресурсів (фінансових, кадрових, технологічних) та результатів діяльності, зосереджуючись на операційній складовій діяльності суб'єктів;

комплексний, який інтегрує зазначені підходи на міждисциплінарній основі, поєднуючи організаційно-структурні елементи (хто?), функціонально-діяльнісні інструменти (як?), системні взаємозв'язки (чому?) та критерії ефективності (для чого?).

Саме з позицій комплексного підходу доцільно розглядати адміністративно-правовий механізм забезпечення інформаційної безпеки держави як підсистему державного управління, що через норми права, діяльність уповноважених інституцій та застосування адміністративних інструментів (дозвільних, реєстраційних, контрольних, примусових) забезпечує захист від внутрішніх і зовнішніх загроз та створює умови для сталого розвитку національного інформаційного простору. Такий механізм має інтегрований і цілісний характер та функціонує у взаємодії з внутрішніми й зовнішніми чинниками.

Водночас у межах цього дослідження адміністративно-правовий механізм розглядається у широкому значенні – як універсальний інструмент забезпечення інформаційної безпеки.

Виходячи з результатів проведеного аналізу та з урахуванням комплексного підходу, до структури адміністративно-правового механізму забезпечення інформаційної безпеки держави доцільно включити такі взаємопов'язані блоки:

нормативно-правовий – сукупність норм права та нормативно-правових актів, що формують правові умови забезпечення інформаційної безпеки;

інституційно-координаційний – система органів державної влади, спеціально уповноважених установ та інших суб'єктів публічного управління, які здійснюють реалізацію державної політики, координацію, моніторинг, аналіз і реагування на загрози;

процедурно-контрольний – принципи, методи, процедури й алгоритми реалізації діяльності у сфері інформаційної безпеки, включно з адміністративними інструментами дозволу, реєстрації, контролю та примусу;

інформаційно-аналітичний – процеси моніторингу, аналізу та оцінки стану інформаційної безпеки, виявлення загроз і підготовки управлінських рішень щодо їх нейтралізації;

комунікаційно-превентивний – система стратегічних комунікацій, освітніх програм, методичних рекомендацій та громадсько-експертних ініціатив, спрямованих на формування культури прозорості, доброчесності та інституційної стійкості.

Узагальнена структура адміністративно-правового механізму забезпечення інформаційної безпеки держави, що відображає його ключові блоки та їх взаємозв'язки у системі державного управління, подана на схемі (див. рис. 1.2.1), яка демонструє місце цього механізму в ієрархічній моделі державного управління та його інтеграційні зв'язки з іншими механізмами забезпечення національної безпеки.

Підсумовуючи результати дослідження адміністративно-правового механізму забезпечення інформаційної безпеки держави доцільно констатувати, що комплексний підхід до розкриття сутності досліджуваного феномену є найбільш доцільним, оскільки він:

забезпечує всебічне охоплення основних аспектів інформаційної безпеки шляхом одночасного застосування системного, структурно-функціонального та діяльнісного підходів;

враховує специфіку інформаційної безпеки як особливого об'єкта адміністративно-правового регулювання, що потребує використання спеціальних інструментів і процедур для захисту національного інформаційного простору;

слугує концептуальним підґрунтям для розробки дієвих моделей правового регулювання, що відповідають сучасним викликам, пов'язаним із кіберзагрозами, інформаційними операціями та зовнішнім впливом на публічне управління;

дозволяє забезпечити необхідний баланс між стабільністю нормативно-правового регулювання та гнучкістю оперативного реагування на загрози інформаційній безпеці держави.



Рис. 1.2.1. Місце адміністративно-правового механізму забезпечення інформаційної безпеки держави в ієрархічній структурі державного управління

Наукова цінність застосування комплексного підходу полягає у формуванні цілісної методологічної основи для подальшого теоретичного осмислення й практичного вдосконалення адміністративно-правового механізму забезпечення інформаційної безпеки держави.

Викладені положення формують необхідну теоретичну базу для проведення наступного етапу дослідження – вивчення адміністративно-правового інструментарію впровадження державної політики у сфері інформаційної безпеки, що здійснюватиметься у наступному підрозділі.

1.3. Зовнішній вплив на публічне управління як загроза інформаційній безпеці держави

Інформаційна безпека держави є складним багатовимірним явищем, що охоплює захист інформаційних ресурсів, процесів обігу інформації, інституційних механізмів вироблення та реалізації державної політики. У центрі цього процесу перебуває публічне управління як форма організації та реалізації владних управлінських рішень.

Зовнішній вплив на публічне управління становить особливу загрозу для інформаційної безпеки держави, оскільки саме через управлінські процедури циркулюють ключові інформаційні потоки, формуються та змінюються порядок денний, пріоритети розвитку й умови функціонування суспільства.

У межах цього дослідження зовнішній вплив розглядається не як абстрактний політичний або інформаційний феномен, а як адміністративно-правова загроза, що проявляється через порушення процедур, механізмів і умов функціонування системи публічного управління. Саме такий підхід дає змогу виявити юридично значущі канали впливу та обґрунтувати необхідність спеціальних правових механізмів протидії.

Виходячи з цього, спробуємо окреслити зміст поняття «публічне управління», визначити його структуру та оцінити ті елементи (складові), які є найбільш вразливими до зовнішнього впливу.

Категорія «публічне управління», що бере свій початок від латинського кореня «publicus» (суспільний, загальнодержавний), ґрунтується на фундаментальному понятті адміністрування. Останнє традиційно інтерпретується як процес спрямованого впливу суб'єктної ланки на відповідний об'єкт задля досягнення конкретної мети. У загальному сенсі управлінська система являє собою структуровану множину взаємопов'язаних компонентів, які мають різні функціональні завдання, діють відносно самостійно, але орієнтовані на спільну ціль. Зі свого боку, кожна така система включає дві взаємодіючі частини: керуючу (суб'єкт, який здійснює управління) та керовану (об'єкт, що піддається впливу). Цілком закономірним є той факт, що в сучасному науковому дискурсі більшість дефініцій публічного управління (незважаючи на розмаїття авторських підходів) акцентують увагу саме на інструментальному впливі керуючого суб'єкта на кероване середовище.

Аналізуючи природу публічного управління крізь призму адміністративного права, вказане явище доцільно типізувати за трьома засадничими векторами: функціональний, організаційно-структурний, а також комбінований (див. табл. 1.3.1).

Функціональний вимір передбачає діяльність відповідних структурних утворень щодо виконання функцій, спрямованих на реалізацію публічного інтересу.

Організаційна архітектура публічного управління в національних правових реаліях охоплює ієрархічно вибудувану систему суб'єктів владних повноважень. В Україні такими органами є Верховна Рада України (далі – ВРУ), Президент України, органи виконавчої влади, місцеві ради, суди, а також усі органи й установи, які реалізують місцеве самоврядування (виконавчі комітети місцевих рад, громадські об'єднання, органи самоорганізації населення) [82, с. 13–14].

Комбінована (гібридна) модель пропонує інтегрований погляд на управлінські процеси, де ключова роль відводиться налагодженню

комунікаційних зв'язків між державним сектором, бізнес-середовищем та ІГС задля синергії в досягненні стратегічних цілей розвитку.

Генезис терміну «публічне управління» (англ. *«public management»*) пов'язують із працями Десмонда Келінга (1972 р.), який виступав активним прихильником функціональної парадигми. У його трактуванні цей концепт розкривається як пошук найбільш раціональних шляхів оперування ресурсами задля ефективного втілення стратегічних цілей державної політики [83, с. 20]. В українському науковому середовищі першими до розробки конструкту «публічне управління» з позицій функціоналізму долучилися О. Ю. Оболенський та А. Ф. Мельник [84; 85].

Зокрема, О. Ю. Оболенський пропонує інтерпретувати це явище як систему цілеспрямованих і раціональних впливів на життєдіяльність соціуму. Такий вплив базується на чіткій програмі управління та аналізі інформації про стан об'єкта, що дає змогу не лише підтримувати стабільність системи, а й забезпечувати її прогресивний розвиток для виконання визначеного переліку завдань [84, с. 30]. При цьому професор окремо підкреслює, що ключовим суб'єктом у цій структурі є саме населення країни. Своєю чергою, А. Ф. Мельник акцентує на взаємодії державного та громадського сегментів управління. На думку автора, вони функціонують як взаємодоповнюючі елементи єдиної системи, що базуються на спільності публічних інтересів і потребують координації управлінських зусиль для досягнення максимальної результативності [85, с. 229].

В межах функціонального підходу вагоме значення мають розвідки В. В. Мамонової. Дослідниця пропонує відійти від розуміння публічного управління як суто лінійної діяльності, наголошуючи на його природі як свідомої інтеракції між керуючими та керованими елементами системи. Така взаємодія, на переконання авторки, втілюється через практичну реалізацію визначеного переліку управлінських функцій [86, с. 31].

Вагомий внесок у розвиток комбінованого підходу зробила Л. М. Новак-Каляєва. Вчена інтерпретує публічне управління як багатогранну активність,

яка консолідує потенціал владних структур, територіальних громад, а також представників бізнесу та ІГС. Така взаємодія, за позицією авторки, має відбуватися суворо у правових координатах із метою розробки та впровадження стратегічно важливих рішень для держави та її територіальних одиниць [87, с. 144]. Також, авторка впевнена, що ефективність такої моделі прямо залежить від рівня консолідації соціуму навколо демократичних цінностей, принципів справедливості, безпеки та верховенства права.

Схожий вектор простежується у працях О. В. Михайловської, Н. В. Філіпової та інших представників цього напряму. Вони акцентують на тому, що публічне управління – це передусім форма активної участі громадян у державотворчих процесах. Така комунікація між владою та громадськістю дозволяє суттєво підвищити результативність управлінського впливу в контексті суспільного прогресу [88, с. 247].

Зі свого боку, Н. І. Обушна, як прихильниця організаційно-структурної парадигми, розглядає публічне управління як складний науковий об’єкт, що базується на тісному переплетенні політичних, правових та владних аспектів у межах соціальної системи [89, с. 57]. Схожі позиції займають К. Поллітт та Г. Букарт, які пропонують диференціювати це поняття через три виміри: практичну діяльність посадових осіб, систему існуючих процедур та структур, а також їх наукове осмислення [90, с. 8–9]. Доповнюючи цю лінію, Р. С. Мельник визначає публічне управління як специфічну форму суспільно корисної діяльності, що реалізується визначеним колом суб’єктів, насамперед органами державної влади [91, с. 96].

Найбільш ґрунтовну спробу декомпозиції публічного управління як цілісної системи здійснила О. В. Марухленко. Дослідниця трактує його як розгалужену мережу соціальних взаємозв’язків та відповідної активності, що охоплює ієрархічні рівні від державних інституцій до окремих громадян. У її розумінні публічне управління постає як динамічна система ролей та рольових відносин, спрямована на ефективне використання людських і природних ресурсів у сферах, де задіяна держава [92, с. 10].

Таблиця 1.3.1

Типологія підходів до визначення публічного управління

№ з/п	Підходи	Основні ідеї	Ключові представники
1.	Функціональний	Орієнтація на раціональне використання ресурсів для втілення державних завдань	Д. Келінг [83], О. Ю. Оболенський [84], В. В. Мамонова [86] та ін.
2.	Організаційно-структурний	Розгляд управління як системи інституцій, формальних процедур та ієрархічних зв'язків	Н. І. Обушна [89], К. Поллітт [90], О. В. Марухленко [92] та ін.
3.	Комбінований	Базується на мережевій взаємодії влади, бізнес-структур та ІГС	Л. М. Новак-Каляєва [88], О. В. Михайловська [89] та ін.

Джерело: складено автором на основі аналізу [82–92].

Отже, аналіз розглянутих визначень свідчить про еволюцію концепту «публічного управління» від класичних інтерпретацій (Д. Келінг, В. В. Мамонова, А. Ф. Мельник, О. Ю. Оболенський), що акцентували на діяльності, до організаційно-структурних підходів (О. В. Марухленко, К. Поллітт, Г. Букарт, Р. С. Мельник, Н. І. Обушна) та сучасних комбінованих (гібридних) моделей (О. В. Михайловська, Н. В. Філіпова, Л. С. Ладонько, Н. В. Ткаченко, Л. М. Новак-Каляєва), де публічне управління виходить за межі державної бюрократії до мережевої системи з суспільною участю.

У науковій літературі є різні підходи не лише до розуміння сутності публічного управління, але й до розкриття системи публічного управління.

У межах наукових підходів до ідентифікації системи публічного управління В. Яцук акцентує увагу на її інституційному складнику. Автор розглядає зазначену систему як сукупність владних інституцій та структур місцевого самоврядування, що здійснюють регулюючий вплив на соціальні процеси шляхом реалізації управлінських завдань у правовому полі [87, с. 163].

Схожої позиції дотримується Н. Р. Нижник, трактуючи систему публічного управління як впорядковану модель, що об'єднує профільних суб'єктів та відповідні процедури впливу. За такої моделі ключова координаційна роль відводиться інституційному центру, який забезпечує розподіл функцій та стабільність життєдіяльності соціуму на певній території [93, с. 167].

Аналіз наведених вище поглядів на поняття «публічне управління» дає змогу виокремити три його основні компоненти: суб'єкт управління, об'єкт управління та зв'язки, що виникають у процесі управлінської діяльності (процесу) [82–93]. У вузькому значенні суб'єктом публічного управління виступають органи виконавчої влади, об'єктом – суспільство, суспільна діяльність. Сама ж управлінська діяльність виступає певного роду суспільними відносинами, через які реалізуються численні прямі та зворотні зв'язки між суб'єктами і об'єктами управління.

На думку Ю. Тихомирова, суб'єктний склад управління суспільством є широким і включає як народ загалом, так і його окремі структуровані об'єднання чи колективи, що діють у легітимних політико-правових формах через мережу державних та громадських інституцій [82, с. 15]. В цілому, публічне управління містить велику кількість суб'єктів – від органів державної влади до окремих громадян. На переконання фахівців у галузі адміністративного права, ключовими суб'єктами тут виступають структури виконавчої влади та органи самоврядування, а також інституції, наділені відповідними делегованими повноваженнями [94; 95]. Щодо об'єктів управління, то ними виступають конкретні складники соціальної системи, на які спрямовується координуючий вплив задля їх стабілізації та розвитку. У науковій думці об'єкт управління пропонується аналізувати крізь призму двох ракурсів: елементно-структурного (як спільність індивідів чи організаційних утворень) та функціонального (як безпосередню активність і поведінкові акти груп) [96, с. 88]. У площині публічного управління об'єктом постають саме соціальні зв'язки, що виникають у процесі реалізації загальнодержавних стратегій. Відповідно, предметна сфера охоплює сукупність юридичних та організаційних засобів, які формують практичний базис виконання управлінських завдань.

Життєдіяльність такої системи неможлива без динамічної комунікації між керуючою ланкою та об'єктом впливу. Така взаємодія реалізується через розгалужену мережу прямих та зворотних зв'язків. Якщо прямі канали забезпечують трансляцію владних рішень, то зворотні є необхідними для

моніторингу результативності та оперативного корегування управлінських кроків. Як слушно зауважує О. Ф. Константінов, управлінський процес набуває завершеності лише за умови функціонування дієвого зворотного зв'язку, який дозволяє суб'єкту отримувати актуальну інформацію про результативність прийнятих рішень [97, с. 5].

Своєю чергою Н. І. Обушна акцентує увагу на тому, що ключовою ланкою в системі управління виступають безпосередні органи публічної влади. До них авторка відносить інституції та посадових осіб (як обраних шляхом прямого волевиявлення, так і призначених відповідними структурами), а також їхні виконавчі підрозділи [89, с. 58]. Дослідниця обґрунтовує особливу роль населення країни та груп інтересів у цьому процесі. В умовах сучасного суспільного розвитку саме суб'єкти громадянського суспільства через механізми прямого або представницького демократичного контролю визначають стратегічні цілі управління, оцінюють ефективність прийнятих рішень та формують підходи до розв'язання актуальних соціальних проблем [89, с. 58–59].

Таким чином, у системі публічного управління межа між суб'єктом та об'єктом є динамічною: структура, що здійснює управління стосовно одного об'єкта, може сама перебувати під керівним впливом іншого суб'єкта.

Виходячи з суб'єктного складу, у структурі публічного управління доцільно виокремити такі напрями:

державне управління, де ключова роль належить державним органам, що реалізують загальнонаціональні інтереси;

місцеве самоврядування, яке здійснюється територіальними громадами через власні виборні органи, що діють в інтересах місцевих мешканців;

громадське управління, у межах якого недержавні інституції реалізують статутні завдання та власні повноваження від свого імені [82, с. 16].

Конституційні засади місцевого самоврядування в Україні закріплені у ст. 140 Основного Закону, де воно визначається як право громади самостійно вирішувати питання місцевого значення в межах правового поля [1].

Деталізація цього поняття, а також базові принципи та архітектура системи самоврядування містяться у відповідному профільному законі [98].

Що стосується державного управління, то його сутність розкривається у нормативних актах як організуючий вплив держави на суспільні процеси через механізми виконавчої влади. При цьому наголошується, що таке управління охоплює не лише діяльність владних структур, а й функціонування державних установ та підприємств [99]. Паралельно з цим розвивається громадське управління, яке представляє собою активність ІГС, спрямовану на гарантування прав і свобод людини у межах, визначених законодавством [82, с. 18].

Цікавою є думка В. В. Мамонової, яка до секторального складу публічного управління, окрім державного управління, місцевого самоврядування та громадського управління, відносить ще й бізнес-стейкхолдерів. На думку дослідниці, «сучасні суб'єкти господарювання (які переважно належать до бізнес-стейкхолдерів) за власною ініціативою чи за ініціативою органів влади активно залучаються до прийняття рішень місцевого рівня, зокрема у таких сферах: розробка стратегій розвитку громади чи регіону та їх впровадження; формування проєктів державно-приватного партнерства; реалізація ініціатив соціальної відповідальності бізнесу тощо» [86, с. 32].

Звертаючись до концептуальних підходів В. В. Мамонової, варто деталізувати запропоновану нею ієрархію суб'єктного складу. Авторка пропонує класифікувати управлінські ланки в Україні за рівнями їхнього функціонування (диференціюючи при цьому судову гілку, яка має відокремлену природу), а саме:

вищий рівень, куди віднесено інституцію глави держави, вищий законодавчий орган та Кабінет Міністрів України (далі – КМУ);

центральний рівень, представлений галузевими міністерствами та іншими профільними установами виконавчої влади;

регіональний та муніципальний рівні, що охоплюють діяльність місцевих адміністрацій, територіальних підрозділів центральних органів виконавчої влади (далі – ЦОВВ), а також усю систему самоврядування територіальних громад разом із їхніми виборними особами [86, с. 34-35].

Узагальнюючи наведені дефініції, можна виокремити низку константних ознак публічного управління. Насамперед це його соціальна спрямованість – діяльність завжди орієнтована на задоволення суспільних потреб. Крім того, суб'єктний склад такої системи є плюралістичним, оскільки об'єднує владні органи з недержавними структурами. Центральним елементом тут виступає інформаційно-комунікаційний обмін, що супроводжує ухвалення рішень, а сама архітектура управління гармонійно поєднує ієрархічну вертикаль із мережевою горизонталлю.

Водночас концептуальні розбіжності між науковими школами зазвичай стосуються ієрархії пріоритетів. Зокрема, йдеться про різну оцінку ролі державного апарату порівняно з громадськими інституціями, а також про акценти на специфіці комунікаційних потоків. Залежно від обраного методологічного орієнтира – функціонального, організаційного чи змішаного – змінюється і бачення кінцевої моделі управління.

З урахуванням викладеного, *публічне управління* доцільно розуміти як діяльність суб'єктів державного управління, місцевого самоврядування та інших залучених інституцій щодо формування та реалізації публічної політики в інтересах суспільства та держави.

Система публічного управління – цілісне багаторівневе утворення, яке об'єднує суб'єкти державного управління та місцевого самоврядування, залучені інституції, управлінські процедури, механізми впливу та інформаційні потоки, взаємопов'язані системоутворюючими зв'язками. У структурному аспекті система має дуалістичну природу: вертикальний вимір представлений ієрархічною діяльністю органів державної влади та місцевого самоврядування, горизонтальний – кооперацією ІГС та бізнес-стейкхолдерів. Взаємодія цих елементів забезпечує ефективну реалізацію публічної політики та визначає стійкість системи до зовнішніх і внутрішніх впливів (див. рис. 1.3.1).



Рис. 1.3.1. Структура публічного управління

Як продемонстровано на рис. 1.3.1, точки взаємодії між вертикальним та горизонтальним вимірами утворюють єдиний управлінський цикл. У межах цієї моделі інформаційні потоки громадського сектору та бізнес-середовища безпосередньо впливають на архітектоніку владних рішень, що робить зони перетину цих вимірів найбільш вразливими до латентного зовнішнього втручання та інституційно-процедурної деформації.

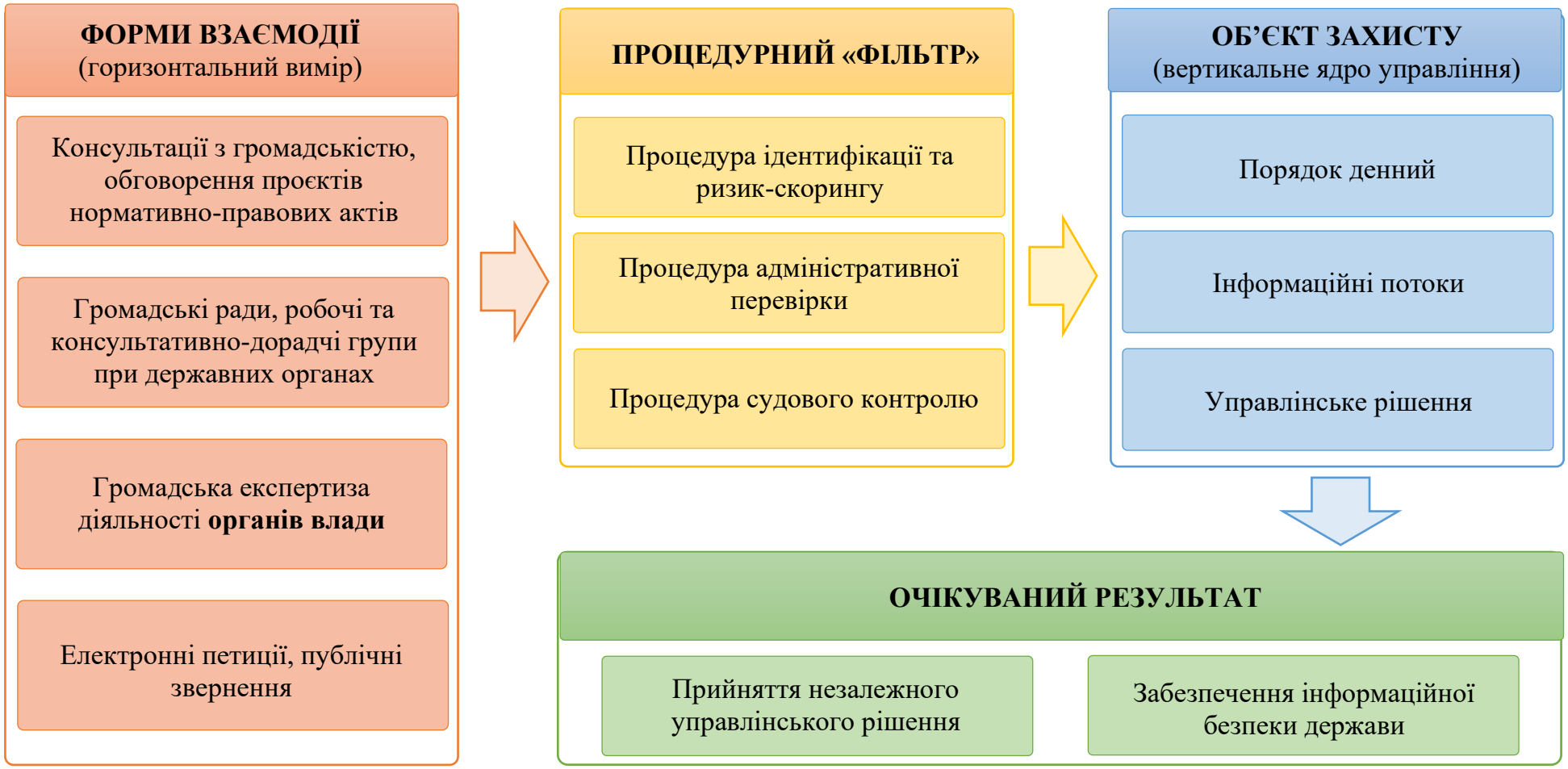
Вертикальний вимір представлений державним управлінням і місцевим самоврядуванням (у частині реалізації делегованих повноважень) та характеризується ієрархічністю, владно-розпорядчим впливом і застосуванням адміністративних процедур. Горизонтальний вимір публічного управління формується через участь ІГС та бізнес-стейкхолдерів, діяльність яких ґрунтується на взаємодії, діалозі та узгодженні інтересів.

Визначене нами ієрархічне місце адміністративно-правового механізму забезпечення інформаційної безпеки (див. підрозділ 1.2) дозволяє деталізувати його функціональну роль у протидії зовнішньому впливу. П’ятикомпонентна структура цього механізму, що включає інституційно-координаційний, нормативно-правовий, процедурно-контрольний, інформаційно-аналітичний та комунікаційно-превентивний блоки, у контексті взаємодії вертикального та горизонтального вимірів публічного управління трансформується у систему процедурних фільтрів (ідентифікація та ризик-скоринг, адміністративна перевірка, судовий контроль).

Функціонування цієї моделі спрямоване на убезпечення точок дотику між суспільною участю та державним владним рішенням, що візуалізовано у загальній структурі механізму (див. рис. 1.3.2).

У функціональному аспекті таке поєднання зумовлює те, що публічне управління постає як складна багаторівнева система, у межах якої вертикаль забезпечує керованість, стабільність і виконання управлінських рішень, тоді як горизонталь – адаптивність, відкритість і соціальну легітимацію управлінського впливу. Поєднання цих вимірів зумовлює трансформацію традиційного державного управління у ширший публічно-управлінський формат, що відповідає сучасним адміністративно-правовим підходам і потребам розвитку демократичної держави.

Розвиненість горизонтальної складової зумовлює перехід від виключно антропоцентричної моделі управління до публічної, яка формується колективними зусиллями та реалізується шляхом урахування легітимних інтересів суспільства через інституціоналізований діалог між владою та громадянами. Ця сфера має визначальний вплив на формування управлінського порядку денного та ухвалення відповідних рішень, оскільки охоплює широкий спектр державних, недержавних і громадських інституцій, експертних середовищ, громадських організацій та представників бізнесу, які конкурують за доступ до ресурсів і вплив на процеси вироблення державної політики.



1.3.2. Функціональна модель адміністративно-правового механізму як системи процедурних фільтрів і точок взаємодії вертикального та горизонтального вимірів публічного управління

Узагальнюючи викладене, слід зазначити, що кожна зі складових публічного управління має власні механізми функціонування, рівень інституційної стійкості та ступінь захищеності від зовнішнього втручання. Водночас вони не є однаково вразливими до впливу ззовні.

Доцільно зазначити, що саме громадське управління як складова горизонтального виміру публічного управління є найбільш піддатливим до зовнішнього впливу. Водночас вразливість громадянського суспільства до зовнішнього втручання є не ознакою його інституційної неспроможності, а закономірним наслідком його відкритості, плюралістичного характеру, відсутності жорсткої ієрархії, а також широкого використання формальних і неформальних інформаційно-комунікаційних каналів, у тому числі інституціоналізованих форм взаємодії з органами державної влади та місцевого самоврядування. Участь ІГС у процесах формування управлінського порядку денного, зокрема через консультації з громадськістю щодо проєктів нормативно-правових актів, діяльність громадських рад, публічні обговорення, громадську експертизу, електронні петиції, а також залучення представників громадських організацій до консультативно-дорадчих і робочих органів при суб’єктах владних повноважень, з одного боку, забезпечує демократичність і суспільну легітимацію управлінських рішень, а з іншого – створює сприятливі умови для прихованого зовнішнього впливу [100–102].

Саме через громадське управління можуть здійснюватися інформаційні, смислові та ціннісні впливи, спрямовані на трансформацію суспільних очікувань, зміну пріоритетів державної політики та опосередкований тиск на суб’єктів публічного управління вертикального виміру. У цьому контексті громадське управління виступає своєрідним «транзитним середовищем» між зовнішніми акторами та державно-управлінською вертикаллю, що зумовлює його особливе значення для аналізу загроз інформаційній безпеці держави.

Водночас забезпечення стійкості цього виміру потребує чіткого дотримання балансу, оскільки надмірне адміністративне втручання може призвести до порушення інформаційних прав та приватності громадян.

Виходячи з цього, подальший аналіз зосереджується на розкритті форм зовнішнього впливу через громадське управління. У цьому контексті методологічне значення має типологія впливів І. В. Матвєєнко, доповнена авторською класифікацією в аспекті загроз інформаційній безпеці [103, с. 22–23].

Зовнішній вплив на публічне управління реалізується через сукупність взаємопов'язаних каналів, які відрізняються за способом впливу, інституційним середовищем та ступенем формалізованості. До таких каналів належать інституційні механізми (тиск на нормотворчі й кадрові процеси), інформаційно-комунікаційні та соціально-мережеві впливи (дезінформаційні кампанії, маніпулятивні експертні оцінки, використання медіа та мереж громадської підтримки), економічні й фінансові інструменти (зовнішнє фінансування, матеріальне стимулювання рішень, використання сегменту електронної комерції для прихованих транзакцій), технологічні та цифрові впливи (втручання в інформаційні системи, використання цифрових платформ, штучного інтелекту), а також правові та регуляторні механізми (імпорт нормативних моделей, використання міжнародних інституцій для тиску на внутрішні процеси).

Таким чином, зовнішній вплив на публічне управління набуває адміністративно-правового виміру, оскільки його реалізація безпосередньо пов'язана з деформацією управлінських процедур, інституційних взаємозв'язків та регуляторних рішень, що виходить за межі суто інформаційного чи політичного аналізу.

У цьому контексті доцільно ввести поняття інституційно-процедурної деформації управлінських процесів, яке дозволяє відмежувати динаміку зовнішнього впливу від його адміністративно-правових наслідків.

Інституційно-процедурна деформація управлінських процесів – це системне викривлення нормативно визначеного порядку здійснення публічного управління, зумовлене цілеспрямованим або опосередкованим впливом зовнішніх чи афілійованих суб'єктів на умови формування та ухвалення управлінських рішень, яке проявляється у порушенні автономності та послідовності управлінських процедур, зміні управлінського порядку денного, зсуві пріоритетів публічної політики або підміні публічного інтересу інтересами суб'єктів впливу й у

сукупності створює загрозу суверенітету публічного управління як фундаментальній умові забезпечення інформаційної безпеки держави.

У межах адміністративного права об’єктом протиправного впливу в такому разі виступають не органи публічної влади як інститути, а процедурно значущі процеси формування, інтерпретації та селекції інформації, від яких залежить реалізація адміністративної дискреції та забезпечення об’єктивності управлінських рішень.

На відміну від разових порушень законності чи зловживань владою, інституційно-процедурна деформація управлінських процесів має системний характер і не зводиться до неправомірних дій окремих посадових осіб. Вона виникає внаслідок використання легальних або квазілегальних механізмів участі, комунікації та експертного впливу, які за відсутності належних адміністративно-правових фільтрів дозволяють зовнішнім акторам опосередковано втручатися у внутрішню логіку публічного управління, змінюючи умови формування та реалізації управлінських рішень.

Таким чином, зовнішній вплив на публічне управління доцільно розглядати як фактор, що ініціює інституційно-процедурну деформацію управлінських процесів, але не як тотожне їй явище. Якщо зовнішній вплив характеризує динаміку втручання у інформаційне та смислове середовище ухвалення рішень, то інституційно-процедурна деформація відображає адміністративно-правовий результат такого втручання, який проявляється у порушенні автономності, послідовності та нормативної логіки публічного управління.

Саме цей результат становить безпосередній об’єкт адміністративно-правового аналізу і реагування у сфері забезпечення інформаційної безпеки держави.

У межах цього дослідження використовується категорія суверенітету публічного управління, яка логічно випливає з аналізу адміністративної системи як автономного утворення. Під суверенітетом публічного управління пропонується розуміти здатність системи публічного управління самостійно, без зовнішнього детермінування, формувати управлінський порядок денний,

ухвалювати та реалізовувати рішення відповідно до публічних інтересів у межах установлених правових процедур. Порушення цієї здатності внаслідок інституційно-процедурної деформації означає втрату процесуальної незалежності управління, що безпосередньо підриває стан інформаційної безпеки держави

Узагальнення наведених характеристик, каналів реалізації та адміністративно-правових наслідків зовнішнього втручання на публічне управління свідчить, що наявні в науковій літературі підходи [103–109] або зосереджуються на окремих формах впливу, або обмежуються його політичним чи інформаційним виміром, не розкриваючи цілісно його функціонування як чинника деформації управлінських процесів. У зв'язку з цим постає потреба в авторському визначенні зовнішнього впливу в системі публічного управління, яке узагальнює попередні теоретичні напрацювання та водночас адаптує їх до адміністративно-правового контексту цього дослідження. У такому розумінні зовнішній вплив на публічне управління – цілеспрямована діяльність іноземного чи афілійованого з ним суб'єкта, що полягає у прихованому або позапроцесуальному втручанні у процеси формування, обігу та інтерпретації інформації, прийняття управлінських рішень чи визначення порядку денного публічної політики, з метою зміни її змісту або результатів на користь іноземних суб'єктів.

Ключовими ознаками зовнішнього впливу є його опосередкований характер, використання інформаційно-комунікаційних, експертних, соціально-мережевих або економічних каналів, а також орієнтація не на безпосереднє управління, а на формування умов, у межах яких суб'єкти публічного управління ухвалюють рішення. Саме тому зовнішній вплив найчастіше реалізується через горизонтальний рівень публічного управління – громадське управління, експертні середовища, медіа та мережі взаємодії, які виконують функцію «транзитного середовища між зовнішніми акторами та державно-управлінською вертикаллю.

Тобто суб'єктами зовнішнього впливу виступають: іноземні суб'єкти, афілійовані суб'єкти.

Іноземний суб’єкт – іноземна держава, її органи, міжнародна або іноземна організація, група осіб чи інша структура, яка не входить до системи публічного управління України та реалізує власні інтереси у взаємодії з її інституціями.

Ключові ознаки іноземних суб’єктів: зовнішнє походження щодо системи публічного управління країни перебування; наявність власного інтересу, відмінного від публічного інтересу країни перебування; потенційна здатність впливати на внутрішні процеси без формального мандата.

Афілійований суб’єкт – фізична або юридична особа, що формально діє в межах правового поля України, але перебуває у стійкому фінансовому, організаційному, професійному, інформаційному чи іншому зв’язку з іноземним суб’єктом, що зумовлює фактичну залежність такої особи від нього або її підзвітність такому суб’єкту.

Безпосереднім об’єктом зовнішнього впливу є не органи влади як такі, а: процеси формування, обігу та інтерпретації інформації; управлінський порядок денний; рамки сприйняття проблем і варіанти допустимих рішень; умови, у яких суб’єкти публічного управління ухвалюють рішення.

Таким чином, вплив спрямований на інформаційне та смислове середовище управління, а не на владні повноваження напряму.

Результатом зовнішнього впливу є: зміна змісту, спрямованості або пріоритетів публічної політики; викривлення управлінських рішень; делегітимація або блокування реформ; ухвалення рішень, що суперечать національним інтересам держави.

Важливо пам’ятати, що ефект може бути відстроченим, кумулятивним і не завжди безпосередньо пов’язуваним із діями конкретного суб’єкта.

Під цільовою державою необхідно розуміти державу, система публічного управління якої виступає об’єктом зовнішнього впливу з боку іноземних або афілійованих із ними суб’єктів.

Отже, зовнішній вплив на публічне управління слід розглядати як комплексну загрозу інформаційній безпеці держави, що реалізується переважно опосередковано через горизонтальний вимір публічного управління. Його особливістю є відсутність прямого втручання у владні повноваження та

спрямованість на формування інформаційного, смислового й процедурного середовища ухвалення управлінських рішень. Це зумовлює складність виявлення, ідентифікації та правової оцінки такого впливу в межах чинних адміністративно-правових інструментів. При цьому особливої уваги потребує адміністративно-правове реагування у сфері забезпечення інформаційної безпеки держави в умовах інтенсивної цифрової трансформації, що вимагає розробки нових підходів до захисту суверенітету публічного управління.

Вказані обставини обґрунтовують необхідність подальшого аналізу нормативно-правового забезпечення протидії зовнішньому впливу (розділ 2) та розробки спеціалізованих адміністративно-правових процедур ідентифікації афілійованості та реагування на встановлений зовнішній вплив (розділ 3).

Висновки до розділу 1

У першому розділі дисертаційного дослідження на основі міждисциплінарного аналізу досліджено фундаментальні теоретико-правові передумови формування ефективного адміністративно-правового механізму забезпечення інформаційної безпеки держави.

1. Проаналізовано та систематизовано наукові підходи до розуміння сутності інформаційної безпеки держави як багатовимірного феномену, що поєднує технологічні, політичні, правові, ціннісні та культурні аспекти. Встановлено, що така концептуальна поліфонія зумовлює термінологічний плюралізм, за якого кожен науковий напрям формує власний дискурс, що істотно ускладнює вироблення консолідованого визначення інформаційної безпеки держави.

Виділено дві групи існуючих концептуальних підходів до трактування інформаційної безпеки: за спільними ознаками: системний (безпека як «система»), статичний (безпека як «стан»), процесний (діяльнісний), комплексний (який поєднує статичний і діяльнісний); за трансдисциплінарною природою: технічний (реалізується через систему спеціалізованих механізмів, акцентуючи увагу на інженерно-технологічних рішеннях для запобігання, виявлення та нейтралізації загроз), гуманітарний (розглядає інформаційну безпеку через призму захисту суспільних цінностей та конституційних прав, акцентуючи на необхідності формування методологічних основ та захисту колективної свідомості), нормативний (зосереджений на правових аспектах, зокрема на законодавчому закріпленні норм і механізмів захисту інформаційного простору), психологічний (висуває на перший план захист психіки людини від деструктивних інформаційних впливів), комплексний.

Наголошено, що найбільш прийнятним з огляду на сучасну практику забезпечення інформаційної безпеки держави є саме комплексний підхід, який, з одного боку, інтегрує статичний і діяльнісний виміри, а з іншого – забезпечує цілісне поєднання технічних, правових і соціально-психологічних аспектів.

Обґрунтовано авторське визначення інформаційної безпеки держави як нормативно закріплений стан захищеності національного інформаційного

простору, за якого забезпечується: стійкість інформаційної інфраструктури та цілісність інформаційних ресурсів; стабільність інформаційних процесів і захист прав суб'єктів інформаційних відносин; збереження національної ідентичності; реалізація національних інтересів і досягнення стратегічних цілей в інформаційній сфері; створення умов для сталого розвитку інформаційного суспільства. В основу такого підходу покладено принцип активного захисту, що передбачає не лише реагування на загрози, а й проактивне формування безпечного інформаційного середовища.

2. Розкрито сутність категорії «адміністративно-правовий механізм забезпечення інформаційної безпеки держави» крізь призму різних підходів: системного (розглядає механізм як цілісну систему з елементами (суб'єкти, об'єкти, норми), зв'язками (координація, підпорядкування) та системними якостями (синергія, адаптивність) з акцентом на взаємозалежність усіх компонентів системи); структурно-функціонального (виділення структур (організаційні одиниці: органи влади, установи) та функцій (превенція, контроль, реагування) з акцентом на відповідність структур функціям); діяльнісного (аналіз механізму через процеси (адміністративні процедури, алгоритми дій), ресурси (фінанси, кадри, технології) та результати (ефективність нейтралізації загроз) з акцентом на операційній діяльності суб'єктів); комплексного (синтез усіх підходів (міждисциплінарність) з акцентом на: організаційно-структурні елементи (хто?); функціонально-діяльнісні інструменти (як?); системні взаємозв'язки (чому?); комплексні критерії ефективності (для чого?)). Запропоновано розглядати адміністративно-правовий механізм забезпечення інформаційної безпеки держави в рамках комплексного підходу як підсистему державного управління, що через норми права, діяльність уповноважених інституцій та застосування адміністративних інструментів (дозвільних, реєстраційних, контрольних, примусових) забезпечує захист від внутрішніх і зовнішніх загроз та створює умови для сталого розвитку національного інформаційного простору.

Наголошено, що механізм має інтегрований і цілісний характер та функціонує у взаємодії із внутрішніми й зовнішніми факторами. У межах такого

підходу розкрито структуру адміністративно-правового механізму забезпечення інформаційної безпеки держави, яка включає такі блоки (компоненти): нормативно-правовий – сукупність норм права та нормативно-правових актів, що формують правові умови забезпечення інформаційної безпеки; інституційно-координаційний – система органів державної влади, спеціально уповноважених установ та інших суб'єктів публічного управління, які здійснюють реалізацію державної політики, координацію, моніторинг, аналіз і реагування на загрози; процедурно-контрольний – принципи, методи, процедури й алгоритми реалізації діяльності у сфері інформаційної безпеки, включно з адміністративними інструментами дозволу, реєстрації, контролю та примусу; інформаційно-аналітичний – процеси моніторингу, аналізу та оцінки стану інформаційної безпеки, виявлення загроз і підготовки управлінських рішень щодо їх нейтралізації; комунікаційно-превентивний – система стратегічних комунікацій, освітніх програм, методичних рекомендацій та громадсько-експертних ініціатив, спрямованих на формування культури прозорості, доброчесності та інституційної стійкості.

3. Розкрито зміст і особливості зовнішнього впливу на систему публічного управління як специфічної загрози суверенітету публічного управління та інформаційній безпеці держави, що має опосередкований, прихований і переважно нефронтальний характер. На основі узагальнення наукових підходів публічне управління обґрунтовано як складну багаторівневу систему, що поєднує вертикальний (ієрархічний, владно-розпорядчий) і горизонтальний (мережевий, комунікативний) виміри. Їх взаємодія забезпечує керованість, стабільність і соціальну легітимацію управлінських рішень. Доведено, що саме горизонтальний вимір публічного управління – громадське управління (ІГС, експертні та медійні середовища) – є найбільш вразливим до зовнішнього впливу внаслідок своєї відкритості, плюралістичності, відсутності жорсткої ієрархії та активного використання формальних і неформальних інформаційно-комунікаційних каналів.

Установлено, що зовнішній вплив у системі публічного управління спрямовується не безпосередньо на здійснення владних повноважень, а на

формування інформаційного, смислового та процедурного середовища ухвалення управлінських рішень, зокрема через вплив на управлінський порядок денний, рамки інтерпретації проблем і спектр допустимих управлінських альтернатив. Під зовнішнім впливом на публічне управління запропоновано розуміти цілеспрямовану діяльність іноземного чи афілійованого з ним суб'єкта, що полягає у прихованому або позапроцесуальному втручанні у процеси формування, обігу та інтерпретації інформації, прийняття управлінських рішень чи визначення порядку денного публічної політики, з метою зміни її змісту або результатів на користь іноземних суб'єктів.

Доведено, що наслідком такого впливу є інституційно-процедурна деформація управлінських процесів – системне викривлення нормативно визначеного порядку здійснення публічного управління, зумовлене цілеспрямованим або опосередкованим впливом зовнішніх чи афілійованих суб'єктів на умови формування та ухвалення управлінських рішень, яке проявляється у порушенні автономності та послідовності управлінських процедур, зміні управлінського порядку денного, зсуві пріоритетів публічної політики або підміні публічного інтересу інтересами суб'єктів впливу й у сукупності створює загрозу суверенітету публічного управління. Останній трактується як здатності системи публічного управління самостійно, без зовнішнього детермінування, формувати управлінський порядок денний та реалізовувати рішення в межах правових процедур.

Деталізовано функціональну роль адміністративно-правового механізму забезпечення інформаційної безпеки держави в частині протидії зовнішньому впливу як системи процедурних фільтрів (ідентифікації та ризик-скорингу, адміністративної перевірки, судового контролю). Підкреслено, що така модель дає змогу убезпечити «точки дотику» між вертикальним і горизонтальним вимірами публічного управління.

Зроблено висновок про необхідність подальшої конкретизації адміністративно-правового механізму забезпечення інформаційної безпеки держави в аспекті протидії зовнішньому впливу на публічне управління, зокрема шляхом розробки спеціалізованих процедур ідентифікації афілійованості.

РОЗДІЛ 2
АДМІНІСТРАТИВНО-ПРАВОВИЙ МЕХАНІЗМ ЗАБЕЗПЕЧЕННЯ ІНФОРМАЦІЙНОЇ БЕЗПЕКИ УКРАЇНИ: ПРАКТИЧНА СКЛАДОВА

2.1. Стан нормативно-правового забезпечення інформаційної безпеки України в аспекті протидії зовнішньому впливу на публічне управління

2.1.1. Загальна характеристика чинної нормативно-правової бази у сфері інформаційної безпеки та публічного управління

Предметом правового аналізу в межах цього підрозділу є нормативно-правова база України, що регулює інформаційні відносини, доступ до інформації та діяльність органів публічної влади. З урахуванням комплексного підходу, сформульованого у підрозділі 1.2, відповідні акти аналізуються крізь призму їхньої здатності забезпечувати стійкість управлінських процедур до зовнішнього втручання. Особлива увага приділяється правовому регулюванню процедур взаємодії органів влади з громадськістю, оскільки саме горизонтальний вимір публічного управління становить найбільш вразливе середовище для опосередкованого впливу на формування управлінського порядку денного.

Фундамент адміністративно-правового регулювання у цій сфері закладає Конституція України, яка поєднує гарантії інформаційних прав із можливістю їх обмеження в інтересах національної безпеки. Відповідно до статті 17 Основного Закону, забезпечення інформаційної безпеки визначається однією з найважливіших функцій держави, що надає їй системоутворювального значення у сфері публічного управління [1]. Водночас конституційний рівень регулювання має декларативний характер: за наявності стратегічних орієнтирів він не містить операціоналізованих механізмів протидії впливу, що реалізується через управлінські процедури.

Аналіз положень статей 15, 32, 34, 40, 50 та 57 Конституції України виявляє регуляторну асиметрію, за якої інформаційні відносини врегульовуються переважно крізь призму прав і свобод людини [110, с. 75–76]. За відсутності адміністративно-правових фільтрів це створює умови, за яких відповідні права можуть використовуватися як інструменти зовнішніх деструктивних впливів. Хоча стаття 34 Конституції прямо передбачає можливість обмеження права на інформацію в інтересах національної безпеки, у площині адміністративного права ця норма залишається неопераціоналізованою через відсутність чітких критеріїв розмежування добросовісної реалізації інформаційних прав і цілеспрямованих операцій зовнішнього впливу [1].

При цьому, згідно з усталеною практикою ЄСПЛ, будь-яке обмеження інформаційних прав має відповідати критерію «якості закону» (зокрема, справа «Sunday Times проти Сполученого Королівства» [111]). Це передбачає, що адміністративно-правові норми повинні бути чіткими та передбачуваними, аби суб’єкт міг чітко розрізняти легітимну діяльність від протиправного втручання. Відсутність таких операційних критеріїв у національному законодавстві створює передумови для суб’єктивізму та знижує ефективність захисту національних інтересів.

Зазначена проблема проявляється і на рівні адміністративної відповідальності. Так, стаття 212-3 Кодексу України про адміністративні правопорушення (далі – КУпАП) установлює відповідальність за порушення права на інформацію, однак має виразно однобокий характер: санкційний механізм спрямований виключно на захист запитувача та забезпечення відкритості діяльності органів влади [112]. Водночас чинне законодавство не передбачає відповідальності за зловживання інструментами прозорості, зокрема за системний збір управлінсько значущої інформації іноземними або афілійованими суб’єктами під виглядом реалізації права на звернення громадян чи доступ до інформації [1].

Таким чином, конституційний рівень правового регулювання визначає стратегічний вектор забезпечення інформаційної безпеки, однак їх реалізація у

частині нейтралізації зовнішнього впливу потребує конкретизації на рівні галузевого законодавства. Саме на цьому рівні наразі відсутня послідовна процедурна логіка активного адміністративно-правового захисту управлінських процесів, що зумовлює нормативну незавершеність відповідного механізму.

На рівні галузевого законодавства ключову роль у регулюванні інформаційних відносин у системі публічного управління відіграють закони загального характеру, що визначають принципи доступу до інформації, її обігу та використання суб'єктами владних повноважень. Саме ці акти створюють нормативне підґрунтя для реалізації конституційних гарантій у практичній діяльності публічної адміністрації.

Базовим у цій групі є Закон України «Про інформацію», який закріплює принципи відкритості, достовірності та законності інформації. Водночас закон не містить легального визначення інформаційної безпеки, яке б відповідало «комплексному підходу», та не розкриває специфіку інформаційних ризиків у публічному управлінні, зокрема пов'язаних із зовнішнім впливом на управлінські процеси [7]. Його норми мають універсальний характер і спрямовані передусім на баланс між свободою інформації та її захистом, залишаючи «процедурно-функціональний блок» безпекового механізму незаповненим.

Закон України «Про доступ до публічної інформації» конкретизує обов'язок суб'єктів владних повноважень забезпечувати відкритість управлінської діяльності. У контексті протидії зовнішньому впливу цей закон має подвійне значення: з одного боку, він підвищує прозорість, зменшуючи можливості для прихованого втручання; з іншого – він створює стан «процедурної незахищеності» [113]. Закон не передбачає механізмів оцінки ризиків використання відкритої інформації «афілійованими суб'єктами», які через механізми публічного управління можуть формувати маніпулятивний порядок денний. Це підтверджує нашу тезу про вразливість «горизонтального виміру» публічного управління.

Регулювання інформаційних відносин у сфері масових комунікацій здійснюється Законом України «Про медіа» [114]. Хоча він спрямований на захист інформаційного простору від дезінформації, його фокус зосереджений переважно на медійному сегменті й не охоплює повною мірою управлінські процедури. Окрему групу становлять закони «Про звернення громадян» [115] та «Про громадські об'єднання» [116]. Вони створюють умови для залучення ІГС до процесів ухвалення рішень, що є важливою складовою демократичного управління. Водночас відсутність у цих актах процедур оцінки афілійованості або джерел впливу на відповідних суб'єктів зумовлює підвищену вразливість до зовнішнього втручання.

У сукупності зазначені акти формують нормативний каркас інформаційної відкритості. Проте їх об'єднує спільна риса – орієнтація на регулювання інформаційних відносин як таких, без урахування їхньої безпекової складової у частині впливу на управлінські рішення. Це призводить до ситуації, за якої адміністративно-правові засоби забезпечення прозорості не трансформуються у механізми превенції та нейтралізації зовнішнього впливу, що свідчить про «регуляторну розірваність» механізму безпеки.

Окремого аналізу в межах цього підрозділу потребує нормативно-правове регулювання правового статусу та участі ІГС у формуванні й реалізації державної політики.

Система правових орієнтирів щодо розбудови взаємодії з громадянським суспільством ґрунтується на положеннях Конституції України та знаходить своє відображення у засадах внутрішньої і зовнішньої політики [117], а також у базових нормах муніципального права [98]. Безпосередня регламентація статусу окремих інститутів здійснюється через розгалужену мережу спеціальних законів. Зокрема, це стосується правового регулювання діяльності громадських об'єднань [116] та благодійних структур [118]. Окрему групу нормативних актів становлять закони, що гарантують права професійних спілок [119] та організацій роботодавців [120]. Крім того, специфіка релігійної діяльності [121], функціонування творчих спілок [122] та інструменти реалізації ініціатив через

органи самоорганізації населення [123] також мають чітко визначений законодавчий базис.

Динаміка розвитку цього сектору додатково програмується через акти програмно-стратегічного характеру. Серед них ключове місце посідає Національна стратегія у сфері прав людини (2021 р.) [124], а також вектори регіонального розвитку, визначені Урядом на період до 2027 року [125]. Окремим аспектом підготовки свідомого громадянського активу виступає реалізація Концепції розвитку громадянської освіти, затверджена відповідним розпорядженням Кабінету Міністрів України [126].

Аналіз спеціального законодавства, свідчить, що його нормативна спрямованість зосереджена переважно на забезпеченні реалізації суб'єктивних прав, свободи об'єднання та організаційної автономії відповідних суб'єктів. Водночас питання безпекових аспектів участі ІГС у процесах публічного управління в зазначених актах системно не врегульовані.

Характерною рисою чинного регулювання є відсутність нормативного розмежування функціональних ролей ІГС у публічному управлінні, попри те що на практиці вони залучаються не лише до консультативно-дорадчої діяльності, а й до нормотворчих процесів, правозастосовної діяльності, здійснення громадського контролю, а в окремих випадках – до реалізації делегованих владних або квазі-правоохоронних повноважень [101].

Зазначена багаторівнева інтеграція ІГС у систему публічного управління об'єктивно підвищує їх вплив на формування та реалізацію державної політики. Водночас відсутність у чинному законодавстві процедур адміністративно-правової верифікації афілійованості, джерел впливу та інтересів відповідних суб'єктів створює ризики використання ІГС як опосередкованих суб'єктів зовнішнього впливу на управлінські рішення. У такому разі механізми демократичної участі, як вже зазначалося вище, можуть виконувати функцію транзитного середовища для смислового або процедурного коригування управлінського порядку денного.

Таким чином, законодавство, що регулює діяльність ІГС, формує суперечливу нормативну конструкцію: з одного боку, ці суб'єкти визнаються партнерами держави у здійсненні нормотворчої, правозастосовчої та контрольної діяльності, з іншого – держава не наділена належними адміністративно-правовими інструментами оцінки безпекових ризиків такої взаємодії. Це зумовлює підвищену вразливість горизонтального виміру публічного управління та підтверджує висновок про фрагментарність механізму протидії опосередкованому зовнішньому впливу в інформаційній сфері.

Також, ключовим актом, який закріплює інформаційну безпеку як одну зі складових національної безпеки є Закон України «Про національну безпеку України» [29]. Разом із тим закон не розкриває змісту «адміністративно-правового механізму» у частині впливу на управлінські процедури, а роль інформаційної безпеки у публічному управлінні окреслює фрагментарно. В свою чергу це створює «декларативний розрив» між визначеними цілями та реальними інструментами їх досягнення [127, с. 71].

Закон України «Про основні засади забезпечення кібербезпеки України» встановлює основи захисту інтересів у кіберпросторі [128]. Попри зв'язок кіберзагроз з інформаційними процесами, закон зосереджується насамперед на технічному та інфраструктурному вимірах. Адміністративні процедури ухвалення рішень та ризики інституційно-процедурної деформації управлінських процесів через зовнішній вплив залишаються поза увагою.

Вагоме місце займають акти стратегічного планування: Доктрина інформаційної безпеки України [47] та Стратегія інформаційної безпеки [25]. У цих документах окреслено національні інтереси та визначено актуальні загрози, серед яких особливе місце відводиться інформаційним операціям та дезінформації. Водночас їх зміст має програмний характер: вони не трансформуються у чіткі «адміністративно-правові процедури» превенції та реагування на зовнішній вплив у повсякденній діяльності органів державної влади.

У чинній правовій системі України наявна група нормативно-правових актів, які не декларують протидію зовнішньому впливу як самостійну мету, проте

фактично регулюють окремі канали, через які такий вплив може реалізовуватися. Їхньою спільною рисою є фрагментарність, орієнтація на суміжні цілі (прозорість, доброчесність) та відсутність інтеграції в єдиний адміністративно-правовий механізм забезпечення інформаційної безпеки держави.

До цієї групи належать Закони України «Про запобігання корупції» [129], «Про очищення влади» [130], «Про політичні партії в Україні» [131], а також нещодавно введений у дію Закон України «Про лобіювання» [132].

Зокрема, Закон України «Про запобігання корупції» формує інструменти фінансового контролю та запобігання конфлікту інтересів [129]. Проте цей акт не передбачає механізмів ідентифікації іноземної або афілійованої заінтересованості, якщо вона не має прямого фінансового вираження.

При цьому йдеться не про заперечення легітимності лобіювання як інституту, а про відсутність у чинному регулюванні його інтеграції з механізмами забезпечення інформаційної та управлінської безпеки.

На особливу увагу заслуговує Закон України «Про лобіювання». Уперше в національній правовій системі інституціоналізовано діяльність із впливу на об’єкти публічного управління. Прийняття цього акта стало результатом виконання євроінтеграційних вимог та рекомендацій GRECO щодо прозорості впливу на прийняття рішень [133]. Однак у контексті інформаційної безпеки виникає «дилема демократичного контролю»: процедури, покликані легалізувати цивілізований лобізм, за відсутності спеціальних безпекових фільтрів, створюють ризик «нормативної мімікрії» [134, с. 122]. В адміністративно-правовому аспекті, цей закон створює легальний процедурний канал впливу, водночас зосереджуючись переважно на комерційній природі таких відносин. Політико-ідеологічні та безпекові цілі, характерні для практик зовнішнього впливу, не становлять предмета регулювання цього акта. Відсутність механізмів безпекової верифікації бенефіціарів формує ризик легалізації прихованого зовнішнього впливу під виглядом «прозорого лобізму» та використання легальних інструментів для просування інтересів, що можуть суперечити національній стійкості [135].

Загалом, це законодавство характеризується розпорошеністю та домінуванням фінансово-організаційної логіки. Такі норми частково обмежують окремі прояви впливу, проте не формують цілісного механізму, здатного забезпечити суверенітет публічного управління в інформаційній сфері.

Для систематизації виявлених нормативних розривів та демонстрації їх впливу на стійкість управлінських процедур до зовнішнього втручання доцільно узагальнити результати аналізу у вигляді аналітичної матриці.

В наведеній нижче аналітичній матриці (див. табл. 2.1.1) висвітлені дефіцити адміністративно-правового регулювання, які перешкоджають трансформації декларативних безпекових норм у реальну управлінську практику.

Таким чином, чинна нормативно-правова база у сфері забезпечення інформаційної безпеки України характеризується наявністю значного масиву законодавчих і стратегічних актів, які, проте, не формують цілісної адміністративно-правової моделі протидії зовнішньому впливу на публічне управління. Домінування декларативних, програмних і секторальних норм зумовлює розрив між стратегічними цілями безпеки та відсутністю процедурно оформлених механізмів захисту управлінських процесів. Інформаційна діяльність суб’єктів публічної адміністрації як об’єкт потенційного зовнішнього втручання залишається нормативно недостатньо врегульованою, що обмежує спроможність держави до превентивного виявлення та нейтралізації таких загроз. Систематизовані у дослідженні дефіцити підтверджують необхідність формування спеціалізованого адміністративно-правового механізму забезпечення інформаційної безпеки України в аспекті протидії зовнішньому впливу на публічне управління. Концептуальні засади якого будуть обґрунтовані за результатами комплексного аналізу в межах цього та наступного розділів дослідження.

Таблиця 2.1.1

Комплексна матриця дефіцитів адміністративно-правового регулювання у контексті протидії зовнішньому впливу на публічне управління

Група нормативно-правових актів	Ключові акти (приклади)	Сфера вразливості публічного управління	Тип дефіциту (узагальнений)	Зміст дефіциту та його прояв
Фундаментально-конституційний блок	Конституція України (ст. 17, 34, 40)	Суверенітет публічного управління; інформаційна безпека держави	Процедурний дефіцит	Конституційні норми мають стратегічно-декларативний характер і не містять операціоналізованих адміністративно-правових алгоритмів обмеження інформаційних прав у разі виявлення афілійованого зовнішнього впливу
Загально-інформаційний блок	ЗУ «Про інформацію», ЗУ «Про доступ до публічної інформації»	Процесуальна чистота управлінської діяльності	Регуляторна сліпота	Орієнтація на забезпечення доступу та відкритості без урахування ризиків використання інформації афілійованими або проксі-суб'єктами; відсутність процедур оцінки безпекових наслідків інформаційної відкритості
Блок медіа-комунікацій	ЗУ «Про медіа»	Інформаційний супровід діяльності органів влади	Секторальний дефіцит	Фокус на регулюванні медіаринку та контенту не охоплює внутрішні управлінські процедури та канали смислового впливу на суб'єктів владних повноважень
Блок участі громадськості (горизонтальний вимір)	ЗУ «Про звернення громадян», ЗУ «Про громадські об'єднання», ЗУ «Про благодійну діяльність…»	Горизонтальні управлінські процедури	Інституційний дефіцит	Відсутність адміністративно-правових фільтрів верифікації афілійованості та інтересів ІГС перетворює механізми участі на транзитне середовище проксі-впливу
Спеціальний безпековий блок	ЗУ «Про національну безпеку України», ЗУ «Про кібербезпеку», Стратегія	Загальна стійкість системи безпеки	Функціональний дефіцит	Домінування стратегічних і техноцентричних підходів без інтеграції з адміністративно-правовими процедурами ухвалення рішень;

Група нормативно-правових актів	Ключові акти (приклади)	Сфера вразливості публічного управління	Тип дефіциту (узагальнений)	Зміст дефіциту та його прояв
	інформаційної безпеки			ігнорування гуманітарних і психологічних аспектів впливу
Блок антикорупції та люстрації	ЗУ «Про запобігання корупції», ЗУ «Про очищення влади»	Доброчесність і неупередженість посадовців	Редукційний дефіцит	Зосередження на фінансових і ретроспективних критеріях не охоплює нематеріальні форми зовнішнього впливу (ідеологічні, смислові, інформаційні)
Політико-інституційний блок	ЗУ «Про політичні партії в Україні»	Формування політичної волі	Змістовний дефіцит	Контроль джерел фінансування не доповнюється аналізом змісту та спрямованості впливу на державну політику, що знижує ефективність захисту від зовнішніх маніпуляцій
Блок інституціоналізації впливу	ЗУ «Про лобіювання»	Легальні процедури впливу на рішення	Безпековий дефіцит	Легалізація впливу без процедур безпекової верифікації бенефіціарів створює ризик нормативної мімікрії зовнішнього втручання під прозорий лобізм, що зумовлює інституційно-процедурну деформацію управлінських процесів та провокує конфлікт між вимогами прозорості й національної стійкості

Джерело: складено автором на основі аналізу [1; 7; 25; 29; 47; 98; 101; 110–135].

2.1.2. Нормативні ініціативи та спроби конкретизації законодавства щодо протидії зовнішньому впливу на публічне управління

Виявлені у попередньому підрозділі прогалини чинного нормативно-правового регулювання у сфері інформаційної безпеки України, зокрема критична відсутність інтегрованих адміністративно-правових механізмів протидії зовнішньому впливу безпосередньо в процесах публічного управління, зумовили появу численних законодавчих ініціатив. Проте аналіз цих ініціатив дозволяє констатувати їхню фрагментарність: вони формувалися як ситуативні реакції на політико-безпекові виклики, без єдиного концептуального бачення інформаційної безпеки як «нормативно закріпленого стану» стабільності управлінських процесів.

Унаслідок цього розвиток нормативного реагування не набув ознак цілісної адміністративно-правової конструкції. Замість системної протидії деформаціям управлінського процесу, держава вдавалася до розрізнених спроб – від жорстко репресивних і символічно стигматизаційних до декларативно-прозорих моделей. При цьому домінуючим залишався хибний підхід, за якого об’єктом регулювання визначалися окремі суб’єкти (громадські об’єднання, медіа, донори), тоді як самі управлінські процедури, посадові повноваження та інформаційно-процедурні механізми прийняття рішень фактично випадали з поля системного правового аналізу.

У зв’язку з цим доцільним є аналіз еволюції нормативних ініціатив саме крізь призму суверенітету публічного управління як об’єкта захисту. Це дозволить не лише реконструювати логіку законодавчих пошуків, але й обґрунтувати перехід від контролю за «особою» до контролю за «процесом», що є ключовим для забезпечення інформаційної безпеки держави в умовах гібридних загроз.

Першою спробою нормативного реагування на проблему зовнішнього впливу в Україні стали законодавчі ініціативи початку 2014 року, реалізовані в умовах гострої політичної кризи та підвищеної чутливості до питань

національної безпеки [136]. Ключовим елементом цих змін стало запровадження у законодавство поняття «іноземний агент», зокрема через внесення положень до законів, що регулювали діяльність громадських об’єднань [137, с. 84].

Формально задекларованою метою змін було підвищення прозорості організацій з іноземним фінансуванням, проте за своєю юридичною природою ці норми ґрунтувалися на низці концептуальних помилок. Ми оцінюємо їх як адміністративно-правову деформацію, яка детермінувала викривлення самої моделі реагування: замість створення процедурних запобіжників для захисту суверенітету публічного управління, зусилля законодавця було спрямовано на штучну трансформацію правового статусу суб’єктів.

У результаті поняття «іноземний агент» набуло не стільки регулятивного, скільки виразно стигматизаційного характеру. Його застосування було спрямоване передусім на сферу громадянського суспільства («горизонтальний вимір»), тоді як посадові особи, органи публічної влади та механізми формування управлінських рішень залишалися поза межами нормативної уваги. Це спричинило значний суспільний спротив, делегітимацію відповідних норм та їх подальше скасування.

Водночас значення цього етапу не обмежується його нормативною нетривкістю. Саме у 2014 році було сформовано стійкий негативний символічний ефект терміна «іноземний агент», який у подальшому істотно ускладнив фахову дискусію щодо правових механізмів протидії зовнішньому впливу, оскільки будь-які подібні ініціативи автоматично асоціювалися з репресивними практиками.

Ранні ініціативи продемонстрували фундаментальну методологічну помилку у визначенні об’єкта правового регулювання: проблема була зведена до діяльності окремих суб’єктів, тоді як публічне управління та управлінські процедури як ключові точки ризику залишилися поза сферою системного аналізу.

Наступний етап еволюції законодавчих підходів характеризується відмовою від стигматизаційної моделі «іноземних агентів» та переходом до риторики прозорості, підзвітності й фінансової відкритості. Протягом 2017–

2020 років у Верховній Раді України було зареєстровано низку законопроєктів, зокрема: президентські ініціативи № 6674 [138] та № 6675 [139], а також депутатські проєкти № 8501 [140], № 3564 [141], № 3936 [142], спрямованих на розширення вимог щодо звітності та декларування джерел фінансування суб'єктів публічної взаємодії.

Зміна дискурсу з репресивного на формально нейтральний створювала враження концептуального прогресу. Проте в адміністративно-правовому вимірі ці ініціативи відтворювали ключову методологічну ваду попереднього етапу – неправильне визначення предмета правового впливу. Законодавець знову зосередився не на управлінських процесах, а на фінансових потоках, фактично підміняючи безпекову проблему зовнішнього впливу питанням фінансової прозорості.

Критичний аналіз цих ініціатив через призму комплексного підходу дозволяє виявити наступні дефіцити: прозорість як інструмент фінансового контролю не є тотожною забезпеченню інформаційної безпеки; вона фіксує походження ресурсів, але не дозволяє ідентифікувати способи маніпулятивного формування управлінського порядку денного чи впливу на експертні висновки; у законопроєктах повністю випав з поля зору інформаційно-процедурний аспект впливу, який, як було доведено у підрозділі 1.3, є визначальним у сучасних моделях гібридних загроз;

запропоновані механізми не містили інструментів оцінки ризиків безпосередньо в системі публічного управління, зокрема: алгоритмів перевірки управлінських рішень на предмет зовнішньої зумовленості; процедур верифікації афілійованості осіб, залучених до підготовки стратегічних документів; інструментів адміністративного реагування у разі виявлення системної деформації управлінських процесів.

Таким чином, законодавець працював з об'єктами (організаціями, ресурсами), але не з процесами – ухваленням рішень та формуванням політик. Це підтверджує нашу тезу про «регуляторну сліпоту»: держава намагалася

контролювати фінансові потоки суб'єкта, залишаючи відкритим доступ до інформаційного ядра управління.

Законодавчі ініціативи 2017–2020 років закріпили помилкове ототожнення зовнішнього впливу з фінансовою звітністю. Це не лише не забезпечило захисту суверенітету публічного управління, а й відтермінувало формування повноцінного адміністративно-правового механізму забезпечення інформаційної безпеки України.

Якісно новий етап розвитку нормативних ініціатив у сфері протидії зовнішньому впливу пов'язаний зі зміщенням фокусу регулювання з діяльності окремих суб'єктів громадянського суспільства на систему публічного управління та носіїв владних повноважень. На відміну від попередніх підходів, що концентрувалися на фінансуванні, організаційно-правових формах або формальній прозорості, ці ініціативи вперше окреслили зовнішній вплив як управлінську проблему, що безпосередньо загрожує суверенітету публічного управління.

Ключовим маркером цього концептуального зсуву став проєкт Постанови ВРУ від 08.09.2021 № 6009 [143]. Попри переважно декларативний характер документа, його наукова значущість полягає у спробі змінити саму парадигму юридичного захисту держави: від контролю за фінансовою діяльністю окремих суб'єктів – до утвердження та відновлення державного суверенітету в сфері державного управління.

Разом із тим, на відміну від підходу, закладеного у згаданому проєкті, у цьому дослідженні категорія суверенітету розглядається ширше. Якщо проєкт № 6009 обмежує об'єкт захисту суто державно-управлінською вертикаллю, то запропонований нами суверенітет публічного управління додатково охоплює муніципальний рівень та процедури взаємодії з громадянським суспільством («горизонтальний вимір»).

У межах цієї нормативної ініціативи зовнішній вплив уперше пропонується розглядати не як допустиму форму політичної чи громадської активності, а як втручання у здійснення повноти державної влади та

самостійність органів державної влади України у вирішенні питань державного життя.

Принциповими відмінностями запропонованого підходу стали:

перенесення акценту з правового статусу окремих організацій на сферу державного управління, у якій об'єктом захисту визначається суверенне право держави на самостійне ухвалення управлінських рішень;

фокус на забезпеченні незалежності органів державної влади та їх посадових осіб від будь-яких форм зовнішнього втручання, зокрема з боку іноземних держав, міжнародних організацій та афілійованих з ними суб'єктів;

постановка питання про допустимість участі у формуванні та реалізації державної політики осіб, пов'язаних із фінансуванням або інтересами іноземного походження.

Хоча зазначена постанова мала декларативний характер і не створювала безпосередньо зобов'язувальних норм, її значення полягає у формуванні нової нормативної оптики. Вона заклала підґрунтя для переходу від політично забарвлених дискусій до адміністративно-правового аналізу зовнішнього впливу як системного явища, що проникає у внутрішні механізми державного управління.

Цей перехід дозволяє констатувати зміну самої природи загроз: від прямої дезінформації до складних форм інституційної дифузії. Вона проявляється у тому, що зовнішній чинник не завжди прагне зруйнувати систему ззовні, а намагається «вбудуватися» в її легальні процедури, підміняючи національний інтерес цілями іноземних суб'єктів. Такий підхід свідчить про те, що «об'єкт атаки» зміщується з інформаційного поля безпосередньо в операційне ядро прийняття управлінських рішень.

Водночас обмеженість цього етапу полягала у відсутності чітких процедурних інструментів реалізації задекларованих принципів, визначених суб'єктів контролю та механізмів інтеграції проголошених підходів у чинну систему адміністративного права. Систематизація цих ініціатив та їх статус наведені у таблиці 2.1.2, аналіз якої дозволяє констатувати, що більшість спроб

нормативної конкретизації залишилися на рівні декларацій і не отримали подальшого нормативного розвитку.

Таблиця 2.1.2

Нормативні ініціативи щодо протидії зовнішньому впливу у сфері публічного управління

Рік	№ законопроєкту / документа	Ініціатор(и)	Мета	Статус
2014	№ 3879 (закон «16 січня»)	В. Олійник, В. Колісніченко	Визначення ГО як іноземного агента за умови іноземного фінансування та політичної діяльності	Скасовано у лютому 2014
2017	№ 6674	Президент П. Порошенко	Запровадження прозорої звітності ГО щодо доходів та видатків, підвищення відкритості в їх діяльності	Не прийнято
2017	№ 6675	Президент П. Порошенко	Прозора звітність ГО та фізичних осіб-підприємців, що отримують кошти з бюджетів або міжнародну техдопомогу (податкові пільги)	Відкликано
2018	№ 8501	С. Тарута	Прозорість ГО та благодійних організацій, фінансування яких від іноземних суб'єктів перевищує 50%	Відкликано
2020	№ 3326	Ф. Христенко	Запобігання втручанню через осіб, що отримували кошти/послуги від іноземних суб'єктів, при зайнятті ними посад у держорганах	Не розглянуто
2020	№ 3564	О. Дубінський	Забезпечення прозорості ГО та благодійних організацій, що отримують фінансову підтримку від іноземних держав, організацій чи громадян	Не розглянуто
2020	№ 3936	О. Дубінський	Запровадження звітності для ГО, що отримують фінансову підтримку від іноземних суб'єктів, зокрема в рамках техдопомоги	Не ухвалено
2021	№ 6009 (проєкт Постанови)	А. Поляков	Схвалення Декларації щодо негайного відновлення державного суверенітету у сфері державного управління	Відкликано

Джерело: складено автором на основі аналізу [136–143].

Узагальнюючи, слід констатувати, що нормативні ініціативи аналізованого періоду виконали переважно концептуально-перехідну функцію, окресливши новий вектор правового осмислення зовнішнього впливу, проте не сформували цілісного механізму захисту від інституційно-процедурної деформації управлінських процесів. Головною вадою цих спроб залишається фокусування на фінансовому статусі окремих суб'єктів, що залишає поза увагою ризики викривлення автономності адміністративної дискреції та порушення суверенітету України в публічному управлінні.

Виявлена нормативна фрагментарність, «регуляторна сліпота» та відсутність процедур верифікації афілійованості створюють умови для прихованого втручання в процеси управління. Ефективність протидії таким загрозам визначається не лише якістю правових норм, а й архітектурою системи суб'єктів публічної адміністрації, їхньою здатністю до координації та процесуально контрольованого застосування безпекових фільтрів. Це зумовлює необхідність переходу від аналізу актів до дослідження інституційно-координаційного виміру забезпечення інформаційної безпеки у підрозділі 2.2.

2.2. Система суб'єктів забезпечення інформаційної безпеки України в аспекті протидії зовнішньому впливу на публічне управління

Ключовими елементами адміністративно-правового механізму забезпечення інформаційної безпеки України є суб'єкти забезпечення інформаційної безпеки. Вони формують інституційний каркас державної політики у сфері запобігання, виявлення та протидії загрозам національній безпеці України в інформаційній сфері. У науковій літературі під даною категорією розуміється «система державних і недержавних інституцій, а також громадян України, об'єднаних спільною метою щодо захисту національних інтересів в інформаційній сфері» [144, с. 164].

Відповідно до положень п. 6 Доктрини інформаційної безпеки України функції із забезпечення інформаційної безпеки покладаються на низку органів державної влади, які утворюють інституційну систему реалізації державної

інформаційної політики. До ключових суб'єктів належать, зокрема, Рада національної безпеки і оборони України (далі – РНБО), КМУ, а також ЦОВВ, що формують і реалізують державну політику у відповідних сферах, зокрема Міністерство культури України (далі – Мінкультури) (до реорганізацій – Міністерство інформаційної політики) [145], Міністерство закордонних справ України (далі – МЗС) та Міністерство оборони України (далі – МОУ).

Важливу роль у системі забезпечення інформаційної безпеки відіграють також спеціалізовані органи сектору безпеки і оборони, зокрема Служба безпеки України (далі – СБУ) та розвідувальні органи держави. Відповідно до ст. 5 Закону України «Про розвідку», до них належать Служба зовнішньої розвідки України (далі – СЗР), розвідувальний орган Міністерства оборони України (Головне управління розвідки (далі – ГУР)), а також розвідувальний підрозділ центрального органу виконавчої влади, що реалізує державну політику у сфері охорони державного кордону [146].

Окремі функції у сфері захисту інформаційного простору виконують органи спеціального призначення та інституції, що здійснюють регуляторні й аналітичні функції, зокрема Державна служба спеціального зв'язку та захисту інформації України (далі – Держспецзв'язку), Національний інститут стратегічних досліджень (далі – НІСД), який забезпечує науково-аналітичний супровід формування та реалізації державної інформаційної політики.

До забезпечення інформаційної безпеки також долучаються органи, діяльність яких пов'язана з регулюванням інформаційної та медійної сфери, зокрема Державне агентство з питань кіно, Національна рада України з питань телебачення і радіомовлення та Державний комітет телебачення і радіомовлення України (далі – Держкомтелерадіо) [47].

Зважаючи на комплексний характер сучасних загроз та специфіку функціональних завдань, у складі системи суб'єктів доцільно виділити: спеціально уповноважені суб'єкти, для яких забезпечення національної (зокрема інформаційної) безпеки є основним завданням; суб'єкти, які беруть участь у її забезпеченні під час реалізації своїх профільних функцій.

Дослідження адміністративно-правового статусу учасників безпекових відносин потребує деталізації функцій державних органів, на які покладено специфічні завдання щодо зміцнення інформаційної стійкості у межах їхньої основної компетенції. Окрім РНБО та Кабміну, чия роль чітко детермінована Доктриною інформаційної безпеки України, до цієї ієрархічної структури належать: по-перше, Президент України та Верховна Рада України, які реалізують загальне керівництво, стратегічну координацію та контроль за виконанням заходів у безпековій сфері; по-друге – органи, на які безпосередньо покладено імплементацію практичних заходів у площині інформаційної безпеки.

Розглянемо детальніше повноваження суб'єктів, що здійснюють загальне управління та нагляд у цій сфері.

Провідну роль у системі забезпечення інформаційної безпеки відіграє Президент України, який відповідно до конституційного статусу виступає гарантом державного суверенітету, територіальної цілісності, додержання Конституції України та прав і свобод людини і громадянина [1]. У контексті інформаційної безпеки це передбачає стратегічне лідерство у захисті управлінської та інформаційної автономії держави.

Законодавче забезпечення відповідної сфери покладено на ВРУ як єдиний орган законодавчої влади. Функції ВРУ у безпековій царині безпосередньо випливають із її фундаментальних конституційних повноважень щодо нормативного регулювання та парламентського контролю [1].

Координаційні функції у сфері національної безпеки, у тому числі інформаційної, виконує РНБО, яка діє як консультативно-координаційний орган при Президентові України. До її повноважень належить підготовка пропозицій щодо реалізації державної політики у сфері національної безпеки та оборони, а також координація діяльності органів виконавчої влади в умовах як мирного часу, так і в умовах воєнного чи надзвичайного стану, включаючи реагування на кризові ситуації в інформаційній сфері [147].

У структурі РНБО функціонує Центр протидії дезінформації (далі – ЦПД), створений рішенням РНБО та введений у дію Указом Президента України від

19 березня 2021 року № 106/2021 [148]. Основним завданням цієї інституції є формування системного підходу до протидії дезінформаційним впливам і підвищення стійкості інформаційного середовища держави. До ключових напрямів діяльності Центру належать виявлення та нейтралізація інформаційних загроз, розроблення механізмів протидії дезінформаційним кампаніям, а також запобігання спробам маніпулятивного впливу на суспільну свідомість з боку зовнішніх акторів [149].

Значну роль у реалізації державної політики у сфері інформаційної безпеки відіграє КМУ як вищий орган у системі органів виконавчої влади [150]. Відповідно до конституційної моделі державного управління уряд є відповідальним перед Президентом України та підконтрольним і підзвітним ВРУ у межах, визначених ст. ст. 85 та 87 Конституції України [1]. Згідно зі ст. 116 Конституції України КМУ забезпечує спрямування та координацію діяльності міністерств і інших органів виконавчої влади, у тому числі у сфері інформаційної політики та безпеки [1].

Безпосереднє виконання заходів щодо забезпечення інформаційної безпеки покладається на низку спеціалізованих державних органів. Згідно з п. 6 Доктрини інформаційної безпеки України до них належать, зокрема, СБУ, Держспецзв'язку, СЗР, МОУ та МЗС [47]. Поряд із цим до відповідної системи суб'єктів обґрунтовано відносять також Національну комісію, що здійснює державне регулювання у сферах електронних комунікацій, радіочастотного спектра та надання послуг поштового зв'язку (далі – НКЕК), яка є правонаступником Національної комісії, що здійснює державне регулювання у сфері зв'язку та інформатизації, та забезпечує регуляторні механізми функціонування цифрової інфраструктури й електронних комунікацій [151].

Важливі функції у сфері захисту інформаційного простору виконують також органи, діяльність яких пов'язана з регулюванням медійного та культурного середовища, зокрема Мінкультури, Держкіно, Нацрада та Держкомтелерадіо. У межах своєї компетенції ці інституції беруть участь у формуванні політики інформаційної та інформаційно-психологічної безпеки держави.

Водночас у Стратегії інформаційної безпеки визначено дещо іншу конфігурацію суб'єктів, до якої віднесено РНБО, КМУ, центральні органи виконавчої влади, що формують та реалізують державну політику в інформаційній сфері, МЗС, МОУ, СБУ, розвідувальні органи, Нацраду, а також ІГС [25].

Реалізація Стратегії кібербезпеки України забезпечується суб'єктами національної системи кібербезпеки, до яких належать, зокрема, МЗС, Міністерство цифрової трансформації України (далі – Мінцифри), Міністерство освіти і науки України (далі – МОН) та інші органи державної влади, що діють у межах визначених повноважень. Координаційні функції у цій сфері здійснює Національний координаційний центр кібербезпеки (далі – НКЦК), який функціонує як робочий орган РНБО [152].

Водночас найбільш розгорнуте визначення кола суб'єктів кібербезпеки міститься у Законі України «Про основні засади забезпечення кібербезпеки України». У цьому нормативному акті до відповідної системи віднесено Президента України, КМУ та НКЦК, міністерства й інші ЦОВВ, місцеві державні адміністрації та органи місцевого самоврядування, правоохоронні й розвідувальні структури, Збройні Сили України (далі – ЗСУ) та інші військові формування, Національний банк України (далі – НБУ), а також суб'єктів господарювання, операторів критичної інфраструктури і громадян [128].

При цьому до основних суб'єктів національної системи кібербезпеки закон відносить Держспецзв'язку, Національну поліцію України (далі – НПУ), СБУ, МОУ та Генеральний штаб Збройних Сил України (далі – ГШ ЗСУ), розвідувальні органи, НБУ і МЗС [128].

Наведений перелік свідчить про тісний взаємозв'язок інституційного забезпечення кібербезпеки з ширшою системою захисту інформаційної сфери держави.

Відповідно до ч. 4 ст. 3 Закону України «Про національну безпеку України», інформаційна безпека та кібербезпека визначені як окремі сфери державної політики [29]. Тобто у законодавчому вимірі вони функціонують як

самостійні складові національної безпеки. Водночас у науковій літературі простежується тенденція до їхнього інтегрованого розгляду, оскільки заходи кібербезпеки переважно спрямовані на захист інформаційних процесів та інфраструктури, що дає підстави розглядати кібербезпеку як техніко-технологічний вимір інформаційної безпеки [31, с. 72].

Узагальнюючи варіативність складу суб'єктів, представлену в актуальних нормативно-правових актах, вбачається за необхідне сформувати цілісну систему інституційних елементів, адаптовану до специфіки протидії зовнішньому впливу в царині публічного управління. Такий підхід дозволить подолати нормативну фрагментарність та забезпечити комплексний захист інформаційного суверенітету.

В академічному дискурсі традиційно виокремлюють два фундаментальні методологічні підходи до класифікації зазначених суб'єктів: класичний організаційно-правовий (інституційний) та функціональний [153, с. 43].

Класичний організаційно-правовий підхід базується на диференціації суб'єктів за їхнім правовим статусом та приналежністю до державного сектору: державні суб'єкти: охоплюють ЦОВВ, спеціальні служби, правоохоронні інституції, органи регулювання та місцевого самоврядування; недержавні суб'єкти: включають інститути громадянського суспільства, медіа-ресурс, аналітичні центри, а також суб'єкти господарювання та операторів критичної інфраструктури.

Слід констатувати, що попри здатність інституційного підходу чітко окреслити коло залучених учасників, він фактично нівелює їхню реальну функціональну роль у системі забезпечення безпеки. Натомість, функціональний підхід виявляється значно продуктивнішим для системного аналізу, оскільки він зміщує акцент на специфіку конкретних завдань, компетенцій та персональних сфер відповідальності суб'єктів.

З метою обґрунтування авторської моделі протидії зовнішньому впливу, доцільно здійснити стислий функціональний аналіз ключових завдань, покладених на органи державної влади у сфері забезпечення інформаційної

безпеки. Це дозволить виявити існуючі «прогалини» в імплементації заходів контролю та обґрунтувати розширення кола суб'єктів за рахунок інституцій, що відповідають за фінансовий та кадровий моніторинг.

Аналіз функціонального наповнення діяльності суб'єктів державного сектору дозволяє деталізувати їхню роль у забезпеченні інформаційної стійкості держави. Зокрема, Мінкультури виступає регулятором, який здійснює нормативно-правове забезпечення та визначає стратегічні напрями розвитку у сфері інформаційної безпеки. У взаємодії з МЗС відомство реалізує заходи з формування позитивного іміджу держави на міжнародній арені з метою захисту її політичних та економічних інтересів [29].

Водночас Мінкультури, Держкіно, Нацрада та Держкомтелерадіо фокусуються на контрпропаганді, забезпечуючи захист національного простору від деструктивного аудіовізуального контенту держави-агресора. Крім того, вони стимулюють виробництво вітчизняного інформаційного продукту, спрямованого на висвітлення героїчного спротиву Українського народу російській агресії [47].

МОУ є головним органом у системі ЦОВВ, що формує безпекову політику у воєнній сфері та сфері оборони [154].

ГШ ЗСУ є головним органом військового управління з планування оборони держави, стратегічного планування застосування ЗСУ та визначених сил і засобів інших складових сил оборони та здійснює координацію виконання завдань у сфері оборони на всіх рівнях управління. [155].

До цілісної структури інституційного забезпечення інформаційної безпеки у воєнній сфері інтегровано також і спеціалізовані структурні підрозділи ГШ ЗСУ. У межах визначеної компетенції МОУ та ГШ ЗСУ реалізують наступні завдання:

організовують функціонування системи військово-цивільних зв'язків та забезпечують взаємодію з вітчизняними й закордонними медіа для висвітлення поточної ситуації на полі бою;

здійснюють активну протидію спеціальним інформаційним операціям, що спрямовані проти ЗСУ та інших військових формувань;

забезпечують супроводження оборонних завдань інформаційними засобами та донесення верифікованої інформації до особового складу через власні медіа-ресурси [47];

реалізують заходи з відбиття воєнної агресії у кіберпросторі (кібероборону) та координують військову співпрацю з Організацією Північно-Атлантичного договору (далі – НАТО) та міжнародними організаціями щодо колективного захисту від кіберзагроз [128].

Зовнішньополітичний вектор забезпечення інформаційної стійкості держави детермінований діяльністю МЗС як головного органу у системі ЦОВВ у сфері зовнішніх зносин [156]. На відомство покладено завдання щодо:

формування та впровадження стратегій публічної й культурної дипломатії, а також координації інформаційної активності державних органів на міжнародній арені;

донесення офіційної позиції України до керівництва іноземних держав, парламентів, бізнес-спільнот та експертних кіл, що сприяє просуванню позитивного іміджу держави за кордоном;

налагодження двосторонньої та багатосторонньої взаємодії з міжнародними партнерами для адаптації найкращих світових практик у контексті відсічі інформаційним загрозам;

розвитку євроінтеграційних процесів у сфері кібербезпеки та координації спільних із Європейським Союзом (далі – ЄС) і євроатлантичною спільнотою дипломатичних дій у відповідь на деструктивну кіберактивність [128].

Важливу роль у цифровій трансформації безпекових процесів відіграє Мінцифри, що забезпечує формування та реалізацію державної політики у сфері цифрового розвитку, електронного урядування та цифрових інновацій, включаючи розвиток штучного інтелекту та електронних комунікацій [157].

До науково-освітнього та правоохоронного сегментів інституційної системи забезпечення інформаційної безпеки належать низка органів державної

влади, діяльність яких пов’язана з формуванням інтелектуального, технологічного та безпекового потенціалу держави.

МОН забезпечує формування та реалізацію державної політики у сферах освіти, науки, інноваційної діяльності та трансферу технологій. У межах визначених повноважень відомство здійснює державний нагляд за діяльністю закладів освіти та інших суб’єктів освітньої діяльності незалежно від форми власності [158].

СБУ є державним органом спеціального призначення з правоохоронними функціями, діяльність якого спрямована на гарантування державної безпеки [159]. У сфері інформаційної безпеки СБУ здійснює виявлення та нейтралізацію загроз у медійному та цифровому середовищі, протидіє інформаційним операціям, спрямованим на підрив конституційного ладу і територіальної цілісності держави, а також реалізує контррозвідувальні заходи у сфері кібербезпеки та захисту критичної інфраструктури. До її компетенції належить і розслідування кіберінцидентів, що становлять загрозу державним інформаційним ресурсам [128].

Держспецзв’язку виконує функції із розвитку систем урядового та спеціального зв’язку, а також реалізує державну політику у сферах криптографічного та технічного захисту інформації. Її діяльність спрямована на забезпечення кіберзахисту державних інформаційних ресурсів і координацію суб’єктів національної системи кібербезпеки, зокрема шляхом проведення оцінки захищеності об’єктів критичної інфраструктури [128; 160].

Розвідувальні органи України відіграють важливу роль у виявленні та протидії зовнішнім інформаційним загрозам, забезпечуючи захист національних інтересів держави в інформаційній сфері на міжнародному рівні [25].

НПУ як центральний орган виконавчої влади у сфері забезпечення правопорядку виконує завдання з протидії злочинності, у тому числі у цифровому середовищі [161]. У межах своїх повноважень поліція здійснює розслідування кіберзлочинів, забезпечує реагування на правопорушення у

кіберпросторі та сприяє підвищенню обізнаності громадян щодо безпеки в мережі Інтернет [128].

Регуляторний та експертно-аналітичний супровід державної політики у сфері інформаційної безпеки забезпечують окремі спеціалізовані інституції. Зокрема, НБУ встановлює вимоги до кіберзахисту інформаційної інфраструктури банківського сектору та забезпечує функціонування фінансової системи з урахуванням сучасних кіберзагроз [128; 162].

Державне регулювання у сферах електронних комунікацій, радіочастотного спектра та надання послуг поштового зв'язку здійснює НКЕК. Її діяльність спрямована на забезпечення стабільного функціонування цифрової інфраструктури, модернізацію мереж та реалізацію безпекових стандартів у сфері електронних комунікацій відповідно до вимог національної безпеки [151].

Науково-аналітичне забезпечення державної політики у сфері інформаційної безпеки здійснює НІСД, який забезпечує експертний супровід процесу формування стратегічних рішень у відповідній сфері [47].

Важливим елементом реалізації державної інформаційної політики є взаємодія органів державної влади з ІГС. У Стратегії інформаційної безпеки передбачено, що виконання її положень забезпечується органами державної влади у співпраці з органами місцевого самоврядування, ЦПД та громадянським суспільством [25].

Відповідно до п. 7 Порядку проведення консультацій з громадськістю до ІГС належать громадські об'єднання, благодійні та релігійні організації, творчі та професійні спілки, асоціації роботодавців, органи самоорганізації населення, незалежні медіа та інші непідприємницькі організації, легалізовані відповідно до законодавства України [100].

Якщо розглядати систему суб'єктів забезпечення інформаційної безпеки у контексті протидії зовнішньому впливу на публічне управління, доцільно розширити цей перелік інституціями, що здійснюють правовий, кадровий, фінансовий та контрольний нагляд. До них, зокрема, належать Міністерство юстиції України (далі – Мін'юст), Національне агентство України з питань

державної служби (далі – НАДС), Національне агентство з питань запобігання корупції (далі – НАЗК), Державна служба фінансового моніторингу України (далі – Держфінмоніторинг), а також Державна податкова та Державна митна служби (далі – ДПС, ДМС). Саме ці органи забезпечують виявлення та фіксацію фактів прямого або опосередкованого фінансування діяльності суб'єктів з боку іноземних акторів.

Мін'юст реалізує державну правову політику, забезпечує нормотворчу діяльність уряду та ведення державних реєстрів, що дозволяє здійснювати правову верифікацію суб'єктів правовідносин [163].

НАЗК здійснює реалізацію антикорупційної політики, зокрема шляхом аналізу фінансових декларацій та моніторингу потенційних ризиків незаконного збагачення або отримання неправомірного фінансування з іноземних джерел [128].

ДПС та ДМС забезпечують фіскальний контроль і реалізацію державної податкової та митної політики, що дозволяє виявляти порушення у сфері фінансових потоків і запобігати використанню економічних механізмів для зовнішнього впливу [164].

НАДС забезпечує формування та реалізацію державної політики у сфері державної служби і здійснює функціональне управління кадровою системою публічної влади [165].

Держфінмоніторинг реалізує державну політику у сфері запобігання легалізації доходів, одержаних злочинним шляхом, та фінансуванню тероризму, що дозволяє фіксувати факти надходження коштів від іноземних суб'єктів [166].

Залучення зазначених інституцій розширює функціональні можливості державної системи захисту інформаційного простору та дозволяє трансформувати її з моделі переважно технологічного реагування на загрози у комплексний адміністративно-правовий механізм забезпечення інформаційної безпеки держави.

З урахуванням проведеного аналізу функцій та повноважень державних органів, залучених до забезпечення інформаційної безпеки України, а також із застосуванням функціонального підходу систему відповідних суб'єктів у

контексті протидії зовнішньому впливу на публічне управління доцільно структурувати на п’ять взаємопов’язаних підсистем (див. табл. 2.2.1).

Таблиця 2.2.1.

Класифікація суб’єктів забезпечення інформаційної безпеки України

(функціональний підхід)

№ з/п	Підсистема	Суб’єкти	Домінуюча функція	Зміст діяльності
1.	Стратегічно-координаційна	Президент України, РНБО (ЦПД), КМУ, ВРУ	Політико-правова детермінація	Визначення стратегічного вектора, формування нормативного базису та міжвідомча координація
2.	Операційно-виконавча	СБУ, НПУ, Держспецзв’язку, розвідувальні органи	Деструктивна нейтралізація	Безпосереднє виявлення, документування та технічне нівелювання операцій зовнішнього втручання
3.	Контрольно-аналітична	НАЗК, НАДС, НКЕК, Держфінмоніторинг, Мін’юст, НБУ, ДПС, ДМС	Превентивна верифікація	Ідентифікація ознак зовнішньої афілійованості через фінансовий моніторинг та кадровий аудит (спецперевірки)
4.	Гуманітарно-комунікаційна	Мінкультури, МОН, Мінцифри, Нацрада, ЦПД	Формування імунітету	Створення умов для несприйнятливості суспільства до маніпуляцій та стратегічні комунікації
5.	Громадсько-експертна	Інститути громадянського суспільства	Демократичний контроль	Незалежний моніторинг, фактчекінг та забезпечення прозорості безпекових процедур

Джерело: складено автором на основі аналізу [25; 47; 128; 143–166].

Стратегічно-координаційна підсистема виступає центральною ланкою адміністративно-правового механізму забезпечення інформаційної безпеки України. Її ключове призначення полягає у формуванні політико-правових рамок, визначенні державних пріоритетів у сфері інформаційної безпеки та забезпеченні узгодженої міжвідомчої взаємодії на національному рівні. На відміну від інших підсистем, які виконують спеціалізовані (оперативні, контрольно-аналітичні або гуманітарно-комунікаційні) функції, саме

стратегічно-координаційна підсистема визначає загальні «правила гри» та задає вектор розвитку всієї системи забезпечення інформаційної безпеки.

Ключові суб'єкти: Президент України; РНБО (ЦПД); КМУ; ВРУ.

Операційно-виконавча підсистема становить практичний рівень адміністративно-правового механізму забезпечення інформаційної безпеки України, у межах якого реалізуються конкретні заходи з виявлення, документування та нейтралізації деструктивних форм зовнішнього впливу на інформаційні процеси та управлінські рішення. Її діяльність має чітко виражений прикладний характер і спрямована на реагування на загрози в режимі реального часу з використанням спеціальних правових і технічних інструментів.

Ключові суб'єкти: СБУ; НПУ; Держспецзв'язку.

Контрольно-аналітична підсистема поєднує превентивні та наглядові механізми, спрямовані на мінімізацію ризиків зовнішнього впливу шляхом застосування фінансових, правових, фіскальних і кадрових інструментів. Її специфіка полягає в інтеграції органів, що належать до різних сфер державного управління (антикорупційної, фінансово-економічної, податкової, реєстраційно-правової), однак у сукупності формують цілісну систему аналізу потенційних ризиків та виявлення прихованих форм впливу на процеси публічного управління.

Ключові суб'єкти: НАЗК; НБУ; НАДС, НКЕК, ДПС та ДМС; Держфінмоніторинг; Мін'юст.

Гуманітарно-комунікаційна підсистема забезпечення інформаційної безпеки України є стратегічним елементом формування стійкості суспільства до зовнішніх та внутрішніх деструктивних інформаційних впливів. Її принципова відмінність від операційно-виконавчих і контрольно-аналітичних механізмів полягає у випереджувальному характері діяльності: вона не лише реагує на вже наявні загрози, а формує умови для несприйнятливості суспільства до маніпуляцій, дезінформації та нав'язування викривлених наративів. У цьому сенсі гуманітарно-комунікаційна підсистема виконує функцію «інформаційного імунітету» держави.

Ключові суб’єкти: Мінкультури; МОН; Мінцифри; Нацрада; ЦПД.

Громадсько-експертна підсистема у структурі забезпечення інформаційної безпеки України відіграє роль механізму демократичного балансу, забезпечуючи взаємодію державних інституцій з ІГС. Вона формує незалежний моніторинг, аналітичний супровід і громадський контроль за інформаційними процесами, створюючи додатковий рівень суспільної стійкості до зовнішніх впливів.

Ключові суб’єкти:

громадяни України, які відповідно до Стратегії інформаційної безпеки визнаються активними суб’єктами захисту [25], а не лише об’єктами інформаційних впливів;

громадські організації – реалізують моніторингові, освітні та адвокаційні ініціативи;

аналітичні центри – здійснюють незалежні дослідження та експертну оцінку ризиків;

незалежні медіа та фактчек-проєкти – забезпечують перевірку достовірності інформації та викриття маніпулятивних практик;

професійні асоціації, бізнес-об’єднання та академічні спільноти – сприяють формуванню стандартів інформаційної етики та саморегуляції у сфері комунікацій [100].

Необхідно зазначити, що міжвідомча взаємодія та координація діяльності у сфері забезпечення інформаційної безпеки України в аспекті протидії зовнішньому впливу істотно ускладнюється внаслідок фрагментації управлінських рішень, розірваності горизонтальних комунікацій між суб’єктами публічного управління та відсутності єдиного центру аналітичної консолідації даних. За таких умов наявні контрольні, наглядові та інформаційно-аналітичні інструменти функціонують ізольовано, що унеможливлює формування цілісної управлінської оцінки ризиків зовнішнього впливу та своєчасне реагування на них.

У зв’язку з цим обґрунтовано постає потреба у формуванні постійно діючої міжвідомчої структури – Центру протидії зовнішньому впливу (далі – ЦПЗВ), який пропонується як ЦОВВ зі спеціальним статусом. Такий Центр має

виконувати роль інституційного ядра координації, аналітики та інтеграції інформаційних потоків між усіма функціональними підсистемами забезпечення інформаційної безпеки.

Діяльність ЦПЗВ має бути спрямована не на заміщення повноважень існуючих ЦОВВ, а на забезпечення їх процедурної узгодженості, синхронізації управлінських рішень та підвищення загальної керованості системи.

На відміну від ЦПД при РНБО, діяльність якого зосереджена переважно на моніторингу інформаційного контенту, ЦПЗВ фокусується на ідентифікації латентних каналів зовнішнього впливу на суб'єктів підготовки та ухвалення управлінських рішень.

У межах функціонування Центру доцільним є:

запровадження єдиної цифрової платформи міжвідомчого обміну даними – Системи інтегрованого моніторингу афілійованості (далі – СІМА), що забезпечить раннє виявлення ознак зовнішнього впливу та підвищить ефективність інформаційної взаємодії між суб'єктами державного управління, місцевого самоврядування та інститутами громадянського суспільства;

розвиток прозорої системи звітності, механізмів громадського контролю та інструментів публічної комунікації, спрямованих на підвищення довіри до державної політики у сфері інформаційної безпеки та забезпечення балансу між безпековими потребами й демократичними стандартами відкритості та свободи слова.

Таким чином, створення Центру у поєднанні з цифровою інтеграцією, інституційною координацією та чітко визначеними механізмами підзвітності формує системну основу для модернізації адміністративно-правового механізму забезпечення інформаційної безпеки України в умовах гібридних загроз та зростаючого зовнішнього впливу на публічне управління.

2.3. Досвід іноземних держав у протидії зовнішньому впливу на публічне управління та можливості його адаптації в Україні

У сучасних умовах гібридної агресії та зростаючої взаємопов'язаності глобальних політичних і економічних процесів протидія зовнішньому впливу на публічне управління набуває системного характеру та виходить за межі вузькоінтерпретованих безпекових підходів. У центрі уваги держав опиняється не лише діяльність окремих осіб чи організацій, а насамперед стійкість управлінських процесів, автономія прийняття управлінських рішень і захищеність інституцій влади від прихованого або непрямого втручання з боку зовнішніх суб'єктів.

Зарубіжний досвід свідчить, що правові механізми протидії зовнішньому впливу формуються у різних концептуальних площинах: від реєстраційно-прозорих моделей, орієнтованих на забезпечення відкритості взаємодії з іноземними суб'єктами, до комплексних інституційних підходів, спрямованих на захист процесів формування та реалізації державної політики. При цьому діяльність так званих «іноземних агентів» розглядається не як самодостатній об'єкт регулювання, а як один із можливих каналів реалізації зовнішнього впливу, поряд із фінансовими, інформаційними, кадровими та лобістськими механізмами.

Характерною рисою демократичних правопорядків є фокус на управлінському вимірі безпеки, що проявляється у нормативному розмежуванні допустимих і недопустимих форм участі іноземних суб'єктів у публічних процесах, посиленні вимог до прозорості прийняття рішень, а також у створенні спеціалізованих інституцій координації та аналітичного супроводу. Натомість авторитарні та квазі-демократичні моделі демонструють тенденцію до використання законодавства про «іноземний вплив» як інструменту політичного контролю, що призводить до звуження простору публічного управління та ерозії демократичних інститутів.

З огляду на це, аналіз зарубіжного досвіду протидії зовнішньому впливу доцільно здійснювати не за формальною ознакою наявності або відсутності реєстраційних інститутів, а через призму захисту управлінської автономії держави, ефективності міжвідомчої координації та здатності публічної влади виявляти і нейтралізувати комплексні впливи на ранніх стадіях. Такий підхід дозволяє виявити структурні переваги й обмеження різних моделей, а також сформувати підґрунтя для обґрунтування власної адміністративно-правової конструкції протидії зовнішньому впливу на публічне управління в Україні.

У цьому контексті особливого значення набуває питання інституційної інтеграції інформаційно-аналітичних, контрольних і координаційних функцій, що в подальшому обґрунтовує доцільність формування спеціалізованого центру міжвідомчої взаємодії як елементу модернізованого адміністративно-правового механізму забезпечення інформаційної безпеки та стійкості публічного управління.

Дослідження зарубіжного досвіду доцільно розпочати з аналізу підходів Сполучених Штатів Америки (далі – США) до протидії зовнішньому впливу, оскільки саме в цій державі сформовано одну з найбільш розроблених і концептуально цілісних моделей правового регулювання прозорості іноземного лобізму та політичної діяльності. Ключовим елементом такої моделі є Закон про реєстрацію іноземних агентів – Foreign Agents Registration Act (далі – FARA).

FARA був ухвалений у 1938 році як реакція на активізацію пропагандистської діяльності нацистської Німеччини напередодні Другої світової війни. У подальшому закон неодноразово зазнавав змін, серед яких найбільш суттєвими стали поправки 1966, 1995 та 2007 років, унаслідок чого він набув сучасної конфігурації та перетворився на інструмент забезпечення прозорості політичного лобізму іноземних інтересів [167]. Саме реформа 1966 року стала переломною, оскільки зумовила зміщення акценту з боротьби з політичною пропагандою на регулювання лобістської та консультаційної діяльності в інтересах іноземних суб’єктів.

Відповідно до положень FARA, фізичні та юридичні особи (включно з громадянами США), які діють в інтересах іноземних урядів, політичних партій, організацій, компаній або приватних осіб (так званих «іноземних принципалів») та здійснюють таку діяльність за їх дорученням, на прохання або під керівництвом, зобов'язані пройти реєстрацію в Міністерстві юстиції США. Окрім цього, вони повинні кожні шість місяців подавати детальні звіти щодо отриманих коштів і понесених витрат незалежно від джерела фінансування – державного чи недержавного [168].

У контексті доктринального аналізу важливо підкреслити, що даний термін не обмежується лише юридичним замовником послуг, а охоплює будь-яку особу чи організацію, що є реальним бенефіціаром (вигодоодержувачем) відповідної діяльності. Саме такий зміст вкладається у категорію «іноземний суб'єкт», що детально проаналізована у підрозділі 1.3 даного дослідження.

Саме через таку широку інтерпретацію суб'єктного складу, сфера дії FARA охоплює політичну діяльність, інформаційні та консультаційні послуги, політичний і публічний лобізм, збір і розподіл фінансових ресурсів, а також представлення інтересів іноземного принципала перед органами державної влади, посадовими особами або членами Конгресу США. Під час реєстрації особа (агент) зобов'язана надати вичерпну інформацію про іноземного суб'єкта (принципала), його структуру власності, характер і зміст діяльності, отримані кошти та напрями їх використання, а також про інформаційні матеріали, що розповсюджуються в межах відповідної активності.

Окремою вимогою FARA є маркування так званих «інформаційних матеріалів», які повинні супроводжуватися чітким зазначенням, що вони розповсюджуються від імені іноземного суб'єкта. Копії таких матеріалів підлягають обов'язковому поданню до Міністерства юстиції США.

Водночас дія FARA не поширюється на неполітичний лобізм та пропаганду в широкому сенсі. Комерційна, культурна, наукова та релігійна діяльність, а також збір пожертвувань не вимагають реєстрації. Поза межами

регулювання також перебувають офіційні представники іноземних держав, зокрема дипломатичні агенти [169].

Паралельно з механізмом FARA у США функціонує кримінально-правовий інструмент протидії прихованому зовнішньому впливу – 18 U.S.C. § 951, який забороняє здійснювати діяльність в якості агента іноземного уряду на території США без попереднього повідомлення Генерального прокурора. Порушення цієї норми тягне за собою кримінальну відповідальність у вигляді позбавлення волі строком до десяти років або накладення штрафу. На відміну від FARA, § 951 охоплює будь-які форми діяльності – як політичні, так і неполітичні – за умови здійснення їх під керівництвом або на замовлення іноземного уряду чи посадовця [169; 170].

Порівняльна характеристика FARA та § 951 дозволяє дійти висновку, що американська модель базується на подвійному режимі правового регулювання: з одного боку – адміністративно-прозорому механізмі реєстрації та публічного контролю, з іншого – кримінально-правовому реагуванні на приховану агентурну діяльність державного рівня. Попри відносно нечасте застосування цих норм (лише кілька десятків кримінальних справ за всю історію), вони формують чітке нормативне розмежування між допустимими та недопустимими формами іноземного впливу [171, с. 51]. Водночас вузьке тлумачення політичної діяльності у FARA та високий стандарт доказування наміру можуть створювати прогалини у протидії сучасним гібридним формам втручання.

Подібну логіку інституціоналізації прозорості зовнішнього впливу було реалізовано і в Австралійському Союзі. У 2018 році там набув чинності Закон про програму прозорості іноземного впливу – Foreign Influence Transparency Scheme Act (далі – FITS), який запровадив комплексний реєстраційний механізм для осіб, що здійснюють діяльність в інтересах іноземних суб’єктів з метою впливу на політичні процеси, урядові рішення або суспільну думку [172].

Згідно з FITS, агентом іноземного впливу визнається будь-яка фізична чи юридична особа, яка прямо або опосередковано діє в інтересах іноземного принципала з політичними чи урядовими цілями. Обов’язок реєстрації залежить

від трьох ключових критеріїв: статусу іноземного принципала, характеру діяльності (лобіювання, комунікація, матеріальна підтримка) та форми взаємовідносин між агентом і іноземним суб'єктом [171, с. 52; 173].

Зареєстровані особи зобов'язані розкривати відомості про характер своїх відносин з іноземними структурами, мету та зміст діяльності, а також повідомляти про всі суттєві зміни. Частина цієї інформації оприлюднюється у публічному реєстрі, що забезпечує доступ парламенту та громадськості до відомостей про зовнішній вплив. Реєстрація має строковий характер (один рік) і підлягає обов'язковому поновленню; порушення вимог може призвести до автоматичного анулювання та застосування санкцій, включно з позбавленням волі строком до трьох років [174].

Водночас австралійська модель зазнала обґрунтованої критики, зокрема через надмірну бюрократизацію процедур, обмежену ефективність правозастосування в перші роки дії закону, вузьке тлумачення окремих ключових понять, а також значне регуляторне навантаження на осіб, які раніше обіймали публічні посади [173]. У зв'язку з цим парламентські комітети Австралійського Союзу рекомендували перегляд FITS у напрямі розширення поняття «іноземного принципала», спрощення адміністративних процедур та впровадження диференційованого підходу до контролю за впливом з боку авторитарних держав [173].

Таким чином, досвід США та Австралії демонструє еволюцію правових механізмів протидії зовнішньому впливу від суто реєстраційних моделей до комплексних адміністративно-правових конструкцій, орієнтованих на захист автономії публічного управління. Водночас ці моделі виявляють об'єктивні межі ефективності традиційних інструментів у контексті гібридних і цифрових форм втручання, що актуалізує потребу в подальшому інституційному та нормативному розвитку таких механізмів.

У 2023 році у Сполученому Королівстві Великої Британії та Північної Ірландії (далі – Сполучене Королівство) було ухвалено Закон про національну безпеку (National Security Act, 2023), який заклав правові підвалини нового

інструменту протидії зовнішньому впливу – Foreign Influence Registration Scheme (далі – FIRS). Запровадження цього механізму стало складовою ширшої стратегії національної безпеки держави, спрямованої на реагування на зростання гібридних загроз та системні спроби втручання іноземних держав у політичні й суспільні процеси [175].

Метою FIRS є формування системи прозорого обліку, контролю та запобігання прихованій діяльності, що здійснюється в інтересах іноземних держав, шляхом запровадження обов'язкової реєстрації відповідної активності фізичних і юридичних осіб [175]. На відміну від класичних реєстраційних моделей, британський підхід орієнтований не лише на публічність, а й на раннє виявлення ризикових впливів, пов'язаних із діяльністю державних і квазідержавних іноземних акторів.

Механізм FIRS передбачає два рівні реєстрації, диференційовані за ступенем загрози та характером іноземного впливу:

1. Political influence tier – застосовується до суб'єктів, які виконують завдання або здійснюють діяльність в інтересах іноземної держави з метою впливу на політичні процеси, прийняття рішень або формування громадської думки. Реєстрація в межах цього рівня є публічною, а відповідна інформація вноситься до відкритого державного реєстру. Невиконання вимог щодо реєстрації або подання недостовірних даних тягне за собою кримінальну відповідальність [176].

2. Enhanced tier – охоплює діяльність, що координується іноземними державами або підконтрольними їм структурами, віднесеними до спеціального «списку ризикових». Станом на момент ухвалення закону до такого переліку були включені російська федерація та Ісламська Республіка Іран. У межах цього режиму реєстрація має бути здійснена не пізніше ніж протягом десяти днів з моменту укладення відповідної угоди або фактичного початку співпраці [177].

Водночас британська модель не позбавлена дискусійних аспектів. Зокрема, у «списку ризикових» держав відсутній Китай, що в наукових і політичних колах пов'язують із економічними та торговельними інтересами Сполученого

Королівства. Крім того, механізм FIRS передбачає винятки для окремих категорій організацій, зокрема релігійних, що потенційно може створювати можливості для зловживань і використання таких винятків у межах гібридних операцій [178].

До сильних сторін британської моделі слід віднести наявність публічного державного реєстру, чітко визначені часові межі реєстраційних зобов'язань, а також поширення режиму контролю не лише на політичні структури, а й на дослідницькі інституції, університети та громадські організації. Окремої уваги заслуговує висока швидкість реагування на потенційні загрози, що забезпечується диференційованою системою ризик-орієнтованого контролю.

Загалом британський підхід демонструє прагматичну модель регулювання іноземного впливу, яка поєднує елементи прозорості та гнучкості. Водночас ефективність FIRS значною мірою залежатиме від стабільності політичної волі, послідовності правозастосування та здатності Сполученого Королівства своєчасно переглядати винятки й перелік ризикових держав з урахуванням еволюції гібридних загроз.

Окремої уваги заслуговує досвід Канади, яка у відповідь на підтверджені випадки втручання у федеральні вибори 2019–2021 рр. (зокрема з боку Китайської Народної Республіки (далі – КНР)) ухвалила у 2024 році комплексний Countering Foreign Interference Act (Bill C-70). Ключовою складовою акта став Foreign Influence Transparency and Accountability Act (далі – FITAA), що запровадив загальнодоступний реєстр іноземного впливу.

Відповідно до FITAA, будь-яка фізична або юридична особа, яка вступає у домовленість (arrangement) з іноземним суб'єктом – «foreign principal» (іноземним замовником/принципалом), зобов'язана протягом 14 днів повідомити про це Комісара з питань прозорості іноземного впливу та розкрити характер і мету взаємодії. Комісар призначається Кабінетом міністрів, а реєстр є публічним. За порушення передбачено як кримінальну відповідальність, так і фінансові санкції до 5 млн канадських доларів [179].

До сильних сторін такої моделі можна віднести високий рівень прозорості, охоплення як фізичних, так і юридичних осіб, акцент на захист виборчого процесу та медіапростору.

В свою чергу до слабких сторін моделі можна віднести відсутність швидких процедурних механізмів для оперативного реагування на нові загрози. Також, у експертного середовища існують сумніви щодо незалежності Комісії [179].

Канадська модель є орієнтованою на публічну прозорість та запобігання прихованому впливу, однак потребує інституційного посилення у сфері швидкого реагування на гібридні загрози та гарантій незалежності органу-реєстратора.

Однією з перших європейських держав, що здійснила спробу нормативного регулювання іноземного впливу на громадянський сектор, стала Угорщина. У червні 2017 року парламентом країни було ухвалено Закон «Про прозорість організацій, що отримують фінансування з іноземних джерел», відповідно до якого неурядові організації, які отримували щонайменше 7,2 млн форинтів на рік (приблизно 24 тис. євро) з іноземних джерел, підлягали обов’язковій спеціальній реєстрації як «організації, що отримують іноземне фінансування» [180].

Закон передбачав низку додаткових зобов’язань, зокрема вимогу публічно зазначати факт іноземного фінансування у всіх комунікаційних матеріалах, публікаціях та заходах, а також щорічно подавати розширені фінансові звіти. Санкцією за невиконання вимог могла бути примусова ліквідація організації.

Практика застосування закону виявилася проблемною. Попри те, що формально під його дію підпадали близько 152 неурядові організації (далі – НУО), більшість із понад 60 тисяч зареєстрованих громадських організацій відмовилися виконувати вимоги, посилаючись на правову невизначеність процедур ліквідації, а також на потужний суспільний і міжнародний спротив. Закон викликав масштабну критику з боку інституцій Європейського Союзу та правозахисних організацій [171, с. 52].

У 2020 році Суд ЄС визнав закон таким, що порушує свободу об'єднань, принципи пропорційності та основоположні засади європейського права. Унаслідок цього в 2021 році Угорщина формально скасувала зазначений акт, водночас зберігши елементи контролю за «іноземним втручанням» у межах інших нормативних інструментів [181].

Новий етап еволюції угорської моделі розпочався у 2023 році з ухвалення Закону «Про захист національного суверенітету», яким було створено Управління захисту суверенітету (Sovereignty Protection Office, (далі – SPO)). Цей орган отримав широкі повноваження щодо виявлення та розслідування впливу іноземного фінансування на політичні процеси, включно з можливістю ініціювати перевірки без судового дозволу, вести облік осіб і організацій, а також здійснювати вплив на діяльність медіа, політичних партій і неурядових структур [182].

Попри офіційне позиціонування SPO як інструменту національної безпеки, його створення спричинило гостру критику з боку європейських інституцій, правозахисних і журналістських організацій. Основними зауваженнями стали відсутність прозорих процедур, розмитість критеріїв визначення «загроз суверенітету», ризики позасудового втручання та концептуальна подібність до моделей, що застосовуються в авторитарних державах. У цьому контексті SPO дедалі частіше розглядається як інструмент політичного контролю, замаскований під безпекову риторику.

Протягом 2024–2025 років правляча партія «Фідес» здійснила чергову спробу посилення контролю за іноземним фінансуванням. За результатами парламентських дебатів наприкінці 2025 року було остаточно закріплено розширені повноваження SPO, що дозволило йому здійснювати моніторинг фінансових потоків НУО з вищими штрафними санкціями. Попри триваюче провадження у Суді ЄС щодо порушення Угорщиною норм європейського права, створений механізм продовжує функціонувати як інструмент жорсткого адміністративного тиску на суб'єктів, що отримують зовнішню підтримку [183].

У цілому угорська модель регулювання іноземного впливу характеризується жорстким, формалізованим і переважно репресивним підходом, ключовими ознаками якого є:

нав’язування обов’язкової реєстрації та публічного маркування НУО;

розширення повноважень виконавчої влади без ефективного судового контролю;

невизначеність критеріїв «загроз суверенітету»;

використання кримінально-правових механізмів у сфері політичного фінансування.

Відсутність чітких і пропорційних процедур, а також домінування каральної логіки призводять до делегітимації цієї моделі як усередині держави, так і на міжнародному рівні. Кейс Угорщини переконливо демонструє, що порушення балансу між протидією іноземному впливу та захистом демократичних прав і свобод здатне трансформувати безпекові інструменти у засоби політичного тиску.

Певним контрастом до угорського підходу є польський кейс, який ілюструє точкове регулювання іноземного впливу у такій стратегічно чутливій сфері, як медіа. 11 серпня 2021 року Сеймом Республіки Польща були ухвалені поправки до Закону про телерадіомовлення, якими встановлювалося обмеження іноземної участі у власності телерадіокомпаній до 49%, за винятком інвесторів із країн Європейського економічного простору [184].

Законопроєкт також забороняв опосередкований контроль над ліцензіатами з боку суб’єктів, головний офіс яких розташований за межами Європейської економічної зони, що фактично ставило під загрозу діяльність низки медіа, зокрема телеканалу TVN24, який належить американській компанії Discovery. Це спричинило значний внутрішньополітичний резонанс і напруження у відносинах Польщі зі США.

Хоча 9 вересня 2021 року Сенат Польщі відхилив зазначені поправки, сам факт їх ухвалення нижньою палатою парламенту (228 голосів «за» проти 216 «проти»)

засвідчив наявність тенденції до використання регуляторних механізмів у сфері медіа як інструменту впливу на інформаційний простір [185].

Польський приклад демонструє, що навіть вузьконаправлені обмеження, орієнтовані на контроль власності та фінансування, можуть викликати серйозні застереження з погляду свободи слова та політичної нейтральності. Селективний характер регулювання та його спрямованість на конкретний медіа-холдинг породили звинувачення у прихованій цензурі, що ще раз підтверджує: ефективність моделей протидії іноземному впливу визначається не лише нормативною формою, а й контекстом, пропорційністю та прозорістю їх імплементації.

Литва є прикладом пострадянської держави, яка послідовно сформувала комплексну систему запобігання зовнішньому впливу без запровадження спеціальних реєстраційних статусів. Її модель базується на поєднанні контррозвідувальних, нормативних та комунікаційних інструментів і орієнтована насамперед на нейтралізацію гібридних загроз, пов’язаних із дезінформацією, іноземним фінансуванням і впливом на політичне середовище.

Інституційною основою цієї моделі є діяльність Департаменту державної безпеки, який здійснює контррозвідувальний моніторинг і щорічно оприлюднює звіти про загрози національній безпеці. Особливістю литовського підходу є публічне називання конкретних організацій та осіб, пов’язаних з іноземним впливом, що виконує функцію суспільного маркування ризиків без формального надання юридичного статусу. Водночас законодавство Литви передбачає жорсткий контроль за фінансуванням політичних партій, включно з повною забороною іноземного фінансування [186].

Важливим елементом системи є протидія інформаційним операціям. Литва застосовує обмеження на трансляцію іноземних медіа, що поширюють дезінформацію або наративи держав-агресорів, розвиває державні програми з медіаграмотності та запроваджує санкції щодо ЗМІ за систематичне поширення недостовірної інформації. У 2023 році було також посилено вимоги до

політичних партій і кандидатів щодо декларування контактів з іноземними організаціями та фондами, здатними впливати на політичні процеси [187].

Таким чином, литовська модель є прикладом інтегрованого інституційного реагування, у якому превентивні та розвідувальні механізми поєднуються з публічною комунікацією загроз. Її обмеженням є відсутність єдиного реєстру або нормативно закріпленого поняття агента іноземного впливу, що ускладнює правозастосовну ідентифікацію суб'єктів. Для України цей досвід є цінним як альтернатива жорсткому реєстраційному режиму, особливо з огляду на баланс між свободою слова та інформаційною безпекою.

Фінляндія демонструє модель протидії зовнішньому впливу, що ґрунтується не на спеціальному реєстраційному законодавстві, а на розвиненій системі прозорості, відкритості публічної влади та саморегуляції. Такий підхід орієнтований на мінімізацію непрозорого впливу через структурну підзвітність і залучення громадянського суспільства.

Нормативною основою цієї моделі є Закон «Про відкритість у діяльності органів влади», який гарантує доступ до публічної інформації та документів, що створює передумови для постійного суспільного контролю за діяльністю посадовців [188]. У 2024 році Фінляндія додатково запровадила Національний реєстр прозорості, який охоплює лобістську діяльність у взаємодії з міністрами, парламентарями та вищими посадовими особами. Реєстр передбачає обов'язок розкриття інформації про мету, характер і фінансування впливу, у тому числі іноземного походження [189].

Суттєву роль відіграє система медіа-саморегулювання, що функціонує через незалежну Раду з масових комунікацій. Вона здійснює нагляд за дотриманням журналістських стандартів і розглядає випадки прихованого або маніпулятивного впливу, не вдаючись до прямого державного втручання [190]. Додатковим чинником стійкості є високий рівень медіаграмотності населення, який формується через інтеграцію медіаосвіти в навчальні програми та реалізацію державних і громадських ініціатив з цифрової безпеки [191].

Фінська модель забезпечує високу ефективність запобігання непрозорому впливу в умовах стабільного демократичного середовища. Водночас її обмеження проявляються у ситуаціях високої інтенсивності гібридних загроз або збройного конфлікту, коли відсутність жорстких правових запобіжників може бути недостатньою для нейтралізації організованого прихованого втручання. Для України цей досвід є важливим як еталон демократичного.

Франція сформувала одну з найбільш інституційно розвинених моделей протидії іноземному впливу в Європі, яка базується на класифікації загроз національній безпеці, а не на публічному маркуванні суб'єктів як «агентів». Такий підхід поєднує правові, аналітичні та оперативні інструменти з акцентом на захист демократичних інститутів і виборчих процесів.

У 2021 році було ухвалено закон про боротьбу з іноземним втручанням, який криміналізує непрозору фінансову підтримку політичної діяльності, тиск на посадовців і медіа, а також дезінформаційні та кібероперації. Законодавство передбачає ведення реєстру активностей іноземного впливу, можливість заморожування активів і використання цифрових технологій для виявлення втручання у політичні процеси [192].

Ключовим елементом французької моделі є міжвідомча координація, що охоплює органи внутрішньої безпеки, юстиції, закордонних справ і цифрового захисту. Особливу роль відіграє створене у 2021 році агентство Viginum (Service de vigilance et de protection contre les ingérences numériques étrangères), яке спеціалізується на виявленні та нейтралізації іноземних цифрових кампаній впливу, включно з використанням бот-мереж і таргетованої дезінформації [193]. Додатково Франція впровадила спеціальні заходи кіберзахисту виборчих процесів у співпраці з виборчими органами та агентством ANSSI (Agence nationale de la sécurité des systèmes d'information) [194].

Французька модель вирізняється збереженням балансу між безпековими цілями та свободою громадянського суспільства. Контроль зосереджено на зв'язках із іноземними урядами та ризик-орієнтованому аналізі, а не на самому факті іноземного фінансування. Це дозволяє уникнути стигматизації

неурядового сектору та забезпечити захист прав людини через судовий нагляд і процедурні гарантії.

Одним із найбільш відомих і водночас негативних прикладів законодавчого регулювання зовнішнього впливу є досвід російської федерації (далі – рф). Попри задекларовану мету забезпечення прозорості зовнішнього впливу, відповідна нормативна модель фактично еволюціонувала у систему політичного контролю та придушення інакомислення, яка у період з 2012 по 2025 роки набула ознак тотального нагляду за громадянським суспільством.

Початковий етап формування цієї моделі пов’язаний з ухваленням у 2012 році першої редакції закону, який зобов’язував неурядові організації, що отримують фінансування з-за кордону та беруть участь у так званій «політичній діяльності», реєструватися як «іноагенти». При цьому поняття політичної діяльності тлумачилося вкрай широко і охоплювало фактично будь-яку публічну активність, спрямовану на формування громадської думки щодо рішень органів влади [171, с. 53].

У 2017–2020 роках сфера дії закону була розширена на ЗМІ, включно з представництвами міжнародних медіа. Для них було запроваджено обов’язкове маркування матеріалів, розширену фінансову звітність та регулярні аудиторські перевірки, що істотно ускладнило їхню діяльність [195].

Подальша трансформація у 2020–2022 роках призвела до включення до кола «іноагентів» фізичних осіб. Вперше було закріплено можливість визнання особи агентом іноземного впливу навіть за відсутності прямого фінансування, на підставі розмитих критеріїв «поширення думок» або «впливу на громадську думку». Це дозволило включати до реєстру журналістів, науковців, правозахисників і адвокатів без чітких доказів або судового рішення [196].

Завершальним етапом стала кодифікація у 2022–2025 роках, коли було ліквідовано будь-яке розмежування між типами суб’єктів (НУО, ЗМІ, фізичні особи) та запроваджено єдиний централізований Реєстр іноземних агентів, що ведеться міністерством юстиції рф. Законодавство передбачило розгалужену систему адміністративної та кримінальної відповідальності, включно з обмеженням доступу

до освіти, забороною участі у виборах, публічних заходах, отриманні державного фінансування та обов'язковим маркуванням усіх інформаційних матеріалів, зокрема в соціальних мережах [197].

Реалізація російської моделі призвела до низки системних наслідків. По-перше, поняття «іноагент» було навмисно перетворене на стигматизуюче тавро, що делегітимізує будь-яку незалежну від держави публічну діяльність. По-друге, процедура внесення до реєстру має несудовий характер, що унеможливлює ефективний захист прав і оскарження відповідних рішень. По-третє, включення до реєстру фактично означає заборону повноцінної участі у професійному, науковому, освітньому та політичному житті.

Окремо слід відзначити використання так званого «дзеркального аргументу», коли російська влада обґрунтовує відповідне законодавство як відповідь на дії США чи інших держав щодо іноземних медіа [197]. Водночас за своїм змістом і наслідками російська модель є значно більш репресивною та несумісною з демократичними стандартами.

Кейс рф наочно демонструє, як механізм протидії іноземному впливу може трансформуватися у інструмент системного придушення громадянських свобод. Нечіткі критерії, довільне трактування поняття «впливу», відсутність судового контролю та каральна логіка законодавства створили умови, за яких сам факт участі у публічному житті стає потенційно криміналізованим.

Для України цей досвід має значення виключно як антиприклад, що підкреслює принципову необхідність спирання на верховенство права, пропорційність втручання, недискримінаційність та ефективний судовий контроль.

Проведений порівняльно-правовий аналіз міжнародних моделей протидії зовнішньому впливу на публічне управління засвідчує відсутність універсального нормативного підходу, придатного для прямого або механічного імплементування в український правопорядок. Практика різних держав демонструє широкий спектр інструментів – від реєстраційних і прозорих механізмів до інституційно-безпекових та репресивних моделей, ефективність

яких істотно залежить від політичного режиму, рівня правової культури та характеру безпекових загроз.

З метою узагальнення виявлених підходів та забезпечення їх системного порівняння, у таблиці 2.3.1 здійснено класифікацію основних моделей протидії зовнішньому впливу на публічне управління з урахуванням їх концептуальної спрямованості, інституційних механізмів та використовуваного інструментарію. Така систематизація дозволяє виокремити функціональні відмінності між реєстраційними, інституційно-аналітичними, превентивними та репресивними моделями і створює підґрунтя для подальшого обґрунтування можливостей їх адаптації до українського правопорядку.

Таблиця 2.3.1

Класифікація моделей протидії зовнішньому впливу в публічному управлінні

№ з/п	Тип моделі	Загальна характеристика	Приклади держав	Ключові інструменти
1.	Реєстраційна	Орієнтація на прозорість та підзвітність діяльності, пов'язаної з іноземним впливом	США, Канада, Австралійський Союз, Сполучене Королівство	Реєстри, декларування, маркування, звітність
2.	Інституційно-аналітична	Превентивний моніторинг та міжвідомча координація у сфері безпеки	Франція, Литва	Аналітичні центри, контррозвідувальні заходи, цифрова безпека
3.	Культурно-превентивна	Формування стійкості суспільства до зовнішнього впливу	Фінляндія	Медіаграмотність, саморегуляція, прозорість лобізму
4.	Репресивна	Адміністративно-каральні механізми з елементами стигматизації	рф, Угорщина	Заборони, санкції, обмеження діяльності організацій, криміналізація фінансування

Джерело: складено автором на основі аналізу [167–197].

Демократичні правові системи (США, Канада, Сполучене Королівство, Австралійський Союз, Франція, Литва, Фінляндія,) загалом орієнтуються на превенцію прихованого впливу, забезпечення прозорості взаємодії з іноземними

суб’єктами та захист виборчих і комунікаційних процесів. У межах цієї групи умовно виокремлюються такі основні підходи:

реєстраційні моделі (США, Канада, Сполучене Королівство, Австралійський Союз), що фокусуються на декларуванні та публічному обліку впливу;

інституційно-аналітичні підходи (Франція, Литва), зорієнтовані на міжвідомчу координацію, контррозвідувальне забезпечення та цифрову безпеку;

культурно-превентивні моделі (Фінляндія), які ґрунтуються на відкритості, саморегуляції та розвитку медіаграмотності.

У контексті розбудови вітчизняного адміністративно-правового механізму протидії зовнішньому впливу найбільш релевантним для адаптації видається досвід Французької Республіки, зокрема діяльність спеціалізованого агентства Viginum, модель якого орієнтована не на пасивну реєстрацію суб’єктів, а на техніко-аналітичне виявлення інформаційного втручання у режимі реального часу. На відміну від класичних реєстрових підходів, французька система акцентує увагу на превентивному моніторингу, міжвідомчій координації та аналітичній оцінці загроз.

Водночас перспективним з погляду інституційного дизайну є поєднання зазначеної стратегії технологічного виявлення з британською моделлю ризик-орієнтованої диференціації режимів реєстрації, що дозволяє забезпечити пропорційність державного втручання залежно від рівня потенційного зовнішнього впливу. Саме така комбінація може розглядатися як концептуальна основа для формування в Україні спеціалізованого Центру протидії зовнішньому впливу, діяльність якого поєднувала б аналітичну ефективність із належними процедурними гарантіями.

Висновки до розділу 2

У другому розділі дисертаційного дослідження на основі комплексного аналізу сучасної вітчизняної практики та зарубіжного досвіду розкрито стан і проблеми адміністративно-правового механізму забезпечення інформаційної безпеки України в аспекті протидії зовнішньому впливу на публічне управління, а також окреслено ключові напрями його подальшого розвитку.

1. Здійснено аналіз сучасного стану нормативно-правового блоку адміністративно-правового механізму забезпечення інформаційної безпеки України. Встановлено, що, попри наявність розгалуженого масиву законодавчих і стратегічних актів, чинна система залишається фрагментованою та концептуально незавершеною саме в частині протидії зовнішньому впливу на публічне управління. Встановлено, що суттєвими стримувальними чинниками ефективності правового регулювання є: втрата актуальності окремих нормативно-правових актів; відсутність законодавчо закріплених дефініцій понять «зовнішній вплив», «іноземний суб'єкт», «афілійований суб'єкт»; брак спеціальних реєстраційних, наглядових і контрольних механізмів щодо діяльності потенційних суб'єктів зовнішнього впливу.

Розкрито еволюцію нормативних ініціатив у цій сфері, яка характеризується коливанням між надмірно жорсткими, репресивними підходами, що не витримували суспільного та міжнародного тиску, і декларативними проєктами, позбавленими реальних механізмів імплементації. Доведено, що відсутність системного спеціального закону зумовлює нормативну невизначеність, підвищує ризики політизації та унеможливлює формування прозорої й підконтрольної державі системи протидії зовнішньому впливу. У зв'язку з цим обґрунтовано необхідність створення чітких правових рамок шляхом ухвалення спеціального закону «Про протидію зовнішньому впливу на публічне управління».

2. Аналіз інституційно-координаційного блоку адміністративно-правового механізму забезпечення інформаційної безпеки України показав, що чинна система

суб’єктів, закріплена у стратегічних та нормативно-правових документах, не відзначається достатньою узгодженістю та повною відповідністю сучасній архітектурі загроз. Виявлено наявність застарілих підходів до визначення суб’єктного складу, зокрема у документах, ухвалених до початку повномасштабної збройної агресії російської федерації проти України.

У межах функціонального підходу систему суб’єктів забезпечення інформаційної безпеки в аспекті протидії зовнішньому впливу на публічне управління структуровано у п’ять взаємопов’язаних підсистем: стратегічно-координаційну, операційно-виконавчу, контрольно-аналітичну, гуманітарно-комунікаційну та громадсько-експертну (табл. 2.2.1). Водночас встановлено наявність системних проблем координації між цими підсистемами, зокрема: відсутність єдиного міжвідомчого алгоритму реагування; фрагментація інформаційних ресурсів і реєстрів; низький рівень цифрової інтегрованості; обмежена горизонтальна взаємодія та ризик політичної селективності. Окремо наголошено на необхідності створення Уповноваженого органу з протидії зовнішньому впливу, який забезпечуватиме взаємодію між силовими, аналітичними та регуляторними органами; запровадження єдиної цифрової платформи обміну даними, що дозволить оперативно виявляти ознаки зовнішнього впливу та узгоджувати дії відповідних інституцій; розвитку прозорої системи звітності, активної суспільної взаємодії та механізмів громадського контролю, що сприятиме підвищенню довіри громадян до державної політики у сфері інформаційної безпеки.

3. Узагальнення досвіду іноземних держав (США, Канада, Сполучене Королівство, Австралійський Союз, Франція, Литва, Фінляндія, Польща, Угорщина) дозволило виявити широкий спектр моделей протидії зовнішньому впливу на публічне управління – від реєстраційних (FARA, FIRS, FITS, FITTA) і санкційних до превентивно-аналітичних та культурно-освітніх (табл. 2.3.1). Обґрунтовано, що ефективність кожної з цих моделей визначається конкретним історичним, політичним та інституційним контекстом відповідної держави.

Підкреслено, що результативні моделі поєднують спеціальне законодавство, декларування зв’язків із іноземними суб’єктами, міжвідомчу інтеграцію, прозору публічну комунікацію та ефективні механізми громадського і судового контролю. Водночас на прикладі рф продемонстровано ризики трансформації законодавства про зовнішній вплив у репресивний інструмент політичного тиску.

Обґрунтовано, що для українських реалій найбільш доцільним є впровадження гібридного підходу до протидії зовнішньому впливу на публічне управління, який синтезує: реєстраційні механізми та санкції за недекларування (США, Канада, Сполучене Королівство, Австралійський Союз); контроль фінансування стратегічно чутливих сфер та цифрову безпеку (Франція, Литва); інституційні механізми міжвідомчого моніторингу (Сполучене Королівство, частково Угорщина – з істотними обмеженнями); превентивні та освітні інструменти (Фінляндія); спеціальний режим підвищеної відповідальності в умовах воєнного стану без стигматизації громадянського суспільства.

Отримані висновки створюють теоретичне та практичне підґрунтя для розробки у третьому розділі цілісної адміністративно-правової моделі протидії зовнішньому впливу на публічне управління через запровадження верифікаційних процедур, цифрової інтеграції та спеціалізованих інституцій.

РОЗДІЛ 3
НАПРЯМИ ВДОСКОНАЛЕННЯ АДМІНІСТРАТИВНО-ПРАВОВОГО МЕХАНІЗМУ ЗАБЕЗПЕЧЕННЯ ІНФОРМАЦІЙНОЇ БЕЗПЕКИ УКРАЇНИ

3.1. Особливості адміністративно-правової ідентифікації афілійованості та ризиків зовнішнього впливу на публічне управління

У сучасних умовах трансформації публічного управління ключовою проблемою забезпечення інформаційної безпеки стає відсутність чітко структурованого механізму ідентифікації та оцінки ризиків зовнішнього впливу на публічне управління. На відміну від класичних загроз, що мали чітко виражений суб'єктний і юрисдикційний вимір, сучасні впливи реалізуються переважно у латентний спосіб – через фінансові, інформаційні, кадрові та організаційні зв'язки, які формально можуть перебувати у межах правового поля, однак у сукупності здатні деформувати процеси вироблення та реалізації публічної політики.

За таких умов ключовою проблемою стає не стільки притягнення до відповідальності окремих осіб, скільки відсутність формалізованого адміністративно-правового інструментарію, який дозволяв би:

своєчасно ідентифікувати ризики зовнішнього впливу;

відмежувати легітимну участь у публічному управлінні від прихованої афілійованості;

забезпечити пропорційність і правову визначеність державного реагування.

Саме тому у межах цього підрозділу обґрунтовується та пропонується алгоритм адміністративно-правової ідентифікації зовнішнього впливу, побудований на ризик-орієнтованій моделі та адаптований до природи адміністративно-правового регулювання.

Слід зауважити, що адміністративно-правовий підхід до протидії зовнішньому впливу принципово відрізняється від кримінально-правової або контррозвідувальної логіки. Його об’єктом є не встановлення вини конкретної особи, а оцінка ризиків для публічних інтересів, що виникають унаслідок непрозорих або асиметричних впливів на управлінські процеси.

У цьому контексті ідентифікація зовнішнього впливу має здійснюватися не за формальною ознакою іноземного походження ресурсів чи контактів, а на основі сукупності юридично значущих критеріїв, які дозволяють оцінити:

характер впливу;

його системність і спрямованість;

потенційні наслідки для інформаційної безпеки та суверенітету публічного управління.

Такий підхід відповідає європейській концепції управління ризиками у сфері демократичної стійкості (democratic resilience) та дозволяє уникнути стигматизації суб’єктів публічного життя [198].

Для переведення проблеми зовнішнього впливу у формалізовану адміністративно-правову площину пропонується застосування системи критеріїв, які визначають юридичну значущість відповідних впливів. Такі критерії виконують фільтраційну функцію та дозволяють відмежувати соціально допустиму діяльність від такої, що створює ризики для публічного управління.

Визначення вагових коефіцієнтів критеріїв та індикаторів, а також порогових значень рівнів ризику, здійснювалося із застосуванням методу експертних оцінок. Для цього було проведено анкетування 18 експертів з подальшою перевіркою узгодженості їхніх суджень за допомогою коефіцієнта конкордації Кендалла (W). Детальна методика опитування, анкети та результати узгодження подані у відповідних додатках до дисертації.

Експертна вибірка сформована з представників інститутів громадянського суспільства, що здійснюють діяльність у сферах громадянської освіти, аналітики публічної політики, виборчого спостереження, забезпечення прозорості публічного управління та розвитку демократичного, правового, культурного й

економічного середовища в суспільстві. До опитування було залучено 18 експертів – по 9 представників від двох громадських організацій: Свідома Громадськість, Незалежний центр політичних студій та аналітики «СвідомІнформ».

Розподіл вагових коефіцієнтів критеріїв адміністративно-правової значущості зовнішнього впливу (табл. 3.1.1) визначено на основі експертного опитування з використанням процедури зваженого ранжування. Експертам було запропоновано розподілити 100 балів між п’ятьма критеріями залежно від їхньої значущості для ідентифікації юридично релевантного зовнішнього впливу на публічне управління. Узгодженість експертних оцінок перевірено за допомогою коефіцієнта конкордації Кендалла, що дозволило підтвердити допустимий рівень консенсусу та використати усереднені значення як підґрунтя для подальшого адміністративно-правового моделювання (див. додаток В)

Таблиця 3.1.1

Критерії адміністративно-правової значущості зовнішнього впливу

№ з/п	Критерій	Зміст критерію	Вага %	Адміністративно-правове значення
1.	Сфера впливу	Кадрова, нормативна, інформаційна, експертна	25	Визначає чутливість управлінського процесу
2.	Інтенсивність	Разовий або системний вплив	20	Впливає на рівень ризику
3.	Прихованість	Відкрита або латентна форма	25	Ключова ознака зовнішнього впливу
4.	Афілійованість	Пряма чи опосередкована	20	Визначає доказову вагу
5.	Потенційна шкода	Управлінська, інформаційна, репутаційна	10	Обґрунтовує необхідність реагування
Разом			**100**	

Примітка: поріг активації перевірки – ≥ 51%.

Зазначені критерії не мають самостійного карального значення, а використовуються виключно для аналітичної оцінки ризиків у межах адміністративної процедури.

З метою усунення оціночності та селективності у правозастосуванні пропонується використання системи індикаторів афілійованості, кожному з яких

надається певна доказова вага. Такий підхід дозволяє перейти від інтуїтивних оцінок до формалізованого ризик-скорингу [199].

Розподіл вагових коефіцієнтів індикаторів афілійованості (від 0,10 до 0,30) здійснено шляхом експертного анкетування. Експертам пропонувалося здійснити попарне порівняння індикаторів за шкалою від 1 до 9 відповідно до їхньої доказової значущості у встановленні непрямої або прихованої афілійованості. Узгодженість суджень експертів перевірено за допомогою коефіцієнта конкордації Кендалла, що дозволило забезпечити пропорційність та методичну обґрунтованість отриманих коефіцієнтів (див. додаток Г).

Таблиця 3.1.2

Індикатори афілійованості та коефіцієнти доказової ваги

№ з/п	Індикатор	Характеристика	Коефіцієнт	Приклади джерел верифікації
1.	Фінансова залежність	Отримання коштів або ресурсів	0,30	НАЗК, Держфінмоніторинг, *ProZorro*
2.	Кадрові зв’язки	Контракти, спільна зайнятість	0,25	*YouControl*, ЄДР, трудові договори
3.	Інформаційна синхронізація	Узгоджені наративи, кампанії	0,20	ЦПД, семантичний аналіз ЗМІ
4.	Організаційна інтеграція	Участь у мережах або структурах	0,15	Реєстр НУО, форумні бази
5.	Регулярність контактів	Системна комунікація	0,10	МЗС, СБУ (публічні звіти та відкриті повідомлення)
Разом			1,00	

Примітка: середній ризик – 0.30-0.60; високий ризик – ≥ 0.61.

Сума коефіцієнтів становить 1,0, що забезпечує пропорційність та прозорість аналітичної оцінки.

З метою формалізації процесу ідентифікації та мінімізації суб’єктивізму при прийнятті управлінських рішень, у межах дослідження розроблено математичну модель розрахунку інтегрального показника ризику зовнішнього впливу (IR):

$$IR = \left(\sum_{i=1}^{n} W_i K_i\right)\left(\sum_{j=1}^{m} V_j I_j\right)$$

де:

IR – інтегрований показник ризику (діапазон значень від 0 до 1,0);

W_i – ваговий коефіцієнт i-того критерію адміністративно-правової значущості (згідно з табл. 3.1.1 , виражений у значенні десяткової частини від цілого);

K_i – бінарний показник наявності ознак за критерієм (1 – наявні, 0 – відсутні);

V_j – коефіцієнт доказової ваги j-того індикатора афілійованості (згідно з табл. 3.1.2);

I_j – бінарний показник верифікації індикатора (1 – підтверджено, 0 – не підтверджено).

Використання бінарних показників (0/1) зумовлене необхідністю забезпечення юридичної визначеності, перевірюваності адміністративних рішень та можливості ефективного судового контролю за процедурою ідентифікації ризиків.

Запропонована математична модель дозволяє перевести якісні характеристики зовнішнього впливу у кількісні показники, що формує об’єктивну базу для подальшої класифікації. На основі поєднання критеріїв та індикаторів формується матрична модель оцінки ризиків, яка дозволяє визначити рівень загрози та відповідний йому адміністративно-правовий режим без автоматичного накладення санкцій.

Порогові значення сукупного показника ризику (IR) та відповідні їм адміністративні режими (табл. 3.1.3) визначено на основі експертного оцінювання з урахуванням принципу пропорційності адміністративного втручання. Експертам пропонувалося співвіднести отримані значення ризик-скорингу з допустимими формами державного реагування – від пасивного моніторингу до тимчасових процедурних обмежень. Узгодженість експертних оцінок підтверджено за допомогою коефіцієнта конкордації Кендалла (результати розрахунків подано у додатку Д).

Тимчасове призупинення участі особи в дорадчих органах або робочих групах здійснюється як забезпечувальний захід виключно на період проведення поглибленої перевірки за рішенням адміністративного суду.

Таблиця 3.1.3

Класифікація рівнів ризику зовнішнього впливу

№ з/п	Сукупний показник	Рівень ризику	Адміністративний режим	Процедурні заходи
1.	0–0,31	Низький	Моніторинг	Щорічний автоматизований скринінг
2.	0,32–0,61	Середній	Підвищені вимоги до прозорості	Декларування афілійованості (30 днів)
3.	0,62–0,85	Високий	Спеціальна адміністративна процедура з судовим контролем	Міжвідомча верифікація + судовий контроль
4.	0,86–1,00	Критичний	Тимчасові управлінсько-процедурні заходи	Тимчасове призупинення участі (до 90 днів)

Примітка: поріг активації – ≥ 0,32.

Таким чином, навіть високий рівень ризику сам по собі не означає протиправності, а лише обґрунтовує застосування посилених процедурних гарантій.

Запропонований алгоритм орієнтований на превентивне управління ризиками, а не на репресивне реагування. Юридичними наслідками встановлення ризику можуть бути:

застосування режимів підвищеної прозорості;

спеціальні вимоги до декларування афілійованості;

ініціювання міжвідомчої перевірки;

звернення до суду виключно у випадках застосування обмежувальних заходів.

Такий підхід забезпечує відповідність механізму принципам верховенства права, юридичної визначеності та пропорційності.

Отже, запропонований алгоритм є адміністративно-правовою моделлю управління ризиками зовнішнього впливу на публічне управління, що ґрунтується на превентивній ідентифікації юридично значущих факторів ризику та застосуванні пропорційних процедурних режимів без кваліфікації поведінки як правопорушення та створює надійну методологічну основу для подальшого розгортання авторської моделі адміністративно-правового механізму забезпечення інформаційної безпеки України в аспекті протидії зовнішньому впливу на публічне управління, що отримує розвиток у підрозділі 3.2.

3.2. Пропозиції щодо удосконалення адміністративно-правового механізму забезпечення інформаційної безпеки України в аспекті протидії зовнішньому впливу на публічне управління

Сформульовані у підрозділі 1.3 положення щодо структури та функціонування системи публічного управління дають змогу зробити принципово важливий методологічний висновок: зовнішній вплив реалізується не шляхом прямого втручання у владні повноваження, а через деформацію інформаційного, процедурного та смислового середовища ухвалення управлінських рішень. Саме ця особливість зумовлює необхідність формування спеціалізованого адміністративно-правового механізму, який був би спрямований не на репресивне обмеження суб'єктів горизонтального виміру публічного управління, а на виявлення, ідентифікацію та нейтралізацію прихованої афілійованості та непрозорого впливу.

Європейська правова традиція виходить з того, що протидія зовнішньому впливу є складовою забезпечення демократичної стійкості (democratic resilience), а не інструментом політичного контролю [198]. У документах ЄС, Ради Європи, а також у національних практиках Фінляндії, Франції, Німеччини та Литви простежується спільний підхід: обмеження допускаються лише за умови їх пропорційності, правової визначеності та ефективного судового контролю [186-194].

З огляду на це, запропонована авторська модель адміністративно-правового механізму протидії зовнішньому впливу ґрунтується на поєднанні вертикального регуляторного впливу держави та горизонтальних інструментів прозорості й відповідальності, що відповідає дуалістичній природі публічного управління.

Метою механізму є не обмеження громадської активності як такої, а захист інформаційної безпеки держави шляхом забезпечення прозорості участі суб'єктів у процесах формування управлінського порядку денного. У цьому сенсі зовнішній вплив розглядається як адміністративно-правова проблема лише тоді, коли він:

здійснюється опосередковано або приховано;

впливає на процеси ухвалення публічних рішень;

реалізується поза межами формалізованих процедур;

суперечить публічним інтересам і стратегічним цілям держави.

Таким чином, об’єктом правового реагування є не суб’єкт сам по собі, а факт і характер його афілійованості та спосіб впливу на публічне управління.

Запропонований механізм має багаторівневу структуру та включає взаємопов’язані блоки, кожен з яких виконує самостійну, але не автономну функцію.

Базовим елементом такого механізму виступає нормативно-правовий компонент, який визначає правові рамки допустимої та недопустимої поведінки у сфері публічного управління. Саме через норми адміністративного права встановлюються вимоги до прозорості взаємодії з іноземними суб’єктами, обов’язки щодо декларування потенційної афілійованості, а також процедурні гарантії захисту прав осіб, на яких поширюються відповідні регулятивні режими. Важливо підкреслити, що ефективність цього компоненту залежить не від жорсткості санкцій, а від чіткості правових дефініцій і процедур, що унеможливлюють довільне або політично вмотивоване застосування норм.

Цей блок передбачає формування спеціального законодавчого масиву, ядром якого виступатиме Закон України «Про протидію зовнішньому впливу на публічне управління» (Додаток Е), який:

закріплює чіткі та вузькі визначення понять «зовнішній вплив», «іноземний суб’єкт», «афілійований суб’єкт»;

фіксує принципи протидії зовнішньому впливу (законність, пропорційність, прозорість, політична нейтральність, судовий контроль);

встановлює критерії адміністративно-правової значущості впливу (сфера, інтенсивність, системність, спрямованість);

відмежовує легітимну громадську участь від прихованого зовнішнього втручання.

Принципово важливим є те, що правове регулювання не повинно охоплювати всю діяльність інститутів громадянського суспільства, а лише ту її частину, яка безпосередньо інтегрована у процеси публічного управління.

Таким чином, нормативно-правовий компонент створює правову оболонку механізму, в межах якої всі інші компоненти набувають легітимності та передбачуваності.

Другий елемент становить інституційно-координаційний блок, який охоплює систему суб'єктів публічної управління, залучених до реалізації механізму протидії зовнішньому впливу. У межах моделі ключова роль відводиться органу стратегічної координації, здатному акумулювати аналітичні дані, узгоджувати дії різних відомств і транслювати результати аналізу у площину управлінських рішень. Важливо, що ця координація має не оперативно-каральний, а аналітично-управлінський характер, що відповідає природі адміністративного права.

Для реалізації цих функцій в рамках авторської моделі запропоновано створення ЦПЗВ як ЦОВВ зі спеціальним статусом, що діє на підставі окремого закону (статті 6–7 проєкту Закону, Додаток Е).

Його особливий статус зумовлюється міжсекторальним характером зовнішнього впливу, який перетинає сфери інформаційної безпеки, публічного управління, антикорупційної політики, національної безпеки та захисту демократичних інститутів. Водночас Центр не підміняє повноваження правоохоронних органів, судів чи органів національної безпеки, а функціонує як спеціалізований адміністративно-аналітичний суб'єкт.

Основним призначенням Центру буде забезпечення адміністративно-правової ідентифікації зовнішнього впливу у сфері публічного управління. У цьому контексті його діяльність спрямовується не на оцінку політичних поглядів або ідеологічних позицій, а на виявлення прихованих або непрозорих зв'язків між іноземними суб'єктами та учасниками управлінських процесів.

Центр здійснюватиме:

системний аналіз ризиків зовнішнього впливу на органи публічної влади;

оцінку афілійованості суб’єктів, залучених до формування управлінського порядку денного;

моніторинг інформаційно-комунікаційних, експертних та фінансових каналів впливу;

підготовку мотивованих адміністративних висновків щодо наявності або відсутності ознак зовнішнього впливу.

Таким чином, Центр виступатиме фільтром між аналітичним виявленням ризиків і можливими правовими наслідками, не допускаючи автоматизму чи політичної доцільності у прийнятті рішень.

Ключовою умовою легітимності діяльності Центру буде наявність чітко врегульованих адміністративних процедур. Ідентифікація зовнішнього впливу здійснюватиметься виключно в межах формалізованого процесу, що передбачає:

1. Ініціювання перевірки – на підставі обґрунтованого запиту органу влади, власного аналітичного моніторингу або звернення іншого суб’єкта публічного управління.

2. Збирання та оцінку інформації – із використанням відкритих джерел, офіційних реєстрів та наданих пояснень заінтересованих осіб.

3. Встановлення юридично значущих ознак афілійованості – за критеріями, визначеними законом.

4. Підготовку адміністративного висновку, який не має карального характеру, але може слугувати підставою для подальших рішень.

5. Право на заперечення та судовий контроль – кожен суб’єкт, щодо якого здійснювалася процедура, повинен мати гарантовану можливість оскарження дій Центру.

У такий спосіб Центр не ухвалює рішень про покарання, а діє в межах превентивної адміністративно-правової логіки.

Одним із практичних результатів діяльності Центру буде ведення Реєстру афілійованих суб’єктів, який має публічно-правовий, а не стигматизаційний характер (статті 7, 9 проєкту Закону, Додаток Е).

Включення до Реєстру:

не тягне автоматичних обмежень;

не позбавляє прав;

не означає визнання протиправної діяльності.

Його функція полягає у забезпеченні прозорості участі суб'єктів у публічному управлінні, що відповідає європейським стандартам відкритості та доброчесності.

Центр діятиме у тісній взаємодії з:

органами виконавчої влади;

антикорупційними інституціями;

органами національної безпеки – виключно в межах передбачених законом процедур;

судами – як єдиним органом, уповноваженим застосовувати обмежувальні заходи.

Це унеможливить концентрацію надмірних повноважень в одному органі та запобігає трансформації механізму на репресивний.

Інституційне закріплення Центру в проєкті Закону України «Про протидію зовнішньому впливу на публічне управління» дозволяє:

перевести проблему зовнішнього впливу з політичної площини в адміністративно-правову;

створити процесуально захищений механізм реагування;

забезпечити відповідність європейським стандартам прав людини;

уникнути повторення негативних моделей авторитарного регулювання.

Третім елементом є інформаційно-аналітичний блок, який забезпечує функціонування моделі на основі доказовості та об'єктивних даних. Йдеться про системний збір, обробку й аналіз інформації з відкритих і спеціалізованих джерел, фінансових потоків, комунікаційних наративів та управлінських рішень. У межах авторської моделі аналітика не є допоміжною функцією, а виступає центральною ланкою, що визначає логіку подальшого адміністративного реагування.

По суті, інформаційно-аналітичний компонент є функціональним ядром механізму протидії зовнішньому впливу, оскільки саме на цьому рівні здійснюється перехід від абстрактного уявлення про загрозу до її конкретизації у вигляді ідентифікованих ризиків.

Його особливістю є те, що він не спрямований на безпосереднє управління або примус, а виконує оціночну та прогностичну функції. В умовах гібридних загроз зовнішній вплив рідко проявляється у формі прямих дій; натомість він реалізується через накопичення інформаційних сигналів, непрямих ознак афілійованості, фінансових або комунікаційних зв'язків.

Для реалізації таких завдань передбачається створення єдиної цифрової платформи міжвідомчого обміну даними (CIMA), що функціонуватиме на базі ЦПЗВ та інтегрує дані з відкритих джерел, публічних реєстрів, звітності суб'єктів публічного управління, а також результатів стратегічних комунікацій. Використання CIMA забезпечує централізовану аналітику, раннє виявлення потенційних ризиків зовнішнього впливу та підвищує ефективність міжвідомчої координації.

Аналітична діяльність у межах цього компоненту має бути стандартизованою та позбавленою політичної дискреції. Йдеться не про формування «підозр», а про оцінку ризиків за визначеними законом критеріями, що дозволяє перевести аналіз зовнішнього впливу у формалізовану адміністративну площину.

Таким чином, інформаційно-аналітичний компонент забезпечує доказову основу для прийняття подальших управлінських рішень і виступає запобіжником від довільного трактування впливів.

Четвертим елементом виступає процедурно-контрольний блок, який забезпечує реалізацію принципів належної адміністративної процедури. Саме через цей блок гарантується дотримання презумпції добросовісності, право на захист, можливість оскарження управлінських рішень та судовий контроль. Наявність розвиненого процедурного компоненту дозволяє відмежувати адміністративно-

правовий механізм від репресивних моделей і забезпечити його відповідність європейським стандартам верховенства права.

Фундаментальне значення для легітимності запропонованого механізму має дотримання стандартів, випрацюваних у практиці ЄСПЛ. Зокрема, у справі «Класс та інші проти Німеччини» (Klass and Others v. Germany, 1978) Суд визнав, що держави мають право на здійснення прихованого адміністративного нагляду для захисту демократичних інститутів від зовнішніх загроз, проте за умови встановлення ефективних гарантій проти зловживань. Ключовою такою гарантією Суд визначив судовий контроль, який має перевагу перед адміністративним, оскільки забезпечує незалежність, неупередженість та належну процедуру [200]. Саме тому в основі нашої моделі лежить принцип, згідно з яким аналітична діяльність ЦПЗВ та функціонування системи СІМА підлягають обов'язковому судовому нагляду, а будь-які обмежувальні заходи (наприклад, призупинення участі у дорадчих органах) застосовуються виключно за рішенням адміністративного суду (відповідно до процедур, закріплених у статтях 36–40 проєкту Закону, Додаток Е).

В межах реалізації цього компоненту передбачається:

визначення стадій адміністративного провадження щодо ідентифікації зовнішнього впливу;

закріплення прав заінтересованих осіб на надання пояснень, доступ до матеріалів і оскарження;

обов'язковість судового контролю у випадках застосування будь-яких обмежувальних заходів.

Контрольна складова цього компоненту проявляється у багаторівневій системі нагляду за діяльністю органів, залучених до протидії зовнішньому впливу, що унеможливлює концентрацію повноважень в одному суб'єкті.

У такий спосіб процедурно-контрольний компонент виконує балансуючу функцію, поєднуючи ефективність механізму з дотриманням стандартів правової держави.

Завершальним елементом моделі є комунікаційно-превентивний блок, спрямований на зниження вразливості публічного управління до зовнішнього впливу шляхом формування культури прозорості, доброчесності та інституційної стійкості. Його функція полягає не у реагуванні на вже виявлені загрози, а у створенні умов, за яких зовнішній вплив втрачає ефективність.

Даний компонент передбачає формування державної політики стратегічних комунікацій у сфері публічного управління, спрямованої на підвищення обізнаності посадових осіб, представників місцевого самоврядування, громадського сектору та експертних середовищ щодо ризиків прихованої афілійованості та маніпулятивних практик.

Він реалізується через:

методичні рекомендації та стандарти доброчесної участі в управлінських процесах;

публічну звітність про загальні тенденції зовнішнього впливу без персоніфікації;

підтримку незалежних експертних і освітніх ініціатив.

Зазначені заходи не мають регулятивного або обмежувального характеру та не породжують індивідуальних правових наслідків.

Комунікаційно-превентивний компонент формує культуру стійкості, в межах якої зовнішній вплив втрачає ефективність ще до стадії адміністративного реагування.

Системність запропонованої авторської моделі адміністративно-правового механізму протидії зовнішньому впливу зумовлює необхідність її структурного узагальнення. З цією метою у таблиці 3.2.1 представлено складові механізму з визначенням їх функціонального призначення та внутрішньої логіки взаємодії.

Наведена структура демонструє, що адміністративно-правовий механізм протидії зовнішньому впливу не зводиться до окремих правових норм або інституційних рішень, а постає як багаторівнева система, в якій кожен компонент виконує самостійну, але взаємопов’язану функцію. Нормативно-правовий і процедурно-контрольний блоки забезпечують юридичну визначеність і захист

прав людини, інституційно-координаційний та інформаційно-аналітичний – управлінську спроможність держави, тоді як комунікаційно-превентивний компонент формує довгострокову стійкість публічного управління до зовнішніх впливів.

Таблиця 3.2.1

Структура адміністративно-правового механізму забезпечення інформаційної безпеки України в аспекті протидії зовнішньому впливу на публічне управління

№ з/п	Компоненти	Функції	Ключові інструменти	Відповідність моделям
1.	Нормативно-правовий	Юридична основа	Закон «Про протидію...», матриці 3.1.1-3.1.3	FARA, FIRS
2.	Інституційно-координаційний	Центр протидії	ЦПЗВ, міжвідомча координація	Литва
3.	Інформаційно-аналітичний	Ризик-скоринг	*API ProZorro* + НАЗК, семантичний аналіз	Франція *Viginum*
4.	Процедурно-контрольний	Гарантії прав	Судовий контроль (15 днів), апеляція	Практика ЄСПЛ
5.	Комунікаційно-превентивний	Стійкість	Освітній хаб, методичні рекомендації	Фінляндія

Джерело: розроблено автором.

Функціонування адміністративно-правового механізму забезпечення інформаційної безпеки України в аспекті протидії зовнішньому впливу на публічне управління має розглядатися як безперервний управлінський процес, що реалізується у формі послідовних, взаємопов’язаних стадій.

Початковою стадією є превентивний моніторинг, у межах якого здійснюється постійне спостереження за управлінськими, інформаційними та фінансовими процесами, що можуть бути об’єктом зовнішнього впливу. На цій стадії основний акцент робиться не на виявленні правопорушень, а на фіксації потенційних ризиків і тенденцій, що можуть загрожувати стійкості публічного управління.

Наступною стадією виступає ідентифікація та оцінка ризиків, яка передбачає аналіз джерел, форм і інтенсивності зовнішнього впливу з урахуванням можливих наслідків для публічних інтересів. Важливою особливістю цієї стадії є відмова від

автоматизму у застосуванні обмежувальних заходів: встановлення ризику саме по собі не повинно тягнути санкцій, а має слугувати підставою для прийняття зважених адміністративних рішень.

На стадії адміністративного реагування застосовуються диференційовані заходи впливу, спрямовані на мінімізацію або нейтралізацію встановлених ризиків. Йдеться про підвищені вимоги до прозорості, спеціальні режими контролю, тимчасові обмеження у визначених законом випадках. Ключовою умовою ефективності цієї стадії є процедурна визначеність та можливість перевірки обґрунтованості прийнятих рішень.

Функціональний цикл завершується стадією контролю та перегляду, у межах якої здійснюється оцінка результативності вжитих заходів, їх відповідності принципам верховенства права та можливості корекції управлінських рішень. Судовий контроль на цій стадії виступає не як перешкода, а як гарантія легітимності механізму в цілому.

Завершальним елементом функціонування механізму є публічна комунікація та корекція державної політики, що дозволяє використовувати отримані результати для вдосконалення нормативно-правової бази та інституційної архітектури з питань протидії зовнішньому впливу.

Детальна правова імплементація авторської моделі адміністративно-правового механізму забезпечення інформаційної безпеки України в аспекті протидії зовнішньому впливу на публічне управління представлена у проєкті Закону України «Про протидію зовнішньому впливу на публічне управління» (Додаток Е), який інтегрує всі п’ять компонентів механізму у єдину правову систему.

Висновки до розділу 3

У третьому розділі дисертаційного дослідження здійснено перехід від аналітичного осмислення проблеми зовнішнього впливу на публічне управління до формування цілісної авторської концепції вдосконалення адміністративно-правового механізму забезпечення інформаційної безпеки України. Розділ має прикладно-концептуальний характер і поєднує доктринальні узагальнення з конкретними інструментами нормативної, інституційної та процедурної імплементації.

1. Розроблено формалізований підхід до ідентифікації зовнішнього впливу як загрози суверенітету публічного управління, який ґрунтується на ризик-орієнтованій логіці та відповідає природі адміністративно-правового регулювання. Запропоновано матричну модель оцінки афілійованості фізичних і юридичних суб'єктів з іноземними суб'єктами, що інтегрує юридичні, функціональні та індикативні критерії з визначенням їхньої доказової ваги. Такий підхід дозволяє усунути оціночність і селективність у правозастосуванні, створює підґрунтя для автоматизації аналітичних процедур та забезпечує пропорційність управлінсько-превентивного реагування, що здійснюється під судовим контролем.

Обґрунтовано, що ідентифікація зовнішнього впливу не повинна ототожнюватися з притягненням до юридичної відповідальності, а має розглядатися як інструмент превентивного управління ризиками у сфері публічного управління. У цьому контексті ключове значення мають багаторівнева система верифікації, міжвідомчий обмін інформацією через Систему інтегрованого моніторингу афілійованості, фінансовий і контент-аналіз, а також чітко визначені процедурні гарантії прав і свобод людини.

2. Сформульовано пропозиції щодо вдосконалення нормативно-правового та інституційно-координаційного блоків адміністративно-правового механізму забезпечення інформаційної безпеки України в аспекті протидії зовнішньому впливу на публічне управління. Доведено, що ефективна протидія зовнішньому

впливу потребує спеціального правового регулювання, здатного інтегрувати аналітичні інструменти, адміністративні процедури, інституційну координацію та судовий контроль у єдину системну модель.

У цьому зв’язку обґрунтовано концепцію спеціального законодавчого акту – Закону України «Про протидію зовнішньому впливу на публічне управління», який закріплює: понятійно-категоріальний апарат; критерії ідентифікації та ризик-орієнтовану оцінку; процедурні межі аналітичної діяльності; а також окремий судоцентричний механізм застосування правових наслідків управлінсько-превентивного характеру. Показано, що запропонована модель законодавчого регулювання є результатом адаптації кращих міжнародних практик (США, Канада, Сполучене Королівство, Австралійський Союз, Франція, Литва, Фінляндія) до українських безпекових і правових реалій, з урахуванням умов воєнного стану.

Окрему увагу приділено інституційному забезпеченню реалізації запропонованого механізму. Обґрунтовано доцільність створення спеціалізованого уповноваженого органу з протидії зовнішньому впливу – Центру протидії зовнішньому впливу як центрального органу виконавчої влади зі спеціальним статусом. Підкреслено, що такий орган не має каральних або правоохоронних повноважень і функціонує виключно як спеціалізований суб’єкт адміністративного аналізу, уповноважений ініціювати судовий розгляд щодо застосування правових наслідків.

3. Сформульовано авторську модель адміністративно-правового механізму протидії зовнішньому впливу на публічне управління, яка виступає логічним підсумком проведеного дослідження. Запропонована модель базується на процесно-орієнтованому підході та розглядає зовнішній вплив як об’єкт адміністративно-правового регулювання у площині управлінських відносин, а не як персоніфіковану характеристику окремих осіб.

Авторська модель поєднує нормативно-правовий, інституційно-координаційний, інформаційно-аналітичний, процедурно-контрольний та комунікаційно-превентивний блоки, завершуючись судоцентричним елементом

застосування правових наслідків управлінсько-превентивного характеру, що не мають каральної природи, є строковими та індивідуалізованими. Доведено, що такий підхід повністю відповідає стандартам Європейського суду з прав людини (зокрема, за критеріями «якості закону» та «ефективного судового нагляду»), оскільки забезпечує пріоритет судового контролю над адміністративною дискрецією. Такий підхід забезпечує відповідність механізму принципам верховенства права, юридичної визначеності та пропорційності, а також сучасним європейським стандартам адміністративного права.

Таким чином, результати третього розділу підтверджують можливість і доцільність переходу від фрагментарних заходів протидії зовнішньому впливу до цілісної, науково обґрунтованої адміністративно-правової моделі, що поєднує превентивну аналітику, інституційну координацію та судовий контроль і здатна забезпечити інформаційну безпеку України без порушення балансу між публічними інтересами та правами людини.

ВИСНОВКИ

У дисертації розв’язано наукову проблему, сутність якої полягала в обґрунтуванні теоретичних положень і методологічних підходів, виробленні практичних пропозицій щодо вдосконалення адміністративно-правового механізму забезпечення інформаційної безпеки України в аспекті протидії зовнішньому впливу на публічне управління. Розв’язання проблеми є представленим у таких висновках і положеннях дослідження, що мають наукову новизну.

1. Здійснено аналіз та систематизацію підходів до розуміння сутності інформаційної безпеки держави як складного багатоаспектного феномену, що поєднує технологічні, політичні, правові, ціннісні та культурні аспекти. Виокремлено дві групи існуючих концептуальних підходів до трактування інформаційної безпеки: за спільними ознаками: системний, статичний, процесний (діяльнісний), комплексний; за трансдисциплінарною природою: технічний, гуманітарний, нормативний, психологічний, комплексний. Обґрунтовано прийнятність комплексного підходу, який у першому випадку інтегрує статичний і діяльнісний підходи, в іншому – виступає цілісною концепцією з урахуванням як технічних, так і соціально-психологічні аспектів. Обґрунтовано авторське визначення інформаційної безпеки держави як нормативно закріплений стан захищеності національного інформаційного простору, за якого забезпечується: стійкість інформаційної інфраструктури та цілісність інформаційних ресурсів; стабільність інформаційних процесів і захист прав суб’єктів інформаційних відносин; збереження національної інформаційної ідентичності; реалізація національних інтересів і досягнення стратегічних цілей в інформаційній сфері; створення умов для сталого розвитку інформаційного суспільства.

2. Розкрито сутність категорії «адміністративно-правовий механізм забезпечення інформаційної безпеки держави» через призму системного, структурно-функціонального, діяльнісного та комплексного підходів. Запропоновано розглядати адміністративно-правовий механізм забезпечення інформаційної безпеки держави в рамках комплексного підходу як підсистему

державного управління, що через норми права, діяльність уповноважених інституцій та застосування адміністративних інструментів (дозвільних, реєстраційних, контрольних, примусових) забезпечує захист від внутрішніх і зовнішніх загроз та створює умови для сталого розвитку національного інформаційного простору. Наголошено на тому, що такий механізм має інтегрований і цілісний характер та функціонує у взаємодії із зовнішніми й внутрішніми факторами та умовами. Розкрито структуру адміністративно-правового механізму забезпечення інформаційної безпеки держави, яка включає такі блоки (компоненти): нормативно-правовий – сукупність норм права та нормативно-правових актів, що формують правові умови забезпечення інформаційної безпеки; інституційно-координаційний – система органів державної влади, спеціально уповноважених установ та інших суб'єктів публічного управління, які здійснюють реалізацію державної політики, координацію, моніторинг, аналіз і реагування на загрози; процедурно-контрольний – принципи, методи, процедури й алгоритми реалізації діяльності у сфері інформаційної безпеки, включно з адміністративними інструментами дозволу, реєстрації, контролю та примусу; інформаційно-аналітичний – процеси моніторингу, аналізу та оцінки стану інформаційної безпеки, виявлення загроз і підготовки управлінських рішень щодо їх нейтралізації; комунікаційно-превентивний – система стратегічних комунікацій, освітніх програм, методичних рекомендацій та громадсько-експертних ініціатив, спрямованих на формування культури прозорості, доброчесності та інституційної стійкості.

3. Розкрито теоретико-правову природу зовнішнього впливу на публічне управління як специфічної загрози суверенітету публічного управління та інформаційній безпеці держави, що має опосередкований, прихований і кумулятивний характер та реалізується переважно поза межами формалізованих владно-розпорядчих процедур. У результаті узагальнення сучасних наукових підходів обґрунтовано розуміння публічного управління як складної багаторівневої соціально-правової системи, у межах якої поєднуються вертикальний (ієрархічний, владний) та горизонтальний (мережевий,

комунікативний) виміри, взаємодія яких забезпечує не лише ефективність і стабільність управління, а й соціальну легітимацію управлінських рішень.

Доведено, що горизонтальний вимір публічного управління, який охоплює громадське управління (інститути громадянського суспільства, експертні, аналітичні та медійні середовища), є найбільш вразливим до зовнішнього впливу внаслідок своєї відкритості, плюралістичності, відсутності жорсткої ієрархічної підпорядкованості та активного використання формальних і неформальних інформаційно-комунікаційних каналів. Саме ця вразливість зумовлює трансформацію зовнішнього впливу з класичних форм прямого втручання у приховані механізми деформації управлінських процесів.

Установлено, що зовнішній вплив у системі публічного управління спрямовується не на безпосереднє здійснення владних повноважень, а на формування інформаційного, смислового та процедурного середовища ухвалення управлінських рішень, зокрема через вплив на управлінський порядок денний, рамки інтерпретації проблем і спектр допустимих управлінських альтернатив. У цьому контексті запропоновано авторські визначення зовнішнього впливу на публічне управління та пов’язаних з ним понять: іноземний, афілійований суб’єкт.

Доведено, що результатом такого впливу є інституційно-процедурна деформація управлінських процесів – це системне викривлення нормативно визначеного порядку здійснення управління, що проявляється у підміні публічного інтересу інтересами суб’єктів впливу, яка призводить до втрати суверенітету публічного управління – здатності системи публічного управління самостійно, відповідно до публічних інтересів та правових процедур, формувати порядок денний та ухвалювати рішення.

Деталізовано функціональну роль адміністративно-правового механізму забезпечення інформаційної безпеки держави в частині протидії зовнішньому впливу як системи процедурних фільтрів (ідентифікації та ризик-скорингу, адміністративної перевірки, судового контролю). Підкреслено, що така модель

дозволяє убезпечити «точки дотику» між вертикальним і горизонтальним вимірами публічного управління.

4. Проаналізовано сучасний стан нормативно-правового забезпечення інформаційної безпеки України в аспекті протидії зовнішньому впливу на публічне управління. Встановлено, що нормативно-правове забезпечення інформаційної безпеки України має фрагментарний та концептуально незавершений характер в частині протидії зовнішньому впливу на публічне управління, попри наявність значного масиву законодавчих і стратегічних актів у сфері національної безпеки, інформаційної політики та публічного управління. Проведений аналіз засвідчив, що чинне правове регулювання не формує цілісної моделі реагування на опосередковані та приховані впливи на управлінські процеси, залишаючи поза увагою горизонтальний вимір публічного управління.

Виявлено, що ключовими чинниками, які стримують ефективність нормативно-правового забезпечення протидії зовнішньому впливу, є втрата актуальності окремих нормативно-правових актів, відсутність законодавчо закріпленого понятійно-категоріального апарату (зокрема дефініцій «зовнішній вплив», «іноземний суб’єкт», «афілійований суб’єкт»), а також брак спеціалізованих реєстраційних, наглядових і контрольних механізмів, адаптованих до нефронтального характеру сучасних загроз. У результаті правове регулювання має переважно реактивний і декларативний характер та не забезпечує превентивного управління ризиками.

Проаналізовано еволюцію національних нормативних ініціатив у цій сфері, яка засвідчує нестійкість державної правової політики щодо протидії зовнішньому впливу на публічне управління, що коливається між надмірно жорсткими, репресивними підходами, які призводять до адміністративно-правової деформації статусу суб’єктів (шляхом їхньої необґрунтованої стигматизації) та формально-декларативними проєктами, що підміняють безпекові питання фінансовою звітністю.

Доведено, що така непослідовність призводить до нормативної невизначеності, підвищує ризики політизації правозастосування та

унеможливлює формування прозорої, підконтрольної й легітимної системи протидії зовнішньому впливу.

Обґрунтовано необхідність формування чітких правових рамок шляхом розроблення та прийняття профільного законодавчого акту у цій сфері, який має інтегрувати понятійні, процедурні та інституційні елементи адміністративно-правового механізму на засадах законності, пропорційності, прозорості та судового контролю.

5. Досліджено систему суб'єктів забезпечення інформаційної безпеки України в аспекті протидії зовнішньому впливу на публічне управління. В рамках дослідження проаналізовано систему суб'єктів забезпечення інформаційної безпеки України, представлену у чинних стратегічних та нормативно-правових документах, встановлено відсутність у них узгодженості щодо визначення суб'єктного складу, а також наявність застарілих підходів у частині суб'єктного складу, зокрема у документах, ухвалених до початку повномасштабної збройної агресії російської федерації проти України, у яких не враховано радикальну зміну архітектури загроз та появу нових інституцій.

В рамках функціонального підходу систему суб'єктів забезпечення інформаційної безпеки України розкрито у вигляді п'яти взаємопов'язаних підсистем: стратегічно-координаційної, операційно-виконавчої, контрольно-аналітичної, гуманітарно-комунікаційної та громадсько-експертної. Наголошено на наявності низки проблемних питань в координації між суб'єктами забезпечення інформаційної безпеки: відсутність єдиного міжвідомчого алгоритму реагування, фрагментація інформаційних ресурсів і реєстрів, недостатня горизонтальна взаємодія, низька цифрова інтегрованість, ризик політизації. З метою покращення спроможностей інституційно-координаційного блоку адміністративно-правового механізму забезпечення інформаційної безпеки України в аспекті протидії зовнішньому впливу на публічне управління запропоновано: створити Уповноважений орган з протидії зовнішньому впливу, який забезпечуватиме взаємодію між силовими, аналітичними та регуляторними органами; запровадити єдину цифрову платформу обміну даними, що дозволить

оперативно виявляти ознаки зовнішнього впливу та узгоджувати дії відповідних інституцій; розвивати прозору систему звітності, активної суспільної взаємодії та механізмів громадського контролю, що сприятиме підвищенню довіри громадян до державної політики у сфері інформаційної безпеки.

6. Здійснено порівняльно-правовий аналіз досвіду іноземних держав (США, Канада, Сполучене Королівство, Австралійський Союз, Франція, Литва, Фінляндія, Польща, Угорщина) щодо протидії зовнішньому впливу на публічне управління – від реєстраційних (FARA, FIRS, FITS, FITAA) і санкційних до превентивно-аналітичних та культурно-освітніх. Підкреслено, що результативні моделі поєднують спеціальне законодавство, декларування зв'язків із іноземними суб'єктами, міжвідомчу інтеграцію та ефективні механізми судового контролю. Водночас на прикладі російської федерації продемонстровано ризики трансформації законодавства про зовнішній вплив у репресивний інструмент політичного тиску. Аналіз міжнародної практики засвідчив, що жодна з існуючих моделей не є універсальною, а їх ефективність визначається конкретним історичним, політичним та інституційним контекстом відповідної держави.

7. Розроблено та науково обґрунтовано формалізований алгоритм адміністративно-правової ідентифікації афілійованості та ризиків зовнішнього впливу на публічне управління, що ґрунтується на ризик-орієнтованій, процесно-управлінській логіці та відповідає природі адміністративного права. Запропонований алгоритм інтегрує систему критеріїв адміністративно-правової значущості зовнішнього впливу (сфера, інтенсивність, прихованість, афілійованість, потенційна шкода) з індикаторами доказової ваги, що дозволяє перейти від оціночних підходів до формалізованого ризик-скорингу.

Сформовано матричну модель оцінки рівнів ризику зовнішнього впливу, яка забезпечує диференціацію адміністративних режимів реагування без автоматичного настання правових наслідків. Доведено, що ідентифікація зовнішнього впливу в адміністративно-правовому сенсі не є встановленням протиправності чи вини, а виступає інструментом превентивного управління ризиками у сфері публічного управління. Такий підхід унеможливлює

селективність і політичну доцільність у правозастосуванні, створює підґрунтя для цифровізації аналітичних процедур, забезпечує пропорційність адміністративного реагування та відповідає європейським стандартам демократичної стійкості, верховенства права і юридичної визначеності.

8. Обґрунтовано наукові та нормативно-правові підходи до вдосконалення адміністративно-правового механізму забезпечення інформаційної безпеки України в аспекті протидії зовнішньому впливу на публічне управління, що поєднує нормативно-правовий, інституційно-координаційний, інформаційно-аналітичний, процедурно-контрольний та комунікаційно-превентивний компоненти в єдину функціональну систему.

Підкреслено, що ключовою інновацією механізму є його судоцентричний характер застосування правових наслідків управлінсько-превентивного типу, які не мають каральної природи, є строковими та застосовуються виключно за рішенням суду. Обґрунтовано, що така модель відповідає критеріям «якості закону» та «необхідності у демократичному суспільстві», випрацюваним у сталій практиці Європейського суду з прав людини, що гарантує належний баланс між інтересами національної безпеки та захистом фундаментальних прав і свобод людини. Доведено доцільність створення спеціалізованого уповноваженого органу – Центру протидії зовнішньому впливу як центрального органу виконавчої влади зі спеціальним статусом, який здійснює адміністративно-аналітичну діяльність для захисту суверенітету публічного управління, але не наділений репресивними повноваженнями.

Показано, що запропонована модель дозволяє перевести протидію зовнішньому впливу з фрагментарної площини у процесуально захищену систему, що забезпечує баланс між потребами безпеки та гарантіями прав людини. Практичним результатом реалізації цієї моделі є формування основи для впровадження спеціального Закону України «Про протидію зовнішньому впливу на публічне управління», який інтегрує превентивну аналітику (Система інтегрованого моніторингу афілійованості), координацію та судовий контроль у цілісну правову архітектуру.

СПИСОК ВИКОРИСТАНИХ ДЖЕРЕЛ

1. Конституція України : від 28.06.1996 № 254к/96-ВР : станом на 1 січ. 2020 р. URL: https://zakon.rada.gov.ua/laws/show/254к/96-вр#Text (дата звернення: 10.04.2026).

2. Енциклопедія Сучасної України. Institute of Encyclopedic Research Academic Repository. 2001. URL: https://doi.org/10.37068/b/966022074x (дата звернення: 10.04.2026).

3. Wiener N. Cybernetics or Control and Communication in the Animal and Machine. New York : John Wiley and Sons, 1948. 212 p.

4. Glushkov V. M. Introduction to Cybernetics. New York : Academic Press, 1966. 322 p.

5. Іванов В. Г., Іванов С. М., Карасюк В. В. Сучасні інформаційні системи і технології: конспект лекцій. Харків : Національний юридичний університет імені Ярослава Мудрого, 2014. 347 с.

6. Телешун С. О., Рейтерович І. В. Інформаційно-аналітична діяльність в державному управлінні : навчально-методичні матеріали. Київ : НАДУ, 2013. 36 с. URL: https://files.znu.edu.ua/files/Bibliobooks/Kapritsyn/0041321.pdf (дата звернення: 10.04.2026).

7. Про інформацію : Закон України від 02.10.1992 № 2657-XII : станом на 14 черв. 2025 р. URL: https://zakon.rada.gov.ua/laws/show/2657-12#Text (дата звернення: 10.04.2026).

8. Цивільний кодекс України : Кодекс України від 16.01.2003 № 435-IV : станом на 18 листоп. 2025 р. URL: https://zakon.rada.gov.ua/laws/show/435-15#Text (дата звернення: 10.04.2026).

9. Про захист економічної конкуренції : Закон України від 11.01.2001 № 2210-III : станом на 16 трав. 2024 р. URL: https://zakon.rada.gov.ua/laws/show/2210-14#Text (дата звернення: 10.04.2026).

10. Словарь української мови: у 4 т. / уклад.: Б. Грінченко. Київ : «Киевская Старина», 1907–1909. Т. 1 : А-В. 401 с.

11. Беззубов Д. О. Суспільна безпека (організаційно-правові засади забезпечення) : монографія. Київ : МП «Леся», 2013. 425 с.

12. Стрельбицька Л. М., Стрельбицький М. П. Методологічні та організаційно-правові засади формування і функціонування системи державного управління національною безпекою України. *Інформація і право.* 2020. Вип. 33 (№ 2). С. 110–120. URL: http://il.ippi.org.ua/article/view/208102 (дата звернення: 10.04.2026).

13. Ліпкан В. А., Харченко Л. С., Логінов О. В. Інформаційна безпека України: Глосарій. Київ : Текст, 2004. 136 с.

14. Кунєв Ю. Д. Правове забезпечення інформаційної безпеки як предмет правового дослідження. *Наукові праці Національного авіаційного університету. Серія: Юридичний вісник «Повітряне і космічне право».* 2021. Вип. 58 (№ 1). С. 95–102. URL: https://doi.org/10.18372/2307-9061.58.15314 (дата звернення: 10.04.2026).

15. Ніщименко О. А. Інформаційна безпека України на сучасному етапі розвитку держави і суспільства. *Наше право*. 2016. № 1. С. 17–23. URL: http://nbuv.gov.ua/UJRN/Nashp_2016_1_6 (дата звернення: 10.04.2026).

16. Кочубей Л. О. Інформаційна безпека держави: інструменти захисту українського інформаційного поля (на прикладі особливостей інформаційно-комунікаційних технологій у сучасному Донбасі). *Наукові записки Інституту політичних і етнонаціональних досліджень імені І.Ф. Кураса.* 2015. Вип. 3. С. 220–237. URL: http://nbuv.gov.ua/UJRN/Nzipiend_2015_3_10 (дата звернення: 10.04.2026).

17. Кормич Б. А. Організаційно-правові засади політики інформаційної безпеки України : монографія. Одеса : Юридична література, 2003. 472 с.

18. Шатун В. Т. Інформаційна безпека – невід’ємна складова національної безпеки України. *Наукові праці Чорноморського державного університету імені Петра Могили комплексу «Києво-Могилянська академія»*. 2016. Вип. 255. С. 174–180. URL: http://nbuv.gov.ua/UJRN/Npchdu_2016_267_255_29 (дата звернення: 10.04.2026).

19. Баранов О. П. Передумови створення Державної спеціальної служби транспорту та її завдання в системі національної безпеки України. *Вісник Національної академії державного управління при Президентові України*. 2014. № 3. С. 60–65.

20. Нижник Н. Р., Ситник Г. П., Білоус В. Т. Національна безпека України (методологічні аспекти, стан і тенденції розвитку): навч. посіб. Ірпінь : Акад. ДПС України, 2000. 304 с.

21. Ярема О. Г., Єсімов С. С. Предмет правового забезпечення інформаційної безпеки в інформаційному праві. *Науковий вісник Львівського державного університету внутрішніх справ.* 2016. № 2. С. 244–252. URL: https://dspace.lvduvs.edu.ua/handle/1234567890/1796?locale=en (дата звернення: 10.04.2026).

22. Бєляков К. І. Деякі питання щодо формування реформи інформаційного законодавства України. *Систематизація законодавства в Україні: проблеми теорії і практики* : тези доп. учасників міжнар. наук.-практ. конфер., м. Київ, 19–20 жовт. 1999 р. / інст-т закон-а Верховної Ради України. Київ, 1999. С. 253–255.

23. Заярний О. О. Особливості захисту інформаційних прав Європейським судом з прав людини з урахуванням прояву наслідків війни проти України. *Право України*. 2025. № 2. С. 90–101. URL: https://doi.org/10.33498/louu-2025-02-090 (дата звернення: 10.04.2026).

24. Про Основні засади розвитку інформаційного суспільства в Україні на 2007-2015 роки : Закон України від 09.01.2007 № 537-V. URL: https://zakon.rada.gov.ua/laws/show/537-16#Text (дата звернення: 10.04.2026).

25. 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. URL: https://zakon.rada.gov.ua/laws/show/685/2021#Text (дата звернення: 10.04.2026).

26. Цимбалюк В. С., Бабінська А. В. Правове регулювання інформаційної безпеки в Україні: проблеми теорії та практики. *Адміністративне право і процес*.

2014. Вип. 2 (№ 8). С. 22–30. URL: https://applaw.net/index.php/journal/article/view/418 (дата звернення: 10.04.2026).

27. Гурковський В. І. Безпека як об'єкт правовідносин в умовах глобального інформаційного суспільства. *Правова інформатика*. 2010. Вип. 26 (№ 2). С. 72–77. URL: http://nbuv.gov.ua/UJRN/Pinform_2010_2_14 (дата звернення: 10.04.2026).

28. Калюжний Р. А. Питання концепції реформування інформаційного законодавства України. *Правове, нормативне та метрологічне забезпечення системи інформації в Україні :* тези доп. учасників II наук.-техн. конф. м. Київ, 12 лист. 2000 р. / НТУУ «КПІ». Київ, 2000. С.17–21.

29. Про національну безпеку України : Закон України від 21.06.2018 № 2469-VIII : станом на 5 жовт. 2025 р. URL: https://zakon.rada.gov.ua/laws/show/2469-19#Text (дата звернення: 10.04.2026).

30. Про Концепцію Національної програми інформатизації : Закон України від 04.02.1998 № 75/98-ВР : станом на 1 січ. 2022 р. URL: https://zakon.rada.gov.ua/laws/show/75/98-вр#Text (дата звернення: 10.04.2026).

31. Боднар І. Р. Інформаційна безпека як основа національної безпеки. *Механізм регулювання економіки.* 2014. Вип. 63 (№ 1). С. 68–75. URL: http://mer-journal.sumy.ua/index.php/journal/article/view/529 (дата звернення: 10.04.2026).

32. Цимбал П. В., Лисеюк А. М. Поняття та сутність публічно-правової охорони інформаційної безпеки. *Європейський правничий часопис.* 2023. № 1. С. 21–26. URL: https://doi.org/10.36919/ELJ.1.2023.21 (дата звернення: 10.04.2026).

33. Ткачук Т. Ю. Забезпечення інформаційної безпеки в умовах євроінтеграції України : дис. ... д-ра юрид. наук : 12.00.07. Ужгород, 2019. 487 с.

34. Золотар О. О. Інформаційна безпека людини: теорія і практика : монографія. Київ : ТОВ «Видавничий дім «АртЕк», 2018. 446 с.

35. Корж І. Ф. Внутрішні фактори загроз і викликів інформаційній безпеці України. *Запобігання новим викликам та загрозам інформаційній безпеці*

України: правові аспекти : матеріали наук.-практ. конф., м. Київ, 06 жовт. 2016 р. / «КПІ імені Ігоря Сікорського». Київ, 2016. 204 с.

36. Шопіна І. М. Поняття інформаційної безпеки: концептуальні підходи до визначення. *Науково-інформаційний вісник Івано-Франківського університету імені Короля Данила Галицького*. 2022. Вип. 25 (№ 13). С. 133–140. URL: https://doi.org/10.33098/2078-6670.2022.13.25 (дата звернення: 10.04.2026).

37. Kuniev Y., Sopilko I., Kolpakov V. Object and subject of information law. *Journal of law and political sciences scientific and academy journal*. 2020. Vol. 23. Issue 2. P. 9–41. URL: https://files.znu.edu.ua/files/WOS/0045578.pdf (дата звернення: 10.04.2026).

38. Великий тлумачний словник сучасної української мови / уклад. і голов. ред. В.Т. Бусел. Київ; Ірпінь: ВТФ «Перун», 2005. 1728 с.

39. Предборський В. А. Економічна безпека держави : монографія. Київ : Кондор, 2005. 391 с.

40. Правові засади інформаційної безпеки України : монографія / П.Д. Біленчук та ін. Харків : НУЦЗ України, 2018. 289 с.

41. Тихомиров О. О. Забезпечення інформаційної безпеки як функція сучасної держави : монографія / за ред. Р. А. Калюжний. Київ : НА СБ України, 2014. 196 с.

42. Ліпкан В. А., Максименко Ю. Є., Желіховський В.М. Інформаційна безпека України в умовах євроінтеграції : навч. посіб. Київ : КНТ, 2006. 280 с.

43. Нашинець-Наумова А. Ю. Інформаційна безпека: питання правового регулювання : монографія. Київ : Гельветика, 2017. 168 с.

44. Перун Т. С. Адміністративно-правовий механізм забезпечення інформаційної безпеки в Україні : дис. … канд. юрид. наук : 12.00.07. Львів, 2019. 268 с.

45. Бондаренко Р. В. Інформаційна безпека держави. *Інвестиції: практика та досвід.* 2021. № 5. С. 95–101. URL: https://doi.org/10.32702/2306-6814.2021.5.95 (дата звернення: 10.04.2026).

46. 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 : станом на 7 січ. 2025 р. URL: https://zakon.rada.gov.ua/laws/show/392/2020#Text (дата звернення: 10.04.2026).

47. Про рішення Ради національної безпеки і оборони України від 29 грудня 2016 року «Про Доктрину інформаційної безпеки України» : Указ Президента України від 25.02.2017 № 47/2017 : станом на 30 груд. 2021 р. URL: https://zakon.rada.gov.ua/laws/show/47/2017#Text (дата звернення: 10.04.2026).

48. Філософський енциклопедичний словник / наук. ред.: Л. В. Озадовська, Н. П. Поліщук. Київ : Абрис, 2002. 751 с.

49. Литвинов О. М. Соціально-правовий механізм протидії злочинності в Україні: дис. … д-ра юрид. наук : 12.00.08. Харків, 2010. 432 с.

50. Крук С. І. Методологія побудови інституційних механізмів державного управління у сфері національної безпеки. *Вчені записки Таврійського національного університету імені В.І. Вернадського. Серія: Державне управління.* 2018. Т. 29(68), № 6. С. 8–11. URL: http://nbuv.gov.ua/UJRN/sntvupa_2018_29%2868%29_6_4 (дата звернення: 10.04.2026).

51. Фуртак І. І. Механізм державного управління у сфері охорони здоров'я в контексті європейської інтеграції України: дис. … канд. юрид. наук : 25.00.02. Львів, 2009. 245 с.

52. Радченко О. В. Категорія «механізм» у системі державного управління. *Державне управління та місцеве самоврядування*. 2001. № 2. С. 64–69. URL: http://pa.stateandregions.zp.ua/archive/3_2009/14.pdf (дата звернення: 10.04.2026).

53. Нижник Н. Р., Машков О. А. Системний підхід в організації державного управління: навч. посіб. Київ: УАДУ, 1998. 160 с.

54. Петрова С. В. Механізми забезпечення мотивації працівників у системі охорони здоров'я: державно-управлінський аспект: дис. … канд. наук з держ. упр. : 25.00.02. Одеса, 2010. 220 с.

55. Скакун О. Ф. Теорія держави і права: підручник. 2-ге вид. Київ: Алерта; КНТ; ЦУЛ, 2010. 520 с.

56. Теорія держави і права. Академічний курс: підручник / О. В. Зайчук та ін. Київ: Юрінком Інтер, 2006. 685 с.

57. Теорія держави і права : навч. посіб. / А. М. Колодій та ін. Київ : Юрінком Інтер, 2004. 368 с.

58. Рубан А. В., Шведун В. О. Теоретико-прикладні засади державного управління у сфері національної безпеки: монографія. Харків : НУЦЗУ, 2023. 152 с.

59. Кормич Б. А. Інформаційне право : підручник. Харків : Бурун і К., 2011. 334 с.

60. Економіка та економічна безпека держави. Теорія та практика : навч. посіб. / С. В. Давиденко та ін. Ужгород : РІК-У, 2017. 388 с.

61. Ткачова Н. М. Механізми державного регулювання економічної безпеки регіону : автореф. дис. … канд. наук з держ. упр. : 25.00.02. Запоріжжя, 2009. 40 с.

62. Kulinska A. The mechanism for ensuring the national security of Ukraine as an object of targeted impact management. *Economics: time realities.* 2021. Vol. 1, no. 53. P. 75–83. URL: https://doi.org/10.15276/etr.01.2021.8 (дата звернення: 10.04.2026).

63. Зозуля О. С. Державне управління забезпеченням інформаційної безпеки України в умовах інформаційно-психологічного протиборства : дис. ... канд. наук з держ. упр. : 25.00.01. Київ : НАДУ, 2017. 251 с.

64. Шемчук В. В. Механізм забезпечення інформаційної безпеки держави: теоретично-методологічні основи. *Філософські та методологічні проблеми права*. 2019. № 1. С. 51–59. URL: https://elar.navs.edu.ua/jspui/handle/123456789/18709 (дата звернення: 10.04.2026).

65. Швець С. В., Швець У. С. Основи системного аналізу: навчальний посібник. Суми: Сумський державний університет, 2017. 126 с.

66. Євдоченко Л. О. Удосконалення системи державного забезпечення інформаційної безпеки України в умовах глобалізації : автореф. дис. ... канд. наук з держ. упр. : 25.00.01. Львів, 2011. 20 с.

67. Лісовська Ю. П. Інформаційна безпека України: навч. посіб. Київ: Видавничий дім «Кондор», 2021. 172 с.

68. Ситник Г. П. Державне управління у сфері національної безпеки (концептуальні та організаційно-правові засади) : підручник. Київ : НАДУ, 2012. 544 с.

69. Малиновський В. Я. Державне управління : навч. посіб. Луцьк : Вежа, 2000. 558 с.

70. Державне управління : проблеми адміністративно-правової теорії та практики / В. Б. Авер'янов та ін. Київ : Факт, 2003. 384 с.

71. Адміністративне право України : підручник / Ю. П. Битяк та ін. Київ : Юрінком Інтер, 2005. 544 с.

72. Крестовська Н. М., Матвєєва Л. Г. Теорія держави і права: Елементарний курс. 3-тє вид. Київ : Юрінком Інтер, 2023. 584 с.

73. Томашкова К. Т. Механізм державного управління економічною безпекою особистості : автореф. дис. … канд. наук з держ. упр. : 25.00.02. Донецьк, 2009. 20 с.

74. Котковський В. Р. Державне регулювання економічної безпеки в Україні : автореф. дис. на здобуття наук. ступеня канд. наук з держ. упр. : 25.00.02. Запоріжжя, 2007. 20 с.

75. Державне управління : навч. посіб. / А. Ф. Мельник та ін. Київ : Знання-Прес, 2003. 343 с.

76. Присяжнюк А. Й. Адміністративно-правовий механізм забезпечення економічної безпеки держави. *Форум права* : *електрон. наук. фах. вид*. Харків, 2011. № 1. С. 808–813. URL: https://dspace.univd.edu.ua/handle/123456789/343 (дата звернення: 10.04.2026).

77. Лекарь С. І. Місце адміністративно-правового механізму забезпечення економічної безпеки держави у системі державно-правового механізму.

Адміністративне право і процес. 2013. № 1. С. 15–20. URL: http://nbuv.gov.ua/UJRN/apip_2013_1_4 (дата звернення: 10.04.2026).

78. Мельник Б. О. Адміністративно-правовий механізм забезпечення інформаційної безпеки держави в умовах воєнного стану: теоретичні та практичні аспекти. *Трансформаційні процеси безпекового середовища у воєнний час*: зб. доп. за результатами кругл. столу, м. Кам'янське, 20 берез. 2025 р. / ГО «Молодіжна Організація Починаючих Лідерів». Кам'янське, 2025. С. 37–41. URL: https://dspace.univd.edu.ua/items/aa6aa9ff-30f8-4f27-80e8-ee7de9957f6f (дата звернення: 10.04.2026).

79. Веселова Л. Ю. Механізм адміністративно-правового забезпечення кібербезпеки. *Науковий вісник Міжнародного гуманітарного університету. Серія «Юриспруденція».* 2020. Вип. 43. С. 56–59.

80. Кобко Є. В. Адміністративно-правовий механізм забезпечення національної безпеки держави : реф. дис. ... д-ра юрид. наук : 12.00.07. Харків, 2023. 400 с.

81. Чистоклетов Л. Г., Хитра О. Л. Поняття адміністративно-правового забезпечення та його механізму. *Вісник Національного університету «Львівська політехніка». Серія: «Юридичні науки»*. 2020. Вип. 27 (№ 3). С. 173–180. URL: https://cyberleninka.ru/article/n/ponyattya-administrativno-pravovogo-zabezpechennya-ta-yogo-mehanizmu/viewer (дата звернення: 10.04.2026).

82. Адміністративне право України (загальна частина) : навч. посіб. / О.І. Остапенко та ін. ; 2-е вид. Львів : СПОЛОМ, 2021. 616 с.

83. Keeling, D. Management in Government. London : Allen & Unwin, 1972. 216 p.

84. Оболенський О. Ю. Розвиток суспільства та публічне управління. *Вісник Національної академії державного управління при Президентові України*. 2013. № 3. С. 27–33.

85. Модернізація суспільного сектору економіки в умовах глобальних змін: монографія / за заг. ред. А. Ф. Мельник. Тернопіль: ТНЕУ,

2009. 528 с. URL: https://library.wunu.edu.ua/files/EVD/dumka09/Modernizacija%20Syspilnogo%20Sektary.pdf (дата звернення: 10.04.2026).

86. Мамонова В. В. Публічне управління та адміністрування: співвідношення та суб'єктний склад. *Актуальні проблеми державного управління.* 2020. Вип. 57 (№ 1). С. 29–36. URL: http://nbuv.gov.ua/UJRN/apdy_2020_1_5 (дата звернення: 10.04.2026).

87. Публічне управління: термінол. слов. / уклад.: В. С. Куйбіда, М. М. Білинська, О. М. Петроє та ін. Київ: НАДУ, 2018. 224 с. URL: https://palsg.nmu.org.ua/ua/Sci/Monograph/Публічне_управління_термінологічний%20словник_2018.pdf (дата звернення: 10.04.2026).

88. Михайловська О. В., Філіпова Н. В., Ладонько Л. С., Ткаленко Н. В. Аналіз теоретичних підходів до визначення сутності складових дефініцій публічного управління та адміністрування. *Науковий часопис «Університетські наукові записки».* 2016. Вип. 58 (№ 2). С. 241–253. URL: http://ir.stu.cn.ua/handle/123456789/12836 (дата звернення: 10.04.2026).

89. Обушна Н. І. Публічне управління як нова модель організації державного управління в Україні: теоретичний аспект. *Ефективність державного управління.* 2015. Вип. 44 (№ 1). С. 53–63. URL: http://nbuv.gov.ua/UJRN/efdu_2015_44%281%29__8 (дата звернення: 10.04.2026).

90. Pollitt, C., & Bouckaert, G. Public management reform: A comparative analysis-into the age of austerity. *Oxford University Press*. 2004. 345 p.

91. Мельник Р. С. Категорія «публічне управління» у новій інтерпретації. *Право і суспільство.* 2012. № 6. С. 95–98. URL: http://pravoisuspilstvo.org.ua/archive/2012/6_2012/19.pdf (дата звернення: 10.04.2026).

92. Марухленко О. В. Дискусії щодо поняття «публічне управління». *Вчені записки ТНУ імені В. І. Вернадського. Серія: Державне управління.* 2019. Том. 30(69), № 4. С. 9–13.

93. Нижник Н. Р. Публічна влада та управління: принципи і механізми реалізації : монографія. Чернівці: Технодрук, 2008. 432 с.

94. Адміністративне право України. Повний курс: підручник / В.В. Галунько та ін. Херсон: Олді-плюс, 2018. 446 с.

95. Мельниченко Б. Б. Публічне управління в Україні в умовах євроінтеграції: адміністративно-правовий вимір : монографія. Львів: Видавництво Львівської політехніки, 2019. 372 с.

96. Ортинський В. Л., Кісіль З. Р., Ковалів М. В. Основи управління в органах внутрішніх справ України : навч. посіб. Львів : Львівський державний університет внутрішніх справ, 2007. 190 с.

97. Константінов О. Ф. Поняття та структура суб'єктів публічного управління в Україні. *Вчені записки ТНУ імені В.І. Вернадського. Серія: Публічне управління та адміністрування.* 2024. Том. 35(74), № 4. С. 30–37. URL: https://pubadm.vernadskyjournals.in.ua/journals/2024/4_2024/7.pdf (дата звернення: 10.04.2026).

98. Про місцеве самоврядування в Україні : Закон України від 21.05.1997 № 280/97-ВР : станом на 31 жовт. 2025 р. URL: https://zakon.rada.gov.ua/laws/show/280/97-вр#Text (дата звернення: 10.04.2026).

99. Про заходи щодо впровадження Концепції адміністративної реформи в Україні : Указ Президента України від 22.07.1998 № 810/98 : станом на 28 трав. 2006 р. URL: https://zakon.rada.gov.ua/laws/show/810/98#Text (дата звернення: 10.04.2026).

100. Про забезпечення участі громадськості у формуванні та реалізації державної політики : Постанова Каб. Міністрів України від 03.11.2010 № 996 : станом на 25 берез. 2025 р. URL: https://zakon.rada.gov.ua/laws/show/996-2010-п#Text (дата звернення: 10.04.2026).

101. Взаємодія держави та інститутів громадянського суспільства : Роз'яснення М-ва юстиції України від 03.02.2011.

URL: https://zakon.rada.gov.ua/laws/show/n0018323-11#Text (дата звернення: 10.04.2026).

102. Про затвердження плану заходів до 2024 року щодо реалізації Національної стратегії сприяння розвитку громадянського суспільства в Україні на 2021-2026 роки : Розпорядж. Каб. Міністрів України від 14.02.2023 № 160-р : станом на 9 лип. 2024 р. URL: https://zakon.rada.gov.ua/laws/show/160-2023-р#Text (дата звернення: 10.04.2026).

103. Матвєєнко І. В. Типологія впливів в системі публічного управління у зарубіжних науково-прикладних підходах. *Теоретичні та прикладні питання державотворення.* 2024. № 31. URL: http://taais.oridu.odessa.ua/article/view/306533 (дата звернення: 10.04.2026).

104. Гугнін Е. А. Теоретико-соціологічна рефлексія зовнішнього впливу на соціальні системи: дис... доктора соціол. наук : 22.00.01. Запоріжжя, 2021. 502 с.

105. «В інтересах іншої держави...»: проблеми виявлення та протидії агентам впливу: аналіт. доп. / Д. В. Дубов та ін. Київ : НІСД, 2018. 48 с. URL: https://niss.gov.ua/sites/default/files/2019-05/Dopovid_Agenty_vplyvu.pdf (дата звернення: 10.04.2026).

106. Калетнік В. В. Проблеми юридичної кваліфікації діяльності агентів впливу. *Гілея: науковий вісник.* 2020. Вип. 155 (№ 4). С. 236-241. URL: http://gileya.org/index.php?ng=library&cont=long&id=223 (дата звернення: 10.04.2026).

107. Шутов Р. В. Агенти зовнішніх інформаційно-психологічних впливів в Україні: спроби загального аналізу. *Науковий часопис НПУ імені М.П. Драгоманова. Серія 22 : Політичні науки та методика викладання соціально-політичних дисциплін.* 2011. Вип. 5. С. 98–104. URL: http://nbuv.gov.ua/UJRN/Nchnpu_022_2011_5_20 (дата звернення: 10.04.2026).

108. Dikkaş M. Agent of Influence (Key Influencer). *Academia.edu*. URL: https://www.academia.edu/120369706/Agent_of_Influence_Key_Influencer (дата звернення: 10.04.2026).

109. Michel C. Foreign Agents: How American Lobbyists and Lawmakers Threaten Democracy Around the World. New York: St. Martin’s Press, 2024. 340 p.

110. Калетнік В. В. Інформаційна безпека як система суспільних відносин і об’єкт правової охорони. *Наукові праці Національного авіаційного університету. Серія: Юридичний вісник «Повітряне і космічне право»*. 2022. Вип. 65 (№ 4). С. 72-79. URL: https://doi.org/10.18372/2307-9061.65.17042 (дата звернення: 10.04.2026).

111. «Санді Таймс» (Sunday Times) проти Об’єднаного Королівства (стаття 50) : Справа Ради Європи від 06.11.1980. URL: https://zakon.rada.gov.ua/laws/show/980_164#Text (дата звернення: 10.04.2026).

112. Кодекс України про адміністративні правопорушення (статті 1 - 212-24) : Кодекс України від 07.12.1984 № 8073-X : станом на 1 верес. 2025 р. URL: https://zakon.rada.gov.ua/laws/show/80731-10#Text (дата звернення: 10.04.2026).

113. Про доступ до публічної інформації : Закон України від 13.01.2011 № 2939-VI : станом на 8 серп. 2025 р. URL: https://zakon.rada.gov.ua/laws/show/2939-17#Text (дата звернення: 10.04.2026).

114. Про медіа : Закон України від 13.12.2022 № 2849-IX : станом на 31 жовт. 2025 р. URL: https://zakon.rada.gov.ua/laws/show/2849-20#Text (дата звернення: 10.04.2026).

115. Про звернення громадян : Закон України від 02.10.1996 № 393/96-ВР : станом на 31 груд. 2023 р. URL: https://zakon.rada.gov.ua/laws/show/393/96-вр#Text (дата звернення: 10.04.2026).

116. Про громадські об’єднання : Закон України від 22.03.2012 № 4572-VI : станом на 3 верес. 2024 р. URL: https://zakon.rada.gov.ua/laws/show/4572-17#Text (дата звернення: 10.04.2026).

117. Про засади внутрішньої і зовнішньої політики : Закон України від 01.07.2010 № 2411-VI : станом на 30 серп. 2025 р. URL: https://zakon.rada.gov.ua/laws/show/2411-17#Text (дата звернення: 10.04.2026).

118. Про благодійну діяльність та благодійні організації : Закон України від 05.07.2012 № 5073-VI : станом на 3 верес. 2024 р. URL: https://zakon.rada.gov.ua/laws/show/5073-17#Text (дата звернення: 10.04.2026).

119. Про професійні спілки, їх права та гарантії діяльності : Закон України від 15.09.1999 № 1045-XIV : станом на 24 груд. 2023 р. URL: https://zakon.rada.gov.ua/laws/show/1045-14#Text (дата звернення: 10.04.2026).

120. Про організації роботодавців, їх об'єднання, права і гарантії їх діяльності : Закон України від 22.06.2012 № 5026-VI : станом на 12 верес. 2025 р. URL: https://zakon.rada.gov.ua/laws/show/5026-17#Text (дата звернення: 10.04.2026).

121. Про свободу совісті та релігійні організації : Закон України від 23.04.1991 № 987-XII : станом на 30 серп. 2025 р. URL: https://zakon.rada.gov.ua/laws/show/987-12#Text (дата звернення: 10.04.2026).

122. Про професійних творчих працівників та творчі спілки : Закон України від 07.10.1997 № 554/97-ВР : станом на 31 берез. 2023 р. URL: https://zakon.rada.gov.ua/laws/show/554/97-вр#Text (дата звернення: 10.04.2026).

123. Про органи самоорганізації населення : Закон України від 11.07.2001 № 2625-III : станом на 28 серп. 2025 р. URL: https://zakon.rada.gov.ua/laws/show/2625-14#Text (дата звернення: 10.04.2026).

124. Про затвердження Національної стратегії у сфері прав людини : Указ Президента України від 25.08.2015 № 501/2015 : станом на 26 берез. 2021 р. URL: https://zakon.rada.gov.ua/laws/show/501/2015#Text (дата звернення: 10.04.2026).

125. Про затвердження Державної стратегії регіонального розвитку на 2021-2027 роки : Постанова Каб. Міністрів України від 05.08.2020 № 695 :

станом на 19 груд. 2025 р. URL: https://zakon.rada.gov.ua/laws/show/695-2020-п#Text (дата звернення: 10.04.2026).

126. Про схвалення Концепції розвитку громадянської освіти в Україні : Розпорядж. Каб. Міністрів України від 03.10.2018 № 710-р : станом на 8 жовт. 2022 р. URL: https://zakon.rada.gov.ua/laws/show/710-2018-р#Text (дата звернення: 10.04.2026).

127. Калетнік В. В. Сучасний стан адміністративно-правового забезпечення інформаційної безпеки в Україні: теоретико-правовий аналіз. *Наукові праці Національного авіаційного університету. Серія: Юридичний вісник «Повітряне і космічне право»*. 2021. Вип. 59 (№ 2). С. 70–77. URL: https://doi.org/10.18372/2307-9061.59.15597 (дата звернення: 10.04.2026).

128. Про основні засади забезпечення кібербезпеки України : Закон України від 05.10.2017 № 2163-VIII : станом на 19 жовт. 2025 р. URL: https://zakon.rada.gov.ua/laws/show/2163-19#Text (дата звернення: 10.04.2026).

129. Про запобігання корупції : Закон України від 14.10.2014 № 1700-VII : станом на 12 верес. 2025 р. URL: https://zakon.rada.gov.ua/laws/show/1700-18#Text (дата звернення: 10.04.2026).

130. Про очищення влади : Закон України від 16.09.2014 № 1682-VII : станом на 31 берез. 2023 р. URL: https://zakon.rada.gov.ua/laws/show/1682-18#Text (дата звернення: 10.04.2026).

131. Про політичні партії в Україні : Закон України від 05.04.2001 № 2365-III : станом на 19 груд. 2024 р. URL: https://zakon.rada.gov.ua/laws/show/2365-14#Text (дата звернення: 10.04.2026).

132. Про лобіювання : Закон України від 23.02.2024 № 3606-IX : станом на 1 січ. 2025 р. URL: https://zakon.rada.gov.ua/laws/show/3606-20#Text (дата звернення: 10.04.2026).

133. Регулювання лобіювання та посилення взаємодії зі стейкхолдерами: рекомендації GRECO. *Національне агентство з питань запобігання корупції*. URL: https://nazk.gov.ua/uk/pro-nazk/regulyuvannya-lobiyuvannya-ta-posylennya-vzaemodii-zi-steykholderamy-rekomendatsii-greco/ (дата звернення: 10.04.2026).

134. Калетнік В. В. Аналіз національного законодавства в контексті протидії діяльності агентів впливу як одного з методів прихованого лобіювання. *Науковий вісник Ужгородського національного університету. Серія: Право.* 2024. Вип. 84 (№ 3). С. 115-124. URL: https://doi.org/10.24144/2307-3322.2024.84.3.18 (дата звернення: 10.04.2026).

135. Про запровадження національної системи стійкості : Рішення Ради нац. безпеки і оборони України від 20.08.2021 : станом на 29 верес. 2021 р. URL: https://zakon.rada.gov.ua/laws/show/n0065525-21#Text (дата звернення: 10.04.2026).

136. Про внесення змін до Закону України «Про судоустрій і статус суддів» та процесуальних законів щодо додаткових заходів захисту безпеки громадян : Закон України від 16.01.2014 № 721-VII : станом на 2 лют. 2014 р. URL: https://zakon.rada.gov.ua/laws/show/721-18#Text (дата звернення: 10.04.2026).

137. Калетнік В. В. Теоретичні аспекти удосконалення національного законодавства в контексті протидії деструктивній діяльності агентів впливу. *Наукові праці Національного авіаційного університету. Серія: Юридичний вісник «Повітряне і космічне право»*. 2020. Вип. 56 (№ 3). С. 81–88. URL: https://doi.org/10.18372/2307-9061.56.14895 (дата звернення: 10.04.2026).

138. Проект Закону про внесення змін до деяких законодавчих актів щодо забезпечення відкритості для суспільства інформації про фінансування діяльності громадських об’єднань та використання міжнародної технічної допомоги від 10.07.2017 № 6674. *Верховна Рада України*. URL: http://w1.c1.rada.gov.ua/pls/zweb2/webproc4_1?pf3511=62214 (дата звернення: 10.04.2026).

139. Проект Закону про внесення змін до Податкового кодексу України щодо забезпечення відкритості для суспільства інформації про фінансування діяльності громадських об’єднань та використання міжнародної технічної допомоги від 10.07.2017 № 6675. *Верховна Рада України*. URL:

http://w1.c1.rada.gov.ua/pls/zweb2/webproc4_1?pf3511=62215 (дата звернення: 10.04.2026).

140. Проект Закону про внесення змін до деяких законодавчих актів України щодо прозорості та відкритості інформації про діяльність благодійних організацій та громадських об'єднань, які отримують фінансування від іноземних держав та іноземних неурядових організацій від 20.06.2018 № 8501. *Верховна Рада України*. URL: http://w1.c1.rada.gov.ua/pls/zweb2/webproc4_1?pf3511=64255 (дата звернення: 10.04.2026).

141. Проект Закону Про внесення змін до деяких законодавчих актів України (щодо прозорості діяльності громадських об'єднань з іноземною підтримкою) від 29.05.2020 № 3564. *Верховна Рада України*. URL: https://w1.c1.rada.gov.ua/pls/zweb2/webproc4_1?pf3511=68977 (дата звернення: 10.04.2026).

142. Проект Закону про внесення змін до Податкового кодексу України щодо забезпечення оприлюднення інформації про фінансування діяльності громадських об'єднань від 27.07.2020 № 3936. *Верховна Рада України*. URL: https://w1.c1.rada.gov.ua/pls/zweb2/webproc4_1?pf3511=69609 (дата звернення: 10.04.2026).

143. Проект Постанови про Декларацію Верховної Ради України щодо необхідності вжиття заходів стосовно негайного відновлення державного суверенітету в сфері державного управління від 08.09.2021 № 6009. *Верховна Рада України*. URL: http://w1.c1.rada.gov.ua/pls/zweb2/webproc4_1?pf3511=72698 (дата звернення: 10.04.2026).

144. Стоєцький О. Суб'єкти забезпечення інформаційної безпеки України: адміністративно-правові засади. *Інформаційне право.* 2009. № 11. С. 161–164. URL: https://nasplib.isofts.kiev.ua/items/e9f5a081-1670-41f6-b2dc-d634ac58b10c (дата звернення: 10.04.2026).

145. Про перейменування Міністерства культури та стратегічних комунікацій України : Постанова Каб. Міністрів України від 29.10.2025 № 1396.

URL: https://zakon.rada.gov.ua/laws/show/1396-2025-п#Text (дата звернення: 10.04.2026).

146. Про розвідку : Закон України від 17.09.2020 № 912-IX : станом на 30 жовт. 2024 р. URL: https://zakon.rada.gov.ua/laws/show/912-20#Text (дата звернення: 10.04.2026).

147. Про Раду національної безпеки і оборони України : Закон України від 05.03.1998 № 183/98-ВР : станом на 30 серп. 2025 р. URL: https://zakon.rada.gov.ua/laws/show/183/98-вр#Text (дата звернення: 10.04.2026).

148. Про рішення Ради національної безпеки і оборони України від 11 березня 2021 року «Про створення Центру протидії дезінформації» : Указ Президента України від 19.03.2021 № 106/2021. URL: https://zakon.rada.gov.ua/laws/show/106/2021#Text (дата звернення: 10.04.2026).

149. Положення про Центр протидії дезінформації : указ Президента України від 07.05.2021 № 187/2021. URL: https://zakon.rada.gov.ua/laws/show/187/2021#Text (дата звернення: 10.04.2026).

150. Про Кабінет Міністрів України : Закон України від 27.02.2014 № 794-VII : станом на 30 серп. 2025 р. URL: https://zakon.rada.gov.ua/laws/show/794-18#Text (дата звернення: 10.04.2026).

151. Про електронні комунікації : Закон України від 16.12.2020 № 1089-IX : станом на 27 лют. 2026 р. URL: https://zakon.rada.gov.ua/laws/show/1089-20#Text (дата звернення: 10.04.2026).

152. Про рішення Ради національної безпеки і оборони України від 27 січня 2016 року «Про Стратегію кібербезпеки України» : Указ Президента України від 15.03.2016 № 96/2016 : станом на 28 серп. 2021 р. URL: https://zakon.rada.gov.ua/laws/show/96/2016#Text (дата звернення: 10.04.2026).

153. Ткачук Т. Ю. Суб'єкти забезпечення інформаційної безпеки держави. *Національний юридичний журнал: Теорія і практика.* 2017. С. 42-46. URL: http://jurnaluljuridic.in.ua/archive/2017/6/part_2/9.pdf (дата звернення: 10.04.2026).

154. Про затвердження Положення про Міністерство оборони України : Постанова Каб. Міністрів України від 26.11.2014 № 671 : станом на 24 лип. 2025

р. URL: https://zakon.rada.gov.ua/laws/show/671-2014-п#Text (дата звернення: 10.04.2026).

155. Про Положення про Генеральний штаб Збройних Сил України : Указ Президента України від 30.01.2019 № 23/2019 : станом на 7 січ. 2025 р. URL: https://zakon.rada.gov.ua/laws/show/23/2019#Text (дата звернення: 10.04.2026).

156. Про затвердження Положення про Міністерство закордонних справ України : Постанова Каб. Міністрів України від 30.03.2016 № 281 : станом на 24 серп. 2024 р. URL: https://zakon.rada.gov.ua/laws/show/281-2016-п#Text (дата звернення: 10.04.2026).

157. Про внесення змін до Положення про Міністерство цифрової трансформації України : Постанова Каб. Міністрів України від 29.04.2022 № 501. URL: https://zakon.rada.gov.ua/laws/show/501-2022-п#Text (дата звернення: 10.04.2026).

158. Про затвердження Положення про Міністерство освіти і науки України : Постанова Каб. Міністрів України від 16.10.2014 № 630 : станом на 26 листоп. 2024 р. URL: https://zakon.rada.gov.ua/laws/show/630-2014-п#Text (дата звернення: 10.04.2026).

159. Про Службу безпеки України : Закон України від 25.03.1992 № 2229-XII : станом на 31 лип. 2025 р. URL: https://zakon.rada.gov.ua/laws/show/2229-12#Text (дата звернення: 10.04.2026).

160. Про Державну службу спеціального зв’язку та захисту інформації України : Закон України від 23.02.2006 № 3475-IV : станом на 20 квіт. 2025 р. URL: https://zakon.rada.gov.ua/laws/show/3475-15#Text (дата звернення: 10.04.2026).

161. Про Національну поліцію : Закон України від 02.07.2015 № 580-VIII : станом на 12 верес. 2025 р. URL: https://zakon.rada.gov.ua/laws/show/580-19#Text (дата звернення: 10.04.2026).

162. Про Національний банк України : Закон України від 20.05.1999 № 679-XIV : станом на 28 серп. 2025 р. URL: https://zakon.rada.gov.ua/laws/show/679-14#Text (дата звернення: 10.04.2026).

163. Про затвердження Положення про Міністерство юстиції України : Постанова Каб. Міністрів України від 02.07.2014 № 228 : станом на 3 жовт. 2025 р. URL: https://zakon.rada.gov.ua/laws/show/228-2014-п#Text (дата звернення: 10.04.2026).

164. Про затвердження положень про Державну податкову службу України та Державну митну службу України : Постанова Каб. Міністрів України від 06.03.2019 № 227 : станом на 16 лип. 2025 р. URL: https://zakon.rada.gov.ua/laws/show/227-2019-п#Text (дата звернення: 10.04.2026).

165. Про затвердження Положення про Національне агентство України з питань державної служби : Постанова Каб. Міністрів України від 01.10.2014 № 500 : станом на 21 жовт. 2025 р. URL: https://zakon.rada.gov.ua/laws/show/500-2014-п#Text (дата звернення: 10.04.2026).

166. Про затвердження Положення про Державну службу фінансового моніторингу України : Постанова Каб. Міністрів України від 29.07.2015 № 537 : станом на 1 серп. 2020 р. URL: https://zakon.rada.gov.ua/laws/show/537-2015-п#Text (дата звернення: 10.04.2026).

167. Мошенець О. Ідентифікація «Борна», або Хто такі агенти іноземного впливу. *LB.ua.* URL: https://lb.ua/blog/olena_moshenets/459027_identifikatsiya_borna_abo_hto_taki.html (дата звернення: 10.04.2026).

168. The Justice Department’s New, Unprecedented Use of the Foreign Agents Registration Act. *Default*. URL: https://www.lawfareblog.com/justice-departments-new-unprecedented-use-foreign-agents-registration-act (дата звернення: 10.04.2026).

169. Agents of Foreign Governments – Title 18 U.S. Code § 951. *Eisner Gorin LLP*. URL: https://www.thefederalcriminalattorneys.com/agents-of-foreign-governments (дата звернення: 10.04.2026).

170. Schwellenbach N. Few prosecutions for unregistered foreign agents. *The Center for Public Integrity.* URL: https://publicintegrity.org/national-security/few-prosecutions-for-unregistered-foreign-agents (дата звернення: 10.04.2026).

171. Калетнік В. В. Аналіз законодавства іноземних країн та національного законодавства України в аспекті напрацювання механізмів регулювання діяльності

агентів впливу. *Visegrad Journal on Human Rights*. 2021. № 5. С. 50–58. URL: https://journal-vjhr.sk/wp-content/uploads/2021/12/VJHR_5_2021.pdf (дата звернення: 10.04.2026).

172. Foreign Influence Transparency Scheme. *Attorney-General's Department.* URL: https://www.ag.gov.au/integrity/foreign-influence-transparency-scheme (дата звернення: 10.04.2026).

173. Hurst D. Australian foreign influence register 'focused almost exclusively on China with little success', committee finds. *The Guardian.* URL: https://www.theguardian.com/australia-news/2024/mar/27/australian-foreign-influence-register-china (дата звернення: 10.04.2026).

174. Resetting the deck: revisiting Australia's foreign influence transparency laws. *Bird & Bird / International Law Firm*. URL: https://www.twobirds.com/en/insights/2022/australia/revisiting-australia's-foreign-influence-transparency-laws (дата звернення: 10.04.2026).

175. UK Foreign Influence Registration Scheme Launches on 1 July 2025. *Covington & Burling LLP*. URL: https://www.cov.com/en/news-and-insights/insights/2025/04/uk-foreign-influence-registration-scheme-launches-on-1-july-2025 (дата звернення: 10.04.2026).

176. How to comply with the new Foreign Influence Registration Scheme. *The University of Sussex*. URL: https://staff.sussex.ac.uk/news/article/68649-how-to-comply-with-the-new-foreign-influence-registration-scheme (дата звернення: 10.04.2026).

177. The UK Foreign Influence Registration Scheme – What You Need to Know. *Skadden.* URL: https://www.skadden.com/insights/publications/2025/04/the-uk-foreign-influence-registration-scheme (дата звернення: 10.04.2026).

178. Levine A., Marques E. Bill C-70's New Foreign Influence Registry to Impose Heavy Compliance Burden. *Blakes.* URL: https://www.blakes.com/insights/new-foreign-influence-registry-to-impose-heavy-compliance-burden (дата звернення: 10.04.2026).

179. Zaia R. Canada's foreign agent registry is in limbo: Here's the latest. *Gowling WLG.* URL: https://gowlingwlg.com/en/insights-resources/articles/2025/canadas-foreign-agent-registry (дата звернення: 10.04.2026).

180. Deutsche Welle. Hungary to revoke 2017 anti-NGO law after EU court rebuke. *DW.* URL: https://www.dw.com/en/hungary-to-revoke-2017-anti-ngo-law-after-eu-court-rebuke/a-57282186 (дата звернення: 10.04.2026).

181. Hungary: LexNGO finally repealed but a new threat is on the horizon. *Amnesty International*. URL: https://www.amnesty.org/en/latest/press-release/2021/05/hungary-lexngo-finally-repealed-but-a-new-threat-is-on-the-horizon/ (дата звернення: 10.04.2026).

182. Мельник Р. В Угорщині прийняли аналог російського закону про «іноагентів». *detector. media.* URL: https://detector.media/infospace/article/220527/2023-12-13-v-ugorshchyni-pryynyaly-analog-rosiyskogo-zakonu-pro-inoagentiv/ (дата звернення: 10.04.2026).

183. Hungary ruling party drafts bill to crack down on foreign-funded organisations. *Reuters*. URL: https://www.reuters.com/world/europe/hungary-ruling-party-drafts-bill-crack-down-foreign-funded-organisations-2025-05-14/ (дата звернення: 10.04.2026).

184. Пиріг В. Сейм Польщі ухвалив закон про обмеження частки іноземців у власності ЗМІ. *ZAXID.NET*. URL: https://zaxid.net/seym_polshhi_uhvaliv_zakon_pro_chastkovu_zaboronu_inozemtsyam_voloditi_zmi_n1524124 (дата звернення: 10.04.2026).

185. Губенко Д. Сенат Польщі відхилив спірний закон про телерадіомовлення. *DW.* URL: https://p.dw.com/p/408rp (дата звернення: 10.04.2026).

186. Review of Lithuania's National Agenda on the Prevention of Corruption: Strengthening Public Sector Integrity Strategies. *OECD Publishing*, URL: https://doi.org/10.1787/e6efed26-en (дата звернення: 10.04.2026).

187. Lithuania's Experience in Combating Hybrid Threats. *GLOBSEC Policy Report*. URL: https://www.globsec.org/sites/default/files/2023-

02/Lithuania's%20Experience%20in%20Combating%20Hybrid%20Threats%20v2%20web.pdf (дата звернення: 10.04.2026).

188. The Act on the Openness of Government Activities (621/1999). *Finlex.* URL: http://www.finlex.fi/en/laki/kaannokset/1999/ (дата звернення: 10.04.2026).

189. Front page – Transparency register. *Etusivu – Avoimuusrekisteri*. URL: https://www.avoimuusrekisteri.fi/en (дата звернення: 10.04.2026).

190. Finland. Media Councils in the Digital Age (MCDA). *PressCouncils.eu.* URL: https://www.presscouncils.eu/codes/19_fi/ (дата звернення: 10.04.2026).

191. Finland applauds and supports press freedom and its role in democracy. *thisisFINLAND*. URL: https://finland.fi/life-society/finland-applauds-and-supports-press-freedom-and-its-role-in-democracy/ (дата звернення: 10.04.2026).

192. Prévenir les ingérences étrangères en France. *Assemblée nationale*. URL: https://www.assemblee-nationale.fr/dyn/16/dossiers/prevenir_ingerences_etrangeres_France (дата звернення: 10.04.2026).

193. Duverger F. Lutter contre les ingérences étrangères envers le système démocratique Analyse comparée des lois française et hongroise. *Revuedlf.* URL : https://revuedlf.com/droit-constitutionnel/lutter-contre-les-ingerences-etrangeres-envers-le-systeme-democratique-analyse-comparee-des-lois-francaise-et-hongroise/ (дата звернення: 10.04.2026).

194. Defending the Vote: France Acts to Combat Foreign Disinformation, 2021 – 2022. *Successful Societies.* URL: https://successfulsocieties.princeton.edu/publications/defending-vote-france-acts-combat-foreign-disinformation-2021-–-2022 (дата звернення: 10.04.2026).

195. Скібіцька Ю. Держдума РФ ухвалила закон про визнання ЗМІ іноземними агентами: що це означає?. *Hromadske.* 2017. URL: https://hromadske.ua/posts/derzhduma-rf-ukhvalyla-zakon-pro-vyznannia-zmi-inozemnymy-ahentamy (дата звернення: 10.04.2026).

196. У Росії набрав чинності закон, що дозволяє масово оголошувати людей «іноагентами». *Радіо Свобода.* URL: https://www.radiosvoboda.org/a/news-rosia-inoahenty/32157473.html (дата звернення: 10.04.2026).

197. Федоров М. Держдума РФ посилює кримінальне переслідування «іноагентів». *DW.* URL: https://www.dw.com/uk/u-rosii-posiluut-kriminalne-peresliduvanna-inoagentiv/a-73296570 (дата звернення: 10.04.2026).

198. Shah S., Runey M. Democracy Notes Explainer: What is democratic resilience? *International IDEA*. URL: https://www.idea.int/blog/democracy-notes-explainer-what-democratic-resilience (дата звернення: 10.04.2026).

199. Буряченко А. Є., Служенко А. Ю. Скорингова модель для оцінки ризиків фінансових злочинів. *Економіка та суспільство*. 2024. Вип. 68. URL: https://doi.org/10.32782/2524-0072/2024-68-66 (дата звернення: 10.04.2026).

200. Справа «Класс та інші проти Німеччини» : Справа Ради Європи від 06.09.1978. URL: https://zakon.rada.gov.ua/laws/show/980_093#Text (дата звернення: 10.04.2026).

ДОДАТКИ

Додаток А

СПИСОК ПРАЦЬ, ОПУБЛІКОВАНИХ ЗА ТЕМОЮ ДИСЕРТАЦІЇ

у наукових фахових виданнях України:

1. Калетнік В. В. Теоретичні аспекти удосконалення національного законодавства в контексті протидії деструктивній діяльності агентів впливу. *Наукові праці Національного авіаційного університету. Серія: Юридичний вісник «Повітряне і космічне право»*. 2020. Вип. 56 (№ 3). С. 81–88. URL: https://doi.org/10.18372/2307-9061.56.14895.

2. Калетнік В. В. Сучасний стан адміністративно-правового забезпечення інформаційної безпеки в Україні: теоретико-правовий аналіз. *Наукові праці Національного авіаційного університету. Серія: Юридичний вісник «Повітряне і космічне право»*. 2021. Вип. 59 (№ 2). С. 70–77. URL: https://doi.org/10.18372/2307-9061.59.15597.

3. Калетнік В. В. Інформаційна безпека як система суспільних відносин і об'єкт правової охорони. *Наукові праці Національного авіаційного університету. Серія: Юридичний вісник «Повітряне і космічне право»*. 2022. Вип. 65 (№ 4). С. 72–79. URL: https://doi.org/10.18372/2307-9061.65.17042.

4. Калетнік В. В. Аналіз національного законодавства в контексті протидії діяльності агентів впливу як одного з методів прихованого лобіювання. *Науковий вісник Ужгородського національного університету. Серія: Право.* 2024. Вип. 84 (№ 3). С. 115–124. URL: https://doi.org/10.24144/2307-3322.2024.84.3.18.

в інших наукових виданнях України:

5. Калетнік В. В. Проблема правового забезпечення в контексті протидії «активним заходам». *Гілея: науковий вісник.* 2020. Вип. 154 (№ 3). С. 269–275. ISSN 2076–1554. URL: http://gileya.org/index.php?ng=library&cont=long&id=222

6. Калетнік В. В. Проблеми юридичної кваліфікації діяльності агентів впливу. *Гілея: науковий вісник.* 2020. Вип. 155 (№ 4). С. 236–241. ISSN 2076–1554. URL: http://gileya.org/index.php?ng=library&cont=long&id=223.

7. Калетнік В. В., Калетнік Н. В. Інформаційна безпека і кіберзахист як сучасна інтелектуальна зброя. *Молодий вчений.* 2021. Вип. 93 (№ 5). С. 305–311. URL: https://doi.org/10.32839/2304-5809/2021-5-93-58.

8. Калетнік В. В., Калетнік Н. В. Кібератаки як ключові елементи «інформаційної війни» Російської Федерації. *Молодий вчений*. 2022. Вип. 101 (№ 1). С. 37–42. URL: https://doi.org/10.32839/2304-5809/2022-1-101-8.

у виданнях інших країн:

9. Калетнік В. В. Аналіз законодавства іноземних країн та національного законодавства України в аспекті напрацювання механізмів регулювання діяльності агентів впливу. *Visegrad Journal on Human Rights*. 2021. № 5. С. 50–58. ISSN 1339-7915. URL: https://journal-vjhr.sk/wp-content/uploads/2021/12/VJHR_5_2021.pdf.

у колективній монографії:

10. Калетнік В. В. Аналіз та шляхи вдосконалення нормативно-правового поля України в контексті забезпечення правових основ протидії агентам впливу. *Theoretical foundations of state and law* : монографія. Бондар В., Кузьменко І., Рудніченко С. та ін. Бостон, 2022. С. 28–33. URL: https://doi.org/10.46299/isg.2022.mono.legal.1.1.3.

наукові праці, які засвідчують апробацію дисертації:

11. Калетнік В. В. Захист прав, свобод і безпеки людини в умовах діджиталізації. *Права людини в епоху цифрових трансформацій* : матеріали XII Міжнар. наук.-практ. конф., м. Київ, 25 лют. 2022 р. / Нац. авіац. ун-т. Київ, 2022. С. 166–169. URL: https://ocs.nau.edu.ua/index.php/TL/conference/paper/view/10998/8634.

12. Калетнік В. В. Аналіз деструктивної діяльності агентів впливу в умовах широкомасштабної збройної агресії Російської Федерації проти України. *Development of Scientific Space in the Context of Global Changes* : матеріали Міжнар. наук. конф., м. Рига (Латвія), 25–26 лист. 2022 р. / Publishing House «Baltija

Publishing». Рига, 2022. С. 10–13. URL: https://doi.org/10.30525/978-9934-26-256-2-3.

13. Калетнік В. В. Вплив деструктивної діяльності агентів впливу на національну безпеку держави. *Modern Science: Global Trends, Technologies and Innovations* : тези доп. Міжнар. наук. конф., м. Рига (Латвія), 20–21 жовт. 2023 р. / Publishing House «Baltija Publishing». Рига, 2023. С. 15–19. URL: https://doi.org/10.30525/978-9934-26-354-5-5.

14. Калетнік В. В. Поняття і характеристика адміністративно-правового механізму забезпечення інформаційної безпеки України. *Забезпечення стійкості системи публічної влади та управління в умовах спеціальних адміністративно-правових режимів та відновлення України* : матеріали II Міжнар. наук.-практ. конф., м. Одеса, 17 трав. 2024 р. / Одеська політехніка. Одеса, 2024. С. 480–483. URL: https://op.edu.ua/sites/default/files/publicFiles/studolympconf/mizh_nauk_prak_konf_17.05.2024.pdf

15. Калетнік В. В. Заходи антиукраїнського інформаційного впливу Російської Федерації: механізми, наративи, протидія. *Science in the context of current challenges: from theory to practice* : тези доп. Міжнар. наук. конф., м. Рига (Латвія), 9-10 трав. 2025 р. / Publishing House «Baltija Publishing». Рига, 2025. С. 88–92. URL: https://doi.org/10.30525/978-9934-26-568-6-25.

Додаток Б

ГЛОСАРІЙ

АДМІНІСТРАТИВНО-ПРАВОВИЙ МЕХАНІЗМ ЗАБЕЗПЕЧЕННЯ ІНФОРМАЦІЙНОЇ БЕЗПЕКИ ДЕРЖАВИ – підсистема державного управління, що через норми права, діяльність уповноважених інституцій та застосування адміністративних інструментів (дозвільних, реєстраційних, контрольних, примусових) забезпечує захист від внутрішніх і зовнішніх загроз та створює умови для сталого розвитку національного інформаційного простору *(Адміністративно-правову природу механізму обґрунтовано у підрозділі 1.2, с. 63–67).*

АФІЛІЙОВАНИЙ СУБ'ЄКТ – фізична або юридична особа, що формально діє в межах правового поля України, але перебуває у стійкому фінансовому, організаційному, професійному, інформаційному чи іншому зв'язку з іноземним суб'єктом, що зумовлює фактичну залежність такої особи від нього або її підзвітність такому суб'єкту *(Правовий статус суб'єкта визначено у підрозділі 1.3, с. 86; методику ідентифікації афілійованості на основі ризик-скорингу розроблено у підрозділі 3.1, с. 146–148).*

ЗАБЕЗПЕЧЕННЯ ІНФОРМАЦІЙНОЇ БЕЗПЕКИ ДЕРЖАВИ – складова інформаційної діяльності на всіх рівнях і сферах, що реалізується як постійний процес організованої діяльності державних інституцій та суспільства, спрямований на проактивне виявлення, запобігання та нейтралізацію реальних і потенційних загроз шляхом вжиття комплексних заходів інформаційного впливу та захисту, створення ефективної системи моніторингу, контролю та управління ризиками, що забезпечує стабільне функціонування національного інформаційного простору у довгостроковій перспективі *(Теоретико-правову характеристику діяльності щодо забезпечення інформаційної безпеки розкрито у підрозділах 1.1, 1.2, с. 49, 52–56).*

ЗОВНІШНІЙ ВПЛИВ НА ПУБЛІЧНЕ УПРАВЛІННЯ – це цілеспрямована діяльність іноземного чи афілійованого з ним суб'єкта, що

полягає у прихованому або позапроцесуальному втручанні у процеси формування, обігу та інтерпретації інформації, прийняття управлінських рішень чи визначення порядку денного публічної політики, з метою зміни її змісту або результатів на користь іноземних суб'єктів *(Адміністративно-правову природу явища та алгоритм його ідентифікації обґрунтовано у підрозділах 1.3, 3.1, с. 85, 143–148).*

ІНСТИТУЦІЙНО-ПРОЦЕДУРНА ДЕФОРМАЦІЯ УПРАВЛІНСЬКИХ ПРОЦЕСІВ – це системне викривлення нормативно визначеного порядку здійснення публічного управління, зумовлене цілеспрямованим або опосередкованим впливом зовнішніх чи афілійованих суб'єктів на умови формування та ухвалення управлінських рішень, яке проявляється у порушенні автономності та послідовності управлінських процедур, зміні управлінського порядку денного, зсуві пріоритетів публічної політики або підміні публічного інтересу інтересами суб'єктів впливу й у сукупності створює загрозу суверенітету публічного управління як фундаментальній умові забезпечення інформаційної безпеки держави *(Авторську категорію введено та обґрунтовано у підрозділі 1.3, с. 83; дефіцити регулювання процесу проаналізовано у підрозділі 2.1.1, с. 92–101).*

ІНОЗЕМНИЙ СУБ'ЄКТ – іноземна держава, її органи, міжнародна або іноземна організація, група осіб чи інша структура, яка не входить до системи публічного управління України та реалізує власні інтереси у взаємодії з її інституціями *(Критерії виокремлення та правовий статус суб'єкта визначено у підрозділі 1.3, с. 85).*

ІНФОРМАЦІЙНА БЕЗПЕКА ДЕРЖАВИ – нормативно закріплений стан захищеності національного інформаційного простору, за якого забезпечується: стійкість інформаційної інфраструктури та цілісність інформаційних ресурсів; стабільність інформаційних процесів і захист прав суб'єктів інформаційних відносин; збереження національної ідентичності; реалізація національних інтересів і досягнення стратегічних цілей в інформаційній сфері; створення умов для сталого розвитку інформаційного

суспільства *(Наукове обґрунтування комплексного підходу до дефініції наведено у підрозділі 1.1, с. 48).*

МЕХАНІЗМ ЗАБЕЗПЕЧЕННЯ ІНФОРМАЦІЙНОЇ БЕЗПЕКИ ДЕРЖАВИ – системно впорядковану сукупність правових, організаційних, технічних та соціальних засобів, за допомогою яких уповноважені суб'єкти реалізують цілеспрямовану діяльність з: охорони інформаційного суверенітету (захист критичної інфраструктури, державних інформаційних ресурсів); протидії загрозам (кібератаки, дезінформація, зовнішній вплив, шпигунство); управління ризиками (моніторинг, прогнозування, адаптація до нових викликів); забезпечення стабільності інформаційного середовища *(Сутність та функціональне призначення механізму розкрито у підрозділі 1.2, с. 56–56).*

ПУБЛІЧНЕ УПРАВЛІННЯ – діяльність суб'єктів державного управління, місцевого самоврядування та інших залучених інституцій щодо формування та реалізації публічної політики в інтересах суспільства та держави *(Комбінований підхід до визначення категорії розкрито у підрозділі 1.3, с. 78).*

СИСТЕМА ПУБЛІЧНОГО УПРАВЛІННЯ – цілісне багаторівневе утворення, яке об'єднує суб'єкти державного управління та місцевого самоврядування, залучені інституції, управлінські процедури, механізми впливу та інформаційні потоки, взаємопов'язані системоутворюючими зв'язками *(Архітектуру системи та взаємодію її рівнів обґрунтовано у підрозділі 1.3, с. 78–80).*

СУВЕРЕНІТЕТ ПУБЛІЧНОГО УПРАВЛІННЯ – це здатність системи публічного управління самостійно, без зовнішнього детермінування, формувати управлінський порядок денний, ухвалювати та реалізовувати рішення відповідно до публічних інтересів у межах установлених правових процедур *(Концептуальні засади захисту суверенітету публічного управління розкрито у підрозділі 1.3, с. 84).*

Додаток В

АНКЕТА
для експертного визначення вагових коефіцієнтів критеріїв адміністративно-правової значущості зовнішнього впливу на публічне управління

Загальні положення

Метою опитування є визначення відносної адміністративно-правової значущості критеріїв, що використовуються для ризик-орієнтованої ідентифікації зовнішнього впливу на процеси публічного управління.

Опитування не має карального характеру, не спрямоване на ідентифікацію конкретних осіб і використовується виключно для аналітичного та методологічного моделювання.

Отримані результати будуть узагальнені з використанням:

процедури зваженого ранжування;

коефіцієнта конкордації Кендалла (W) для перевірки узгодженості експертних суджень.

БЛОК І. СОЦІАЛЬНО-ПРОФЕСІЙНИЙ ПРОФІЛЬ ЕКСПЕРТА

(заповнюється анонімно; використовується виключно для опису вибірки)

1. Вік:

☐ до 30 років

☐ 31–40 років

☐ 41–50 років

☐ понад 50 років

2. Стать:

☐ Жіноча

☐ Чоловіча

☐ Відмова від відповіді

3. Сфера професійної діяльності (можливо кілька варіантів):

☐ Аналітика публічної політики

☐ Громадянська освіта

☐ Виборчий моніторинг

☐ Прозорість та підзвітність влади

☐ Інше (вказати) _____

4. Загальний досвід професійної діяльності у сфері публічного управління / ІГС:

☐ до 5 років

☐ 5–10 років

☐ понад 10 років

5. Досвід участі у:

☐ аналітичних дослідженнях

☐ експертних опитуваннях

☐ підготовці рекомендацій для органів влади

(можливо кілька варіантів)

БЛОК ІІ. ОЦІНКА ЗНАЧУЩОСТІ КРИТЕРІЇВ

(основний аналітичний блок)

Інструкція

Просимо розподілити 100 балів між наведеними нижче критеріями залежно від їхньої адміністративно-правової значущості для ідентифікації юридично релевантного зовнішнього впливу на публічне управління.

Чим вищий бал, тим більше значення Ви надаєте критерію.

Сума балів обов'язково має дорівнювати 100 (крок 5).

Таблиця експертного оцінювання

№ з/п	Критерій	Зміст критерію	Вага (бали)
1.	Сфера впливу	Кадрова, нормативна, інформаційна, експертна	____
2.	Інтенсивність впливу	Разовий або системний характер	____
3.	Прихованість впливу	Відкрита або латентна форма	____
4.	Афілійованість суб'єктів	Пряма чи опосередкована	____
5.	Потенційна шкода	Управлінська, інформаційна, репутаційна	____
	Разом		**100**

БЛОК ІІІ. КОНТРОЛЬНІ ПИТАННЯ

(для підвищення валідності оцінок)

6. Який критерій, на Вашу думку, є ключовим для відмежування легітимної участі від ризикового зовнішнього впливу?

☐ Сфера впливу

☐ Інтенсивність

☐ Прихованість

☐ Афілійованість

☐ Потенційна шкода

7. Чи погоджуєтеся Ви з тим, що висока прихованість впливу може бути більш юридично значущою, ніж обсяг залучених ресурсів?

☐ Так

☐ Скоріше так

☐ Скоріше ні

☐ Ні

8. Чи достатньо, на Вашу думку, п’яти критеріїв для первинної адміністративно-правової оцінки ризику зовнішнього впливу?

☐ Так

☐ Ні (вказати, який критерій варто додати) _____

Заключна частина

Дякуємо за участь в експертному опитуванні.

Ваші відповіді є важливим елементом формування формалізованої, пропорційної та правової визначеної моделі оцінки ризиків зовнішнього впливу на публічне управління.

ІНДИВІДУАЛЬНІ ОЦІНКИ ЕКСПЕРТІВ
(вагові коефіцієнти критеріїв адміністративно-правової значущості)

Експерти	Сфера впливу	Інтенсивність	Прихованість	Афілійованість	Потенційна шкода
E1	25	15	30	20	10
E2	30	20	20	20	10
E3	20	25	25	20	10
E4	25	20	30	15	10
E5	30	15	25	25	5
E6	20	25	35	15	5
E7	25	20	25	20	10
E8	20	30	25	15	10
E9	35	15	20	20	10
E10	25	20	25	20	10
E11	25	25	20	20	10
E12	20	20	30	20	10
E13	30	15	25	20	10
E14	25	20	25	25	5
E15	20	15	30	20	15
E16	25	20	25	20	10
E17	30	20	20	20	10
E18	25	25	15	25	10
Середнє	**25,0**	**20,0**	**25,0**	**19,7**	**9,7**

Примітки:

З метою методичної чіткості показники були заокруглені до цілих значень, що дозволило сформувати вагові коефіцієнти, наведені у табл. 3.1.1 дисертації.

Коефіцієнт конкордації Кендалла становить W = 0,72, що свідчить про достатній рівень узгодженості експертних оцінок і дозволяє використовувати усереднені значення у подальшому адміністративно-правовому моделюванні.

Додаток Г

АНКЕТА
для експертного визначення коефіцієнтів доказової ваги індикаторів афілійованості

Загальні положення

Метою опитування є визначення відносної доказової значущості індикаторів, що використовуються для виявлення прямої або опосередкованої афілійованості суб'єктів публічного управління в контексті ризиків зовнішнього впливу.

Опитування не має карального характеру, не спрямоване на ідентифікацію конкретних осіб і використовується виключно для аналітичного та методологічного моделювання.

Отримані результати будуть узагальнені з використанням:

процедури зваженого ранжування;

коефіцієнта конкордації Кендалла (W) для перевірки узгодженості експертних суджень.

БЛОК І. СОЦІАЛЬНО-ПРОФЕСІЙНИЙ ПРОФІЛЬ ЕКСПЕРТА

(заповнюється анонімно; використовується виключно для опису вибірки)

1. Вік:

☐ до 30 років

☐ 31–40 років

☐ 41–50 років

☐ понад 50 років

2. Стать:

☐ Жіноча

☐ Чоловіча

☐ Відмова від відповіді

3. Сфера професійної діяльності (можливо кілька варіантів):

☐ Аналітика публічної політики

☐ Громадянська освіта

☐ Виборчий моніторинг

☐ Прозорість та підзвітність влади

☐ Інше (вказати) _____

4. Загальний досвід професійної діяльності у сфері публічного управління / ІГС:

☐ до 5 років

☐ 5–10 років

☐ понад 10 років

5. Досвід участі у:

☐ аналітичних дослідженнях

☐ експертних опитуваннях

☐ підготовці рекомендацій для органів влади

(можливо кілька варіантів)

БЛОК ІІ. ПОПАРНЕ ПОРІВНЯННЯ ІНДИКАТОРІВ

(основний аналітичний блок)

Інструкція для експерта

Просимо оцінити доказову вагу кожного індикатора афілійованості за шкалою від 0 до 1 таким чином, щоб сума всіх коефіцієнтів дорівнювала 1,00.

Таблиця експертного оцінювання

№ з/п	Індикатор	Коротка характеристика	Коефіцієнт
1.	Фінансова залежність	Отримання коштів, ресурсів, грантів	____
2.	Кадрові зв’язки	Спільна зайнятість, контракти	____
3.	Інформаційна синхронізація	Узгоджені наративи, кампанії	____
4.	Організаційна інтеграція	Участь у мережах, структурах	____
5.	Регулярність контактів	Системна комунікація	____
	Разом		**1,00**

БЛОК ІІІ. КОНТРОЛЬНЕ ПИТАННЯ

(для підвищення валідності оцінок)

6. Який індикатор, на Вашу думку, має найвищу доказову вагу при встановленні прихованої афілійованості?

☐ Фінансова залежність

☐ Кадрові зв’язки

☐ Інформаційна синхронізація

☐ Організаційна інтеграція

☐ Регулярність контактів

Заключна частина

Дякуємо за участь в експертному опитуванні.

Ваші відповіді є важливим елементом формування формалізованої, пропорційної та правової визначеної моделі оцінки ризиків зовнішнього впливу на публічне управління.

ІНДИВІДУАЛЬНІ ОЦІНКИ ЕКСПЕРТІВ
(коефіцієнти доказової ваги індикаторів афілійованості)

Експерти	Фінансова залежність	Кадрові зв'язки	Інформаційна синхронізація	Організаційна інтеграція	Регулярність контактів
E1	0,35	0,20	0,20	0,15	0,10
E2	0,25	0,30	0,25	0,10	0,10
E3	0,30	0,25	0,20	0,15	0,10
E4	0,40	0,20	0,15	0,15	0,10
E5	0,30	0,30	0,20	0,10	0,10
E6	0,35	0,25	0,20	0,15	0,05
E7	0,25	0,25	0,25	0,15	0,10
E8	0,30	0,20	0,20	0,20	0,10
E9	0,30	0,25	0,20	0,15	0,10
E10	0,35	0,25	0,15	0,15	0,10
E11	0,25	0,25	0,20	0,20	0,10
E12	0,30	0,30	0,15	0,15	0,10
E13	0,35	0,20	0,25	0,10	0,10
E14	0,25	0,25	0,20	0,20	0,10
E15	0,30	0,25	0,20	0,15	0,10
E16	0,30	0,25	0,20	0,15	0,10
E17	0,35	0,25	0,15	0,15	0,10
E18	0,25	0,30	0,25	0,10	0,10
Середнє	**0,308**	**0,250**	**0,200**	**0,144**	**0,097**

Примітки:

Після нормалізації та заокруглення зазначені показники були приведені до значень 0,30; 0,25; 0,20; 0,15; 0,10, що відображено у табл. 3.1.2.

Коефіцієнт конкордації Кендалла становив W = 0,81, що свідчить про високий рівень узгодженості експертних суджень.

Додаток Д

АНКЕТА
для експертного визначення порогових значень активації адміністративних режимів реагування

Загальні положення

Метою опитування є встановлення **порогових значень інтегрального показника ризику**, при досягненні яких доцільним є застосування відповідних адміністративних заходів.

Опитування **не має карального характеру**, не спрямоване на ідентифікацію конкретних осіб і використовується **виключно для аналітичного та методологічного моделювання**.

Отримані результати будуть узагальнені з використанням:

процедури **зваженого ранжування**;

коефіцієнта **конкордації Кендалла (W)** для перевірки узгодженості експертних суджень.

БЛОК І. СОЦІАЛЬНО-ПРОФЕСІЙНИЙ ПРОФІЛЬ ЕКСПЕРТА

(заповнюється анонімно; використовується виключно для опису вибірки)

1. Вік:

☐ до 30 років

☐ 31–40 років

☐ 41–50 років

☐ понад 50 років

2. Стать:

☐ Жіноча

☐ Чоловіча

☐ Відмова від відповіді

3. Сфера професійної діяльності (можливо кілька варіантів):

☐ Аналітика публічної політики

☐ Громадянська освіта

☐ Виборчий моніторинг

☐ Прозорість та підзвітність влади

☐ Інше (вказати) _____

4. Загальний досвід професійної діяльності у сфері публічного управління / ІГС:

☐ до 5 років

☐ 5–10 років

☐ понад 10 років

5. Досвід участі у:

☐ аналітичних дослідженнях

☐ експертних опитуваннях

☐ підготовці рекомендацій для органів влади

(можливо кілька варіантів)

БЛОК ІІ. ВИЗНАЧЕННЯ ПОРОГІВ

(основний аналітичний блок)

Інструкція

Просимо вказати значення інтегрального ризик-скорингу (від 0 до 1), починаючи з якого, на Вашу думку, доцільно:

Таблиця експертного оцінювання

№ з/п	Рівень	Значення
1.	Активація підвищених вимог до прозорості	____
2.	Запровадження спеціальної процедури	____
3.	Тимчасові процедурні обмеження	____

Контрольне питання

(для підвищення валідності оцінок)

6. Чи погоджуєтесь Ви, що застосування обмежувальних заходів можливе виключно за рішенням суду?

☐ Так

☐ Ні

ІНДИВІДУАЛЬНІ ОЦІНКИ ЕКСПЕРТІВ
(порогові значення рівнів ризику зовнішнього впливу)

Експерти	Поріг активації середнього ризику	Поріг високого ризику	Поріг критичного ризику
E1	0,30	0,60	0,85
E2	0,35	0,65	0,90
E3	0,25	0,55	0,80
E4	0,30	0,60	0,85
E5	0,40	0,70	0,90
E6	0,30	0,60	0,85
E7	0,35	0,65	0,90
E8	0,25	0,55	0,80
E9	0,30	0,60	0,85
E10	0,30	0,60	0,85
E11	0,35	0,65	0,90
E12	0,30	0,60	0,85
E13	0,40	0,70	0,90
E14	0,25	0,60	0,85
E15	0,30	0,65	0,90
E16	0,30	0,60	0,85
E17	0,35	0,65	0,80
E18	0,30	0,60	0,85
Середнє	**0,317**	**0,622**	**0,861**

Примітки:

З метою забезпечення юридичної визначеності та уніфікації правозастосування зазначені значення були заокруглені до 0,32; 0,62; 0,86, що відображено у табл. 3.1.3 дисертації.

Узгодженість експертних суджень перевірено за допомогою коефіцієнта конкордації Кендалла, який становить W = 0,76, що свідчить про високий рівень узгодженості та допустимість використання усереднених значень у подальшому моделюванні.

Додаток Е

Проєкт

ЗАКОН УКРАЇНИ

«Про протидію зовнішньому впливу на публічне управління»

Розділ І

ЗАГАЛЬНІ ПОЛОЖЕННЯ

Стаття 1. Мета і завдання Закону

1. Цей Закон визначає правові та організаційні засади протидії зовнішньому впливу на публічне управління, спрямовані на забезпечення національної стійкості, захист державного суверенітету та демократичного конституційного ладу України.

2. Метою цього Закону є забезпечення суверенітету публічного управління шляхом створення адміністративно-правових запобіжників проти прихованого або позапроцесуального втручання іноземних суб'єктів у систему прийняття управлінських рішень, встановлення прозорих процедур ідентифікації афілійованості та моніторингу зовнішнього впливу.

3. Завданнями цього Закону є:

1) забезпечення прозорості та підзвітності взаємодії суб'єктів публічного управління з іноземними та афілійованими з ними суб'єктами;

2) запобігання прихованому, маніпулятивному або деструктивному впливу на процеси формування та реалізації публічної політики;

3) розроблення та впровадження адміністративно-правових механізмів ідентифікації, моніторингу та нейтралізації зовнішнього впливу;

4) забезпечення балансу між вимогами національної безпеки у сфері публічного управління та гарантіями прав і свобод людини;

5) формування єдиного адміністративно-правового підходу до протидії зовнішньому впливу на публічне управління;

6) визначення інституційної системи протидії зовнішньому впливу та повноважень відповідних суб’єктів;

7) запровадження прозорих процедур обліку, аналізу та реагування на встановлені факти зовнішнього впливу;

8) запобігання політизації та зловживанням у сфері протидії зовнішньому впливу.

Стаття 2. Сфера дії Закону

1. Дія цього Закону поширюється на відносини, що виникають у процесі формування, ухвалення, реалізації та контролю управлінських рішень у системі публічного управління України.

2. Суб’єктами, на яких поширюється дія цього Закону, є:

1) органи державної влади та їх посадові особи;

2) органи місцевого самоврядування та їх посадові особи;

3) юридичні особи публічного права;

4) інші юридичні та фізичні особи – у частині їх участі у формуванні управлінських рішень або здійсненні впливу на публічну політику.

3. Дія цього Закону не поширюється на:

1) дипломатичну діяльність іноземних держав, що здійснюється відповідно до міжнародного права;

2) діяльність міжнародних організацій у межах міжнародних договорів України;

3) законну діяльність іноземних інвесторів у сфері господарювання, якщо вона не спрямована на вплив на управлінські рішення.

Стаття 3. Принципи протидії зовнішньому впливу на публічне управління

Протидія зовнішньому впливу на публічне управління здійснюється на основі таких принципів:

1. Верховенства права, що передбачає законність, юридичну визначеність, заборону зловживання владою, рівність перед законом і недискримінацію, ефективний доступ до правосуддя та повагу до прав і свобод людини.

2. Пропорційності, за якою будь-які заходи протидії зовнішньому впливу мають бути необхідними, обґрунтованими та співмірними встановленим ризикам.

3. Політичної нейтральності, що виключає використання механізмів протидії зовнішньому впливу в інтересах окремих політичних сил або ідеологій.

4. Інституційної підзвітності та прозорості, що забезпечує демократичний контроль за діяльністю уповноважених органів.

Застосування цього Закону не може мати наслідком криміналізацію легальної громадської, наукової, журналістської чи політичної діяльності.

Розділ ІІ
ТЕРМІНИ ТА ЇХ ВИЗНАЧЕННЯ

Стаття 4. Визначення термінів

У цьому Законі терміни вживаються в такому значенні:

1. Зовнішній вплив на публічне управління – цілеспрямована діяльність іноземного чи афілійованого з ним суб’єкта, що полягає у прихованому або позапроцесуальному втручанні у процеси формування, обігу та інтерпретації інформації, прийняття управлінських рішень чи визначення порядку денного публічної політики, з метою зміни її змісту або результатів на користь іноземних суб’єктів.

2. Іноземний суб’єкт – іноземна держава, її органи, міжнародна або іноземна організація, група осіб чи інша структура, яка не входить до системи публічного управління України та реалізує власні інтереси у взаємодії з її інституціями.

3. Афілійований суб’єкт – фізична або юридична особа, що формально діє в межах правового поля України, але перебуває у стійкому фінансовому, організаційному, професійному, інформаційному чи іншому зв’язку з іноземним суб’єктом, що зумовлює фактичну залежність такої особи від нього або її підзвітність такому суб’єкту.

4. Публічне управління – діяльність суб’єктів державного управління, місцевого самоврядування та інших залучених інституцій щодо формування та реалізації публічної політики в інтересах суспільства та держави.

5. Система публічного управління – цілісна сукупність суб’єктів державного управління, органів місцевого самоврядування, залучених інституцій громадянського суспільства та бізнес-середовища, а також управлінських процедур та інформаційних потоків, що взаємодіють між собою з метою реалізації публічної політики.

6. Суверенітет публічного управління – здатність системи публічного управління самостійно, без зовнішнього детермінування, формувати управлінський порядок денний, ухвалювати та реалізовувати рішення відповідно до публічних інтересів на підставі Конституції та законів України у межах установлених правових процедур.

7. Протидія зовнішньому впливу – система адміністративно-правових, організаційних, інформаційно-аналітичних і превентивних заходів, спрямованих на виявлення, моніторинг та нейтралізацію ризиків зовнішнього впливу.

8. Ідентифікація афілійованості – адміністративна процедура встановлення та документального підтвердження зв’язків суб’єкта з іноземними суб’єктами на підставі визначених цим Законом критеріїв.

Розділ ІІІ
СУБ’ЄКТИ ПРОТИДІЇ ЗОВНІШНЬОМУ ВПЛИВУ ТА ЇХ ПОВНОВАЖЕННЯ

Стаття 5. Система суб’єктів протидії зовнішньому впливу на публічне управління

1. Система суб’єктів протидії зовнішньому впливу на публічне управління утворюється з метою забезпечення комплексного, скоординованого та правомірного реагування на загрози інформаційній безпеці та суверенітету України у сфері публічного управління.

2. До системи суб’єктів протидії зовнішньому впливу належать:

1) Верховна Рада України – у частині законодавчого забезпечення та парламентського контролю;

2) Кабінет Міністрів України – у частині формування та реалізації державної політики у сфері протидії зовнішньому впливу;

3) Центр протидії зовнішньому впливу – центральний орган виконавчої влади, уповноважений на реалізацію державної політики у сфері протидії зовнішньому впливу;

4) інші центральні та місцеві органи виконавчої влади – у межах визначених повноважень;

5) органи місцевого самоврядування – у частині запобігання зовнішньому впливу на місцевому рівні;

6) суди – у частині здійснення судового контролю та захисту прав і свобод людини.

3. Система суб’єктів протидії зовнішньому впливу функціонує на засадах взаємодії, розмежування повноважень та недопущення концентрації надмірних дискреційних повноважень в одному органі.

Стаття 6. Центр протидії зовнішньому впливу

1. Реалізація державної політики у сфері протидії зовнішньому впливу на публічне управління покладається на Центр протидії зовнішньому впливу (далі – ЦПЗВ), який утворюється як центральний орган виконавчої влади зі спеціальним статусом.

2. ЦПЗВ є політично нейтральним, не здійснює оперативно-розшукову діяльність та діє виключно в межах адміністративних процедур, визначених цим Законом.

Стаття 7. Повноваження ЦПЗВ

1. ЦПЗВ у межах своєї компетенції:

1) здійснює інформаційно-аналітичну діяльність щодо виявлення ризиків зовнішнього впливу;

2) координує діяльність органів виконавчої влади у сфері протидії зовнішньому впливу;

3) розробляє методичні рекомендації та стандарти оцінки афілійованості;

4) здійснює ідентифікацію афілійованості та веде Реєстр афілійованих суб'єктів;

5) веде облік і формує аналітичні узагальнення без застосування репресивних заходів;

6) готує пропозиції щодо вдосконалення законодавства;

7) звертається до суду у випадках, передбачених законом;

8) готує та подає до суду матеріали щодо застосування правових наслідків відповідно до Розділу VIII цього Закону.

2. ЦПЗВ не має права:

1) самостійно визнавати особу винною у правопорушенні;

2) обмежувати права і свободи людини без рішення суду;

3) втручатися у політичну діяльність, що здійснюється в межах Конституції України.

Стаття 8. Взаємодія ЦПЗВ з іншими суб'єктами

1. ЦПЗВ взаємодіє з:

1) органами державної влади – у частині обміну інформацією та координації дій;

2) органами місцевого самоврядування – у частині запобігання впливу на місцеве управління;

3) судовими органами – у межах процедур судового контролю;

4) інститутами громадянського суспільства – у формі відкритого діалогу та консультацій.

2. Взаємодія здійснюється з дотриманням принципів:

1) законності;

2) пропорційності;

3) невтручання у незалежну діяльність суб'єктів публічного управління;

4) захисту персональних даних.

Стаття 9. Реєстр афілійованих суб’єктів

1. Реєстр афілійованих суб’єктів (далі – Реєстр) є єдиною державною інформаційною системою, що містить відомості про осіб, щодо яких у встановленому цим Законом порядку підтверджено факт афілійованості з іноземними суб’єктами з метою впливу на публічне управління.

2. Ведення Реєстру здійснюється ЦПЗВ з метою забезпечення прозорості публічного управління та інформування органів державної влади про потенційні ризики зовнішнього впливу.

3. Внесення відомостей до Реєстру здійснюється виключно на підставі:

1) добровільної заяви суб’єкта про розкриття афілійованості;

2) рішення суду, що набрало законної сили, за результатами процедури ідентифікації.

4. Відомості Реєстру є відкритими та публічними, крім випадків, передбачених законом щодо захисту державної таємниці.

5. Включення до Реєстру не тягне за собою автоматичного обмеження прав і свобод особи, а слугує інструментом забезпечення прозорості та підставою для застосування заходів, визначених Розділом VIII цього Закону.

Стаття 10. Судовий контроль у сфері протидії зовнішньому впливу

1. Рішення, дії або бездіяльність ЦПЗВ можуть бути оскаржені в судовому порядку.

2. Будь-які заходи, що можуть призвести до обмеження прав або законних інтересів фізичних чи юридичних осіб, застосовуються виключно на підставі судового рішення.

3. Судовий контроль є обов’язковим елементом механізму протидії зовнішньому впливу.

Розділ IV
НОРМАТИВНО-ПРАВОВИЙ КОМПОНЕНТ МЕХАНІЗМУ ПРОТИДІЇ ЗОВНІШНЬОМУ ВПЛИВУ НА ПУБЛІЧНЕ УПРАВЛІННЯ

Стаття 11. Нормативно-правова основа протидії зовнішньому впливу

1. Нормативно-правовий компонент механізму протидії зовнішньому впливу на публічне управління становить сукупність норм Конституції України, законів України, міжнародних договорів, згода на обов'язковість яких надана Верховною Радою України, а також підзаконних нормативно-правових актів, що регулюють відносини у сфері забезпечення інформаційної безпеки та захисту суверенітету держави.

2. Цей Закон є спеціальним законом, що визначає правові та організаційні засади протидії зовнішньому впливу на публічне управління та застосовується з урахуванням положень Конституції України.

3. Норми цього Закону не можуть тлумачитися або застосовуватися таким чином, що призводить до обмеження прав і свобод людини і громадянина інакше як на підставах, у межах повноважень та способом, визначеними Конституцією та законами України.

Стаття 12. Ієрархія та співвідношення нормативно-правових актів

1. Регулювання відносин у сфері протидії зовнішньому впливу здійснюється з дотриманням такої ієрархії нормативно-правових актів:

1) Конституція України;

2) міжнародні договори України;

3) закони України;

4) акти Кабінету Міністрів України;

5) нормативно-правові акти ЦПЗВ, прийняті в межах його компетенції.

2. Підзаконні нормативно-правові акти не можуть:

1) встановлювати нові обмеження прав і свобод людини;

2) розширювати перелік підстав втручання у публічну або приватну діяльність;

3) змінювати зміст правових понять, визначених цим Законом.

3. У разі колізії між нормами цього Закону та іншими законами України застосовуються норми цього Закону, якщо вони не суперечать Конституції України та міжнародним зобов'язанням України у сфері прав людини.

Стаття 13. Юридична визначеність та передбачуваність правового регулювання

1. Норми цього Закону та підзаконних актів, прийнятих на його виконання, повинні відповідати принципу юридичної визначеності.

2. Юридична визначеність у сфері протидії зовнішньому впливу забезпечується шляхом:

1) чіткого і вичерпного визначення правових понять і термінів;

2) встановлення зрозумілих процедур ухвалення рішень;

3) визначення строків, підстав і меж втручання держави;

4) недопущення зворотної дії норм, які погіршують становище особи.

3. Забороняється застосування оціночних понять без законодавчо визначених критеріїв.

Стаття 14. Межі нормативного регулювання та заборона зловживання владою

1. Нормативно-правовий компонент механізму протидії зовнішньому впливу не може використовуватися як інструмент політичного тиску, обмеження свободи думки, слова, наукової діяльності чи громадянської активності.

2. Забороняється:

1) встановлення колективної відповідальності;

2) застосування заходів без індивідуалізованої оцінки ризиків;

3) делегування дискреційних повноважень без визначених законом меж.

3. Будь-яке рішення, прийняте з перевищенням нормативно встановлених повноважень, є незаконним і підлягає судовому скасуванню.

Стаття 15. Співвідношення з законодавством у сфері національної безпеки та інформаційної безпеки

1. Реалізація цього Закону здійснюється у взаємодії з законодавством України у сфері:

1) національної безпеки;

2) інформаційної безпеки;

3) захисту персональних даних;

4) запобігання корупції;

5) публічної служби.

2. Положення цього Закону не замінюють і не підміняють:

1) законодавство про кримінальну відповідальність;

2) законодавство про оперативно-розшукову діяльність;

3) законодавство про санкції.

Стаття 16. Нормативне забезпечення реалізації цього Закону

1. Кабінет Міністрів України у шестимісячний строк з дня набрання чинності цим Законом:

1) забезпечує приведення своїх нормативно-правових актів у відповідність із цим Законом;

2) затверджує положення про ЦПЗВ;

3) визначає порядок міжвідомчої координації.

2. ЦПЗВ має право приймати нормативно-правові акти виключно процедурного та методичного характеру.

Розділ V
ІНФОРМАЦІЙНО-АНАЛІТИЧНИЙ КОМПОНЕНТ МЕХАНІЗМУ ПРОТИДІЇ ЗОВНІШНЬОМУ ВПЛИВУ НА ПУБЛІЧНЕ УПРАВЛІННЯ

Стаття 17. Мета та завдання інформаційно-аналітичного забезпечення

1. Інформаційно-аналітичний компонент механізму протидії зовнішньому впливу на публічне управління спрямований на:

1) виявлення, аналіз та оцінку ризиків зовнішнього впливу;

2) формування обґрунтованих управлінських рішень;

3) запобігання непропорційному або свавільному втручанню держави;

4) забезпечення доказовості заходів протидії.

2. Інформаційно-аналітична діяльність здійснюється виключно з превентивною та аналітичною метою і не є формою оперативно-розшукової або розвідувальної діяльності.

Стаття 18. Джерела інформації та межі їх використання

1. Інформаційно-аналітичне забезпечення ґрунтується на використанні:

1) відкритих джерел інформації;

2) офіційних державних реєстрів;

3) даних фінансового та антикорупційного моніторингу;

4) інформації, наданої органами державної влади в межах їх повноважень;

5) аналітичних матеріалів наукових та експертних установ.

2. Забороняється використання:

1) незаконно отриманої інформації;

2) персональних даних без законних підстав;

3) матеріалів, що не підлягають перевірці або мають оціночний характер без критеріїв.

3. Обробка інформації здійснюється з дотриманням законодавства про захист персональних даних.

Стаття 19. Аналітична оцінка ризиків зовнішнього впливу

1. Аналітична оцінка ризиків зовнішнього впливу здійснюється на підставі системи критеріїв, визначених цим Законом та затверджених у встановленому порядку.

2. Такими критеріями можуть бути:

1) наявність стійких організаційних або фінансових зв’язків з іноземними суб’єктами;

2) системність та повторюваність дій, спрямованих на вплив на управлінські рішення;

3) прихований або оманливий характер діяльності;

4) спрямованість впливу на стратегічні сфери державного управління;

5) координація дій з іноземними державними або підконтрольними їм структурами.

3. Жоден окремий критерій не може бути підставою для застосування заходів протидії без комплексної оцінки.

4. Перелік критеріїв не є автоматичною підставою для висновків про зовнішній вплив і застосовується виключно у межах процедур, визначених цим Законом.

Стаття 20. Аналітичні продукти та їх правовий статус

1. Результатами інформаційно-аналітичної діяльності є:

1) аналітичні звіти;

2) оцінки ризиків;

3) рекомендації щодо управлінських рішень;

4) інформаційні довідки.

2. Аналітичні матеріали:

1) не є автоматичною підставою для притягнення до відповідальності;

2) не мають презумпції вини;

3) підлягають перевірці та оскарженню.

3. Аналітичні продукти можуть бути використані як допоміжні матеріали у судових та адміністративних процедурах.

Стаття 21. Єдина система інформаційно-аналітичної взаємодії

1. З метою забезпечення міжвідомчої координації створюється Єдина інформаційно-аналітична система «Система інтегрованого моніторингу афілійованості» (далі – СІМА).

2. Система СІМА забезпечує:

1) обмін знеособленими аналітичними даними;

2) уникнення дублювання функцій;

3) оперативне реагування на загрози;

4) збереження цифрових слідів прийняття рішень.

3. Доступ до системи здійснюється за принципом функціональної необхідності.

Стаття 22. Гарантії об’єктивності та аналітичної доброчесності

1. Інформаційно-аналітична діяльність ґрунтується на:

1) доказовості;

2) перевірюваності джерел;

3) міждисциплінарному підході;

4) професійній незалежності аналітиків.

2. Забороняється:

1) формування аналітичних матеріалів на підставі політичних вказівок;

2) маніпулювання висновками;

3) приховування альтернативних оцінок.

3. Порушення аналітичної доброчесності тягне дисциплінарну та іншу відповідальність, передбачену законом.

Розділ VI

ПРОЦЕДУРНО-КОНТРОЛЬНИЙ КОМПОНЕНТ МЕХАНІЗМУ ПРОТИДІЇ ЗОВНІШНЬОМУ ВПЛИВУ НА ПУБЛІЧНЕ УПРАВЛІННЯ

Стаття 23. Загальні засади процедур протидії зовнішньому впливу

1. Процедури протидії зовнішньому впливу є адміністративними процедурами спеціального характеру, що здійснюються з метою:

1) виявлення фактів зовнішнього впливу;

2) перевірки наявності афілійованості;

3) запобігання деформації управлінських рішень;

4) забезпечення інформаційної безпеки держави.

2. Процедури здійснюються з дотриманням принципу верховенства права.

3. Будь-які обмежувальні заходи допускаються лише за наявності встановленої законом процедури, мотивованого рішення та можливості судового контролю.

Стаття 24. Ініціювання процедур перевірки

1. Процедура перевірки щодо можливого зовнішнього впливу може бути ініційована у разі наявності:

1) аналітичної оцінки ризиків, підготовленої відповідно до цього Закону;

2) обґрунтованого звернення органу державної влади;

3) встановлених законом сигналів ризику.

2. Забороняється ініціювання перевірки:

1) з політичних мотивів;

2) на підставі неперевірених або непідтверджених даних;

3) у формі вибіркового або дискримінаційного застосування.

3. Рішення про початок процедури має бути мотивованим, письмовим та реєстрованим.

Стаття 25. Процедура адміністративної перевірки

1. Адміністративна перевірка здійснюється у визначені законом строки та включає:

1) збір і аналіз релевантної інформації;

2) запит пояснень у заінтересованої особи;

3) оцінку наявності ознак зовнішнього впливу або афілійованості.

2. Особа, щодо якої здійснюється перевірка, має право:

1) бути поінформованою про предмет перевірки;

2) надавати пояснення та докази;

3) користуватися правовою допомогою;

4) отримати копію мотивованого рішення.

3. Забороняється застосування прихованих або примусових методів, не передбачених законом.

Стаття 26. Рішення за результатами перевірки

1. За результатами перевірки може бути ухвалене одне з таких рішень:

1) відсутність ознак зовнішнього впливу;

2) встановлення підвищеного ризику та застосування превентивних заходів;

3) встановлення факту афілійованості або зовнішнього впливу у порядку, що передбачає судове підтвердження.

2. Рішення повинно бути:

1) мотивованим;

2) пропорційним;

3) обмеженим у часі;

4) таким, що підлягає оскарженню.

3. Рішення не може ґрунтуватися виключно на аналітичному висновку без процедурної перевірки.

Стаття 27. Судовий контроль та оскарження

1. Будь-яке рішення, прийняте в межах процедур протидії зовнішньому впливу, може бути оскаржене в судовому порядку.

2. Справи щодо оскарження рішень, дій чи бездіяльності ЦПЗВ розглядаються адміністративним судом у строк, що не перевищує 15 робочих днів з дня відкриття провадження у справі.

3. Розгляд таких справ здійснюється за правилами спрощеного позовного провадження. Подання позову зупиняє дію оскаржуваного рішення до набрання судовим рішенням законної сили, крім випадків, коли зволікання створює безпосередню загрозу національній безпеці.

Стаття 28. Контроль за діяльністю ЦПЗВ

1. Контроль за дотриманням процедур здійснюється шляхом:

1) внутрішнього адміністративного контролю;

2) парламентського контролю у визначених законом формах;

3) судового контролю;

4) аудиту процедурної доброчесності.

2. Забороняється втручання у конкретні процедури з боку політичних органів.

3. Результати контролю підлягають узагальненню та оприлюдненню у знеособленому вигляді.

Стаття 29. Відповідальність за порушення процедур

1. Порушення встановлених процедур протидії зовнішньому впливу тягне:

1) дисциплінарну відповідальність;

2) адміністративну відповідальність;

3) іншу відповідальність, передбачену законом.

2. Рішення, прийняті з істотним порушенням процедур, є нікчемними або підлягають скасуванню судом.

Розділ VII

КОМУНІКАЦІЙНО-ПРЕВЕНТИВНИЙ КОМПОНЕНТ МЕХАНІЗМУ ПРОТИДІЇ ЗОВНІШНЬОМУ ВПЛИВУ НА ПУБЛІЧНЕ УПРАВЛІННЯ

Стаття 30. Мета та завдання комунікаційно-превентивного компоненту

1. Комунікаційно-превентивний компонент механізму протидії зовнішньому впливу спрямований на:

1) формування стійкості системи публічного управління до інформаційних і смислових впливів;

2) попередження виникнення умов для зовнішнього впливу;

3) підвищення обізнаності суб'єктів публічного управління щодо ризиків афілійованості;

4) забезпечення відкритості та довіри суспільства до державної політики у сфері протидії зовнішньому впливу.

2. Комунікаційно-превентивні заходи не мають карального характеру та не можуть використовуватися для обмеження свободи вираження поглядів або свободи об'єднань.

Стаття 31. Інформаційна відкритість і стратегічні комунікації

1. Держава забезпечує системне інформування суспільства про:

1) загальні загрози зовнішнього впливу без розкриття чутливої інформації;

2) цілі та принципи державної політики у цій сфері;

3) узагальнені результати діяльності ЦПЗВ.

2. Стратегічні комунікації здійснюються з дотриманням принципів:

1) достовірності;

2) пропорційності;

3) недискримінаційності;

4) поваги до прав людини.

3. Забороняється використання державних комунікацій для формування образу «внутрішнього ворога» або дискредитації законної громадської діяльності.

Стаття 32. Превентивна робота з суб’єктами публічного управління

1. З метою зниження вразливості до зовнішнього впливу держава забезпечує:

1) проведення навчальних програм для державних службовців і посадових осіб місцевого самоврядування;

2) розробку методичних рекомендацій щодо виявлення ознак зовнішнього впливу;

3) впровадження стандартів доброчесної взаємодії з іноземними та афілійованими суб’єктами.

2. Такі заходи мають рекомендаційний і освітній характер та не можуть підміняти собою контрольні або каральні процедури.

Стаття 33. Взаємодія з громадянським суспільством та експертним середовищем

1. Держава сприяє відкритому діалогу з інститутами громадянського суспільства, науковими та експертними середовищами з питань:

1) ризиків зовнішнього впливу;

2) стандартів прозорості;

3) захисту інформаційної безпеки.

2. Така взаємодія здійснюється на засадах:

1) добровільності;

2) рівності сторін;

3) невтручання у внутрішню діяльність організацій.

3. Участь у комунікаційно-превентивних заходах не може бути підставою для ініціювання перевірок або застосування обмежень.

Стаття 34. Раннє попередження та саморегуляція

1. У межах комунікаційно-превентивного компоненту запроваджуються механізми раннього попередження, що включають:

1) індикатори ризиків зовнішнього впливу;

2) рекомендації щодо добровільного розкриття афілійованості;

3) можливість попереднього консультування.

2. Добровільне розкриття інформації про потенційну афілійованість враховується як обставина, що свідчить про добросовісність суб'єкта.

Стаття 35. Заборона превентивного зловживання

1. Забороняється використання комунікаційно-превентивних заходів:

1) для тиску на суб'єктів публічного управління;

2) для формування політичної лояльності;

3) як прихованої форми контролю або збору інформації.

2. Порушення цієї статті тягне відповідальність, передбачену законом.

Розділ VIII
ПРАВОВІ НАСЛІДКИ ВСТАНОВЛЕННЯ ФАКТІВ ЗОВНІШНЬОГО ВПЛИВУ НА ПУБЛІЧНЕ УПРАВЛІННЯ

Стаття 36. Загальні засади застосування правових наслідків

1. Правові наслідки встановлення фактів зовнішнього впливу на публічне управління застосовуються виключно на підставі рішення суду в порядку, визначеному цим Законом.

2. Застосування правових наслідків не є формою юридичної відповідальності чи санкційного покарання та має превентивно-управлінський характер, спрямований на захист інформаційної безпеки, суверенітету та публічних інтересів України.

3. Правові наслідки застосовуються з дотриманням принципів:

1) верховенства права та юридичної визначеності;

2) пропорційності та необхідності втручання;

3) індивідуалізації з урахуванням характеру, інтенсивності та тривалості зовнішнього впливу;

4) строковості та тимчасовості обмежень;

5) поваги до прав і свобод людини і громадянина.

4. Жодні правові наслідки не можуть застосовуватися автоматично, колективно або без належної оцінки конкретних обставин справи.

Стаття 37. Види правових наслідків встановлення фактів зовнішнього впливу

1. За результатами судового розгляду можуть застосовуватися такі правові наслідки управлінсько-превентивного характеру:

1) тимчасове обмеження доступу особи до участі в окремих управлінських, регуляторних або консультативних процедурах у сфері публічного управління;

2) тимчасова заборона зайняття посад, пов’язаних із формуванням, реалізацією або впливом на державну політику, у тому числі на керівних або стратегічно чутливих посадах;

3) обмеження участі в дорадчих, експертних, конкурсних або робочих органах при органах державної влади та органах місцевого самоврядування;

4) покладення обов’язку щодо публічного або службового розкриття встановленої судом афілійованості з іноземними суб’єктами у порядку, визначеному законом;

5) інші обмежувальні заходи управлінського характеру, прямо передбачені цим Законом, які не мають каральної природи.

2. Вид і обсяг правових наслідків визначаються судом з урахуванням ступеня ризику для інформаційної безпеки та публічних інтересів України.

Стаття 38. Судовий порядок застосування правових наслідків

1. Підставою для звернення до суду є встановлення ЦПЗВ ознак зовнішнього впливу за результатами адміністративно-аналітичної процедури, проведеної відповідно до цього Закону.

2. Судовий розгляд здійснюється з дотриманням принципів змагальності сторін, рівності процесуальних прав та презумпції добросовісності особи.

3. Суд ухвалює рішення про застосування правових наслідків або про відмову в їх застосуванні протягом 15 робочих днів з дня надходження відповідної заяви від ЦПЗВ.

4. Особа, щодо якої розглядається питання застосування правових наслідків, має право на:

1) правову допомогу;

2) ознайомлення з матеріалами справи;

3) подання доказів і пояснень;

4) участь у судовому розгляді;

5) оскарження судового рішення в установленому законом порядку.

5. Рішення суду у справах цієї категорії підлягає негайному виконанню, проте може бути оскаржене в апеляційному порядку. Подання апеляційної скарги не зупиняє виконання рішення, якщо інше не встановлено судом апеляційної інстанції.

Стаття 39. Строк дії та перегляд правових наслідків

1. Правові наслідки встановлення фактів зовнішнього впливу застосовуються на визначений судом строк, який не може перевищувати строків, прямо встановлених цим Законом.

2. Суд зобов’язаний визначити конкретний строк дії кожного правового наслідку з урахуванням принципу мінімального необхідного втручання.

3. Правові наслідки можуть бути достроково припинені у разі:

1) усунення обставин, що стали підставою для їх застосування;

2) зміни характеру або інтенсивності зовнішнього впливу;

3) виконання особою покладених на неї зобов’язань;

4) наявності нових обставин, що мають істотне значення для справи.

4. Перегляд правових наслідків здійснюється виключно судом за заявою заінтересованої особи або ЦПЗВ.

Стаття 40. Гарантії прав і свобод людини при застосуванні правових наслідків

1. Застосування правових наслідків не може мати дискримінаційного характеру за будь-якими ознаками, визначеними Конституцією України та міжнародними договорами України.

2. Забороняється застосування колективної відповідальності або обмежень за ознакою належності до організацій, груп чи професійних спільнот без індивідуальної оцінки.

3. Застосування правових наслідків не може обмежувати права і свободи людини понад межі, необхідні для досягнення легітимної мети захисту публічних інтересів.

4. Право на справедливий суд та ефективний засіб юридичного захисту гарантується на всіх стадіях застосування цього Розділу.

Розділ IX
ПРИКІНЦЕВІ ТА ПЕРЕХІДНІ ПОЛОЖЕННЯ

1. Набрання чинності

1. Цей Закон набирає чинності через 6 місяців з дня його опублікування, крім положень, для яких встановлено інший строк введення в дію.

2. Положення Розділу IX застосовуються після набрання чинності положеннями Розділів V та VI, що забезпечують необхідні процесуальні та інституційні підстави.

2. Поетапне впровадження механізму

1. Протягом 9 місяців з дня набрання чинності цим Законом:

1) утворюється ЦПЗВ (відповідно до статей цього Закону);

2) затверджуються підзаконні нормативно-правові акти;

3) формується інформаційно-аналітична інфраструктура.

2. До повного запуску механізму застосовуються лише превентивні та аналітичні заходи.

3. Узгодження законодавства

1. Кабінету Міністрів України **протягом 12 місяців**:

1. привести свої нормативно-правові акти у відповідність із цим Законом;

2. подати пропозиції щодо внесення змін до законів України у частині:

адміністративних процедур;

захисту інформації;

судового контролю.

4. Гарантії прав людини в перехідний період

1. У перехідний період забороняється:

1) застосування обмежувальних заходів без судового контролю;

2) автоматичне включення до будь-яких реєстрів;

3) ретроспективне застосування цього Закону.

5. Моніторинг та оцінка ефективності

1. Через 3 роки з дня набрання чинності Законом здійснюється незалежна оцінка його ефективності з урахуванням:

1) впливу на права людини;

2) інституційної ефективності;

3) відповідності стандартам верховенства права.

2. Результати оцінки підлягають оприлюдненню.

Додаток Є

ГЕНЕРАЛЬНИЙ ШТАБ
ЗБРОЙНИХ СИЛ УКРАЇНИ
ГОЛОВНЕ
ОПЕРАТИВНЕ УПРАВЛІННЯ
проспект Повітряних Сил, 6 Київ, 03168
Тел.: (044) 230-73-26
E-mail: gou@post.mil.gov.ua
Код ЄДРПОУ 14304422
01.01.2026 № 304/9

ЗАТВЕРДЖУЮ
Тимчасово виконуючий обов'язки начальника Головного оперативного управління Генерального штабу Збройних Сил України
полковник
Ігор ПРОХОРЕНКО
"01" 01 2026 року

АКТ
про впровадження результатів дисертаційного дослідження "Адміністративно-правовий механізм забезпечення інформаційної безпеки України"

Комісія у складі:
голова комісії – полковник Дубінін Дмитро Володимирович
члени комісії: полковник Омельянчук Андрій Володимирович
полковник Греца Євгеній Сергійович

засвідчує (склали цей акт про те), що окремі наукові та практичні положення дисертаційної роботи "Адміністративно-правовий механізм забезпечення інформаційної безпеки України" аспіранта кафедри теорії держави і права, конституційного та адміністративного права факультету права та міжнародних відносин Державного університету "Київський авіаційний інститут" Калетніка Василя Васильовича були використані під час розробки у 2025 році проєкту Доктрини "Інформаційні операції".

Голова комісії: полковник Дмитро ДУБІНІН
Члени комісії: полковник Андрій ОМЕЛЬЯНЧУК
полковник Євгеній ГРЕЦА

Додаток Ж

ЗАТВЕРДЖУЮ
Тимчасово виконуючий обов'язки
начальника Військово-юридичного інституту
Національного юридичного університету
імені Ярослава Мудрого
полковник
Олександр БАБАРИЦЬКИЙ
23.02.2026р.

ДОВІДКА

щодо впровадження в освітній процес Військово-юридичного інституту Національного юридичного університету імені Ярослава Мудрого дисертаційного дослідження аспіранта кафедри теорії держави і права, конституційного та адміністративного права факультету права та міжнародних відносин Національного університету «Київський авіаційний інститут» Калетніка Василя Васильовича, поданого на здобуття ступеня доктора філософії з галузі знань: 08 «Право», за спеціальністю: 081 «Правознавство».

Повідомляємо про те, що в освітній процес Військово-юридичного інституту Національного юридичного університету імені Ярослава Мудрого на кафедрі військового права застосовано в якості допоміжного інформаційно-аналітичного матеріалу у 2025-2026 навчальному році при опануванні навчальної дисципліни: «Правові основи інформаційної безпеки у воєнній сфері» окремі наукові та практичні положення дисертаційного дослідження на тему: «Адміністративно-правовий механізм забезпечення інформаційної безпеки України» аспіранта Калетніка Василя Васильовича.

Начальник кафедри військового права
Військово-юридичного інституту
полковник Єгор БРІДНЯ
20.02.2026р.