НАУКОВО-ДОСЛІДНИЙ ІНСТИТУТ ПУБЛІЧНОГО ПРАВА

Кваліфікаційна наукова
праця на правах рукопису

БАТІЩЕВ СЕРГІЙ ОЛЕКСАНДРОВИЧ

УДК 342.951:351.817:004

ДИСЕРТАЦІЯ

АДМІНІСТРАТИВНО-ПРАВОВІ ЗАСАДИ ДІЯЛЬНОСТІ ОРГАНІВ ПУБЛІЧНОЇ АДМІНІСТРАЦІЇ У СФЕРІ ЗАХИСТУ ІНФОРМАЦІЇ

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_____ С.О. Батіщев

Науковий керівник **Боровик Андрій Володимирович,** доктор юридичних наук, професор

Київ – 2026

АНОТАЦІЯ

Батіщев С. О. Адміністративно-правові засади діяльності органів публічної адміністрації у сфері захисту інформації. – *Кваліфікаційна наукова праця на правах рукопису*.

Дисертація на здобуття наукового ступеня доктора філософії за спеціальністю 081 «Право». – Науково-дослідний інститут публічного права, Київ, 2026.

У дисертаційному дослідженні здійснено наукове обґрунтування теоретико-методологічних основ та сформульовано практичні рекомендації, спрямовані на вирішення актуальних проблем реалізації адміністративно-правового захисту інформації в Україні.

Визначено, що адміністративне право в механізмі формування стійкого інформаційного середовища в Україні відіграє одну із ключових ролей, адже з-поміж того, що визначає порядок організації та функціонування органів публічної адміністрації, що здійснюють адміністративно-правовий захист інформації, також забезпечує організаційну основу для реалізації інших важливих заходів, пов’язаних із протидією інформаційним загрозам, безперервністю перебігу важливих інформаційних процесів, впровадженням цифрових рішень в буденність тощо.

Доведено, що адміністративно-правовий захист інформації є різновидом діяльності органів публічної адміністрації, що безпосередньо пов’язаний із забезпеченням стійкості інформаційного середовища індивідуального, колективного та національного рівнів через реалізацію заходів попереджувального та реагувального характеру, спрямованих на запобігання порушенням, відновлення порушених прав та інтересів суб’єктів інформаційних відносин, а також створення умов для безпечного використання інформації як стратегічного ресурсу в публічних цілях. Зауважено, що індивідуальний, колективний та національний рівні інформаційного середовища є взаємопов’язаними.

Інструментами адміністративно-правового захисту названо: а) нормотворчі – передбачають розробку та прийняття нормативів, що встановлюють правила доступу до інформації, порядок її збирання, обробки, зберігання та поширення, а також визначають відповідальність за порушення режиму інформаційної безпеки. У цьому контексті йдеться як про нормативно-правові акти загальної та індивідуальної сили, так і про акти реагування та документи, якими оформлюються відповідні домовленості; б) превентивні – спрямовані на запобігання порушенням прав на інформацію та загрозам інформаційній безпеці. До них належать контроль за дотриманням правил доступу до інформації, інструктажі та навчання працівників, проведення інформаційно-просвітницьких кампаній, аудит інформаційних систем, моніторинг інформаційного середовища та раннє виявлення потенційних загроз; в) оперативні – реалізуються у разі фактичного порушення інформаційної безпеки та передбачають невідкладні дії щодо локалізації загроз і нейтралізації негативних наслідків. Це можуть бути тимчасові обмеження доступу до інформації, блокування неправомірних джерел, реагування на спроби несанкціонованого втручання або поширення дезінформації, а також координація між різними суб’єктами інформаційного простору; г) відновлювальні – спрямовані на відновлення порушених прав та цілісності інформації, ліквідацію наслідків інформаційних порушень та забезпечення стійкості інформаційного середовища у майбутньому. Йдеться зокрема про відновлення доступу до обмеженої або заблокованої інформації, публічні спростування фейків, компенсаційні дії, а також впровадження додаткових заходів контролю для запобігання повторних порушень.

Уточнено питання щодо співвідношення превентивних інструментів адміністративно-правового захисту та адміністративно-правової охорони, оскільки на перший погляд їх змістовне наповнення є подібним. Зауважено, що відмінність є. Вона полягає у цільовій спрямованості та функціональному контексті застосування. Так, превентивні інструменти адміністративно-правової охорони мають загально-регулятивний, стабілізаційний характер і

спрямовані на формування належного правового режиму інформаційних відносин, у межах якого мінімізується сама можливість виникнення правопорушень. Натомість превентивні інструменти адміністративно-правового захисту, хоча і мають попереджувальний характер, однак застосовуються вже в умовах наявності підвищених ризиків, загроз або передумов до порушення прав на інформацію чи інформаційної безпеки. Тобто їх превентивність є більш цільовою та ризик-орієнтованою, а не загальною.

Водночас органами публічної адміністрації у сфері захисту інформації названо: 1) органи стратегічного управління – Рада національної безпеки і оборони України та її робочі органи (Національний координаційний центр кібербезпеки, Центр протидії дезінформації), Кабінет Міністрів України; 2) органи виконавчої влади спеціальної компетенції – Міністерство цифрової трансформації України, Державна служба спеціального зв'язку та захисту інформації України, Служба безпеки України; 3) органи виконавчої влади секторальної компетенції – міністерства, правоохоронні органи, розвідувальні та контррозвідувальні органи, Національний банк України тощо; 4) органи влади регіонального та місцевого рівня – місцеві державні адміністрації та органи місцевого самоврядування; 5) інші інституції публічно-владного та правозахисного характеру – Уповноважений Верховної Ради України з прав людини, уповноважені підрозділи Національної поліції та інших органів.

Окремо уточнено, що суб'єкти та органи публічної адміністрації не є тотожними категоріями, а отже і правовими явищами. Зокрема остання є вужчою за змістом, адже суб'єктний склад публічної адміністрації представлений також допоміжними та залученими суб'єктами, які здійснюють захист інформації у власних інформаційно-комунікаційних системах та беруть участь у забезпеченні інформаційної безпеки у межах делегованих або покладених на них законом повноважень, не набуваючи при цьому статусу органів публічної влади у класичному розумінні (оператори

критичної інфраструктури, державні підприємства, установи та організації, суб’єкти господарювання та громадяни).

Запропоновано під адміністративно-правовим статусом органів публічної адміністрації у сфері захисту інформації розуміти сукупність нормативно визначених універсальних характеристик, які детермінують правове положення цих органів як суб’єктів публічної адміністрації в колі адміністративно-правових взаємозв’язків, пов’язаних із реалізацією ними повноважень під час забезпечення інформаційної безпеки та здійснення адміністративно-правового захисту прав громадян, юридичних осіб і держави в інформаційній сфері.

Узагальнено, що адміністративно-правовий статус органів публічної адміністрації у сфері захисту інформації характеризується функціональною диференціацією, що проявляється у розмежуванні їх основних цілей діяльності: від стратегічного планування та координації до безпосередньої реалізації заходів захисту та протидії загрозам, тобто кожен суб’єкт виконує специфічну роль, спрямовану на досягнення спільної мети – гарантування інформаційної безпеки держави, суспільства та особи.

Результати аналізу положень статті 10 Закону України «Про захист інформації в інформаційно-комунікаційних системах» є такими:

– по-перше, повноваження органів публічної адміністрації у сфері захисту інформації мають чітко виражену ієрархічну структуру, в межах якої Кабінет Міністрів України виконує нормотворчу та системоутворюючу функцію, визначаючи мінімальні вимоги до захисту інформації (базовий профіль безпеки), тоді як інші суб’єкти конкретизують ці вимоги на галузевому та інституційному рівнях;

– по-друге, простежується функціональна диференціація повноважень між органами: Державна служба спеціального зв'язку та захисту інформації України наділена спеціалізованими повноваженнями у сфері формування та реалізації політики, нормативного регулювання, контролю, експертизи та методичного забезпечення, що підтверджує її ключову роль як центрального

органу технічного та криптографічного захисту інформації;

– по-третє, уповноважені органи вправі не тільки встановлювати вимоги, а й забезпечувати їх реалізацію через процедури експертизи, авторизації, моніторингу та надання рекомендацій;

– по-четверте, повноваження органів публічної адміністрації у досліджуваній сфері реалізуються через механізм профілювання безпеки (базові, галузеві та цільові профілі), що дозволяє адаптувати загальні вимоги до конкретних умов функціонування інформаційних систем, рівня ризиків та специфіки відповідної сфери;

– по-п’яте, закріплено секторальний підхід до регулювання, відповідно до якого окремі органи, зокрема Національний банк України, Міністерство оборони України та Служба безпеки України, наділяються спеціальними повноваженнями щодо визначення вимог до захисту інформації з урахуванням специфіки відповідних сфер (фінансової, оборонної, правоохоронної);

– по-шосте, характерною є декомпозиція відповідальності між суб’єктами, за якої органи державної влади та місцевого самоврядування не лише виконують встановлені вимоги, а й самостійно розробляють цільові профілі безпеки для підпорядкованих систем, що свідчить про їх залучення до безпосередньої реалізації заходів захисту інформації.

Доведено, що у сфері захисту інформації взаємодія постає як обов’язкова умова належного виконання покладених на суб’єктів владних повноважень функцій у цій сфері, що знаходить своє закріплення у спеціальному законодавстві, передбачаючи як партнерський тип її здійснення, так і ієрархічний (субординаційний) характер взаємовідносин між відповідними суб’єктами, а також сприяння як особливу форму взаємодії, що має допоміжний, забезпечувальний характер і спрямована на створення належних умов для реалізації повноважень. Однак уточнено, що можна виокремлювати й інші форми взаємодії, які пов’язані з рівнями її реалізації.

Окремо визначається, що у сфері захисту інформації співробітництво не може розглядатися виключно як добровільна форма взаємодії суб'єктів, адже для його характерним є й імперативний компонент. У цій сфері воно набуває ознак функціонально обумовленого інструменту публічного адміністрування, який спрямований не лише на підвищення ефективності діяльності окремих суб'єктів, а й на мінімізацію ризиків, пов'язаних із фрагментарністю системи захисту інформації.

Встановлено, що чинне адміністративне законодавство України у сфері захисту інформації характеризується фрагментарністю, декларативністю окремих норм та недостатньою процедурною визначеністю, що ускладнює ефективну діяльність органів публічної адміністрації. Узагальнено, що його вдосконалення не може обмежуватися точковими змінами. Воно має носити системний характер і передбачати узгоджене реформування нормативної, інституційної та процедурної складових – через узгодження норм різних галузей права, усунення колізій, деталізацію процедур та запровадження нових правових інститутів, адаптованих до умов цифрової трансформації та воєнного стану.

Ключові слова: адміністративна діяльність, воєнний стан, електронне врядування, захист, інформаційна безпека, інформаційні мережі, інформаційні технології, кіберзахист, національна безпека, органи публічної адміністрації, публічне адміністрування, стійкість, цифрова трансформація.

SUMMARY

Batishchev, S. O. Administrative and legal principles of the activity of public administration bodies in the field of information protection. – *Qualification scientific work on the rights of the manuscript.*

The thesis for obtaining a scientific degree of Doctor of Philosophy in speciality 081 «Law». – Scientific Institute of Public Law, Kyiv, 2026.

The dissertation provides a scientific substantiation of the theoretical and methodological foundations and formulates practical recommendations aimed at addressing current issues in the implementation of administrative and legal protection of information in Ukraine.

It is established that administrative law plays a pivotal role in the formation of a sustainable information environment in Ukraine. In addition to defining the organizational and functional framework of public administration bodies responsible for the administrative and legal protection of information, it provides the institutional basis for implementing measures to counteract information threats, ensure the continuity of critical information processes, and integrate digital solutions into social practice.

The study demonstrates that the administrative and legal protection of information is a specialized activity of public administration bodies directly aimed at ensuring the stability of the information environment at individual, collective, and national levels. This is achieved through the implementation of preventive and responsive measures designed to prevent violations, restore the rights and interests of subjects of information relations, and create conditions for the secure use of information as a strategic resource for public purposes. The research emphasizes that the individual, collective, and national levels of the information environment are inherently interconnected.

The instruments of administrative and legal protection are identified as follows:

a) Norm-setting instruments – involve the development and adoption of standards that establish rules for access to information, procedures for its

collection, processing, storage, and dissemination, as well as define liability for violations of the information security regime. In this context, these include regulatory legal acts of both general and individual application, as well as enforcement acts and documents formalizing relevant agreements;

b) Preventive instruments – are aimed at preventing violations of information rights and threats to information security. These include monitoring compliance with access rules, staff briefings and training, information and awareness-raising campaigns, auditing of information systems, monitoring of the information environment, and early detection of potential threats;

c) Operational instruments – are implemented in the event of an actual breach of information security and involve immediate actions to localize threats and neutralize their negative consequences. These may include temporary restrictions on access to information, blocking unlawful sources, responding to unauthorized interference or dissemination of disinformation, and coordination among various stakeholders in the information space;

d) Restorative instruments – are aimed at restoring violated rights and the integrity of information, eliminating the consequences of information breaches, and ensuring the future resilience of the information environment. This includes restoring access to restricted or blocked information, issuing public corrections of false information, compensatory measures, and the implementation of additional control mechanisms to prevent recurrence.

The issue of the correlation between preventive instruments of administrative and legal protection and administrative and legal safeguarding has been clarified, as their substantive content appears similar at first glance. However, a distinction exists, which lies in their purposive orientation and functional context of application. Thus, preventive instruments of administrative and legal safeguarding are of a general regulatory and stabilizing nature and are aimed at establishing an appropriate legal regime for information relations, within which the very possibility of offences is minimized. In contrast, while preventive instruments of administrative and legal protection are also precautionary in nature, they are

applied specifically in conditions of increased risks, threats, or preconditions for violations of information rights or information security. Accordingly, their preventive character is more targeted and risk-oriented rather than general.

At the same time, public administration bodies in the field of information protection are identified as follows: (1) strategic management bodies – the National Security and Defense Council of Ukraine and its working bodies (the National Cybersecurity Coordination Center, the Center for Countering Disinformation), and the Cabinet of Ministers of Ukraine; (2) executive bodies of special competence – the Ministry of Digital Transformation of Ukraine, the State Service for Special Communications and Information Protection of Ukraine, and the Security Service of Ukraine; (3) executive bodies of sectoral competence – ministries, law enforcement agencies, intelligence and counterintelligence bodies, the National Bank of Ukraine, etc.; (4) regional and local authorities – local state administrations and local self-government bodies; and (5) other institutions of public authority and human rights mandate – the Ukrainian Parliament Commissioner for Human Rights, specialized units of the National Police, and other relevant bodies.

It is separately clarified that subjects of public administration and public administration bodies are not identical categories and, consequently, do not represent identical legal phenomena. In particular, the latter category is narrower in scope, as the subjective composition of public administration also includes auxiliary and involved entities that ensure information protection within their own information and communication systems and participate in guaranteeing information security within the limits of delegated powers or powers assigned to them by law, without acquiring the status of public authorities in the classical sense (such as critical infrastructure operators, state enterprises, institutions and organizations, business entities, and citizens).

It is proposed to define the administrative and legal status of public administration bodies in the field of information protection as a set of normatively established general characteristics that determine the legal position of these bodies

as subjects of public administration within administrative and legal relations related to the exercise of their powers in ensuring information security and implementing administrative and legal protection of the rights of individuals, legal entities, and the state in the information sphere.

It is generalized that the administrative and legal status of public administration bodies in the field of information protection is characterized by functional differentiation, which is manifested in the delimitation of their primary operational objectives, ranging from strategic planning and coordination to the direct implementation of protection measures and countering threats. Accordingly, each subject performs a specific role aimed at achieving a common goal – ensuring the information security of the state, society, and the individual.

The results of the analysis of the provisions of Article 10 of the Law of Ukraine “On the Protection of Information in Information and Communication Systems” are as follows:

– firstly, the powers of public administration bodies in the field of information protection have a clearly defined hierarchical structure, within which the Cabinet of Ministers of Ukraine performs norm-setting and system-forming functions, establishing minimum information protection requirements (basic security profile), while other subjects specify these requirements at the sectoral and institutional levels;

– secondly, there is a clear functional differentiation of powers among the bodies: the State Service for Special Communications and Information Protection of Ukraine is endowed with specialized powers in policy formulation and implementation, regulatory oversight, control, expertise, and methodological support, which confirms its key role as the central authority for technical and cryptographic information protection;

– thirdly, the authorized bodies are empowered not only to establish requirements but also to ensure their implementation through procedures of expertise, authorization, monitoring, and the provision of recommendations;

– fourthly, the powers of public administration bodies in this field are implemented through the mechanism of security profiling (basic, sectoral, and target profiles), which enables the adaptation of general requirements to the specific operating conditions of information systems, risk levels, and sectoral particularities;

– fifthly, a sectoral regulatory approach is established, under which individual bodies, in particular the National Bank of Ukraine, the Ministry of Defense of Ukraine, and the Security Service of Ukraine, are granted special powers to define information protection requirements, taking into account the specifics of their respective domains (financial, defense, and law enforcement);

– sixthly, a decentralization of responsibility among subjects is characteristic, whereby state and local government bodies not only comply with established requirements but also independently develop target security profiles for subordinate systems, indicating their direct involvement in the implementation of information protection measures.

It has been demonstrated that, in the field of information protection, interaction is an essential precondition for the proper performance of the functions assigned to public authorities in this area. This is enshrined in special legislation, which provides for both partnership-based implementation and hierarchical (subordinative) relations between the respective subjects, as well as for assistance as a specific form of interaction that is auxiliary and supportive in nature and aimed at creating appropriate conditions for the exercise of powers. At the same time, other forms of interaction may be identified depending on the levels at which it is implemented.

It is further determined that, in the field of information protection, cooperation cannot be viewed exclusively as a voluntary form of interaction between subjects, as it also contains an imperative component. In this sphere, it functions as a functionally conditioned instrument of public administration aimed not only at enhancing the efficiency of individual actors but also at minimizing risks associated with the fragmentation of the information protection system.

It is established that the current administrative legislation of Ukraine in the field of information protection is characterized by fragmentation, a declarative nature of certain provisions, and insufficient procedural certainty, which complicates the effective functioning of public administration bodies. It is generalized that its improvement cannot be limited to isolated amendments. It must be systemic in nature and involve the coordinated reform of normative, institutional, and procedural components through the harmonization of legal norms across different branches of law, the elimination of legal conflicts, the specification of procedures, and the introduction of new legal institutions adapted to the conditions of digital transformation and martial law.

***Keywords**:* administrative activity, cyber protection, digital transformation, e-governance, information networks, information security, information technologies, martial law, national security, protection, public administration bodies, public administration, resilience,

СПИСОК ПУБЛІКАЦІЙ ЗДОБУВАЧА ЗА ТЕМОЮ ДИСЕРТАЦІЇ

в яких опубліковані основні наукові результати дисертації:

1. Danylenko, A., Sokiran M., ***Batishchev S.***, Slabko K. Space Debris: Legal Status and Liability Regime. *Advanced Space Law*. 2022. Vol. 10. P. 4–13. DOI: https://doi.org/10.29202/asl/10/1

2. Батіщев С.О. Інформація як об’єкт правового захисту. *Право і суспільство*. 2023. № 3. С. 638–642. DOI: https://doi.org/10.32842/2078-3736/2023.3.96

3. Batishchev S. Peculiarities of interaction between public administration bodies and other subjects in the field of information protection. *Entrepreneurship, Economy and Law*. 2024. № 6. P. 257–262. DOI: https://doi.org/10.32849/2663-5313/2024.6.43

4. Батіщев С.О. Адміністративно-правовий захист інформації: теоретико-правовий аналіз. *Вісник Одеського національного університету. Правознавство*. 2025. Т. 27. №. 2(41). С. 12–16. DOI: https://doi.org/10.32782/2304-1587/2025-27-2(41)-2

які засвідчують апробацію матеріалів дисертації:

5. Батіщев С. О. Інформація та публічна адміністрація: точки перетину. *Інноваційні підходи до реформування сучасного законодавства*: матеріали міжнародної науково-практичної конференції (Київ, 20–21 квіт. 2023 р.). Київ: Науково-дослідний інститут публічного права, 2023. С. 44–46.

6. Батіщев С. О. Захист інформації через призму адміністративного законодавства України. *Актуальні проблеми імплементації наукових досягнень у практичну діяльність*: матеріали міжнародної науково-практичної конференції (Київ, 4–5 черв. 2024 р.). Київ: Науково-дослідний інститут публічного права, 2024. С. 98–100.

7. Батіщев С. О. Категорійно-понятєва визначеність правового концепту «адміністративно-правовий статус органів публічної адміністрації» на прикладі сфери захисту інформації. *Актуальні питання розвитку правової системи в сучасній Україні*: матеріали міжнародної науково-практичної

конференції (Львів–Торунь, 4 лют. 2025 р.). Науково-дослідний інститут публічного права. Львів–Торунь: Liha-Pres, 2025. С. 26–28.

ЗМІСТ

ВСТУП

Обґрунтування вибору теми дослідження. У сучасних умовах розвитку інформаційного суспільства дедалі більшої ваги набуває інформація як особлива нематеріальна цінність, що безпосередньо впливає на реалізацію прав і свобод людини, функціонування держави та стабільність суспільних відносин.

Як стратегічний ресурс інформація виступає ключовим елементом, що визначає якість прийняття управлінських рішень, забезпечує ефективну взаємодію громадськості з органами публічної адміністрації через підвищення прозорості та підзвітності їх діяльності, а також є основою для надання якісних адміністративних послуг. За таких умов процеси збору, обробки, зберігання та використання інформації набувають ознак не лише інформаційно-аналітичної діяльності, а й безперервної функціональної складової діяльності будь-якого суб’єкта публічного управління.

Водночас стрімка цифровізація суспільних відносин, посилення кіберзагроз, розвиток інформаційних технологій та зростання обсягів оброблюваних даних істотно ускладнюють забезпечення належного рівня захисту інформації. Це зумовлює появу нових викликів для системи публічного адміністрування, пов’язаних із необхідністю одночасного забезпечення відкритості інформації та її безпеки, протидії кібератакам, витокам даних і деструктивному інформаційному впливу.

За таких умов питання адміністративно-правового захисту інформації набуває особливого значення, адже саме держава виступає центральним та системоутворюючим актором, здатним забезпечити організацію ефективної системи інформаційної безпеки, координацію діяльності уповноважених органів, протидію сучасним інформаційним загрозам і створення належних умов для стабільного та безпечного функціонування інформаційного простору.

Зв'язок теми дисертації із сучасними дослідженнями. Проблематика адміністративно-правового захисту інформації перебуває у фокусі міждисциплінарних досліджень, що здійснюються на перетині наукових розвідок у сфері адміністративного права, інформаційного права, кібербезпеки та публічного управління. Сучасний науковий дискурс концентрується навколо питань трансформації ролі держави в умовах цифровізації, забезпечення стійкості інформаційного простору, протидії кіберзагрозам та дезінформації, а також удосконалення механізмів публічного адміністрування у цифровому середовищі. Серед таких варто виділити, приміром, роботу Ю. Шкіндера, який визначив вплив цифровізації на забезпечення правопорядку в Україні (Івано-Франківськ, 2025), О. Дубовського, що схарактеризував інформаційну безпеку України в умовах глобалізації світового інформаційного простору (Київ, 2025), В. Крушеніцького, який здійснив комплексне наукове дослідження адміністративно-правових засад забезпечення національної безпеки в публічно-інформаційній сфері (Кропивницький, 2025), М. Александрової, що визначила зміст та особливості адміністративно-правового забезпечення інформаційної безпеки у сфері електронного урядування (Київ, 2024), А. Тарасюка, який схарактеризував теоретико-правові основи забезпечення кібербезпеки України (Київ, 2021).

Водночас, попри наявність значного наукового доробку, питання комплексного адміністративно-правового забезпечення діяльності органів публічної адміністрації у сфері захисту інформації, зокрема в умовах воєнного стану та гібридних загроз, залишаються недостатньо розробленими та потребують подальшого наукового осмислення. Тому джерельною базою для цього дослідження слугували праці таких вчених як: В. Авер'янов, М. Баран, Ю. Битяк, В. Богуш, В. Борисов, А. Боровик, І. Бочкова, М. Вавринчук, І. Габро, К. Гарбузюк, М. Гончаров, А. Гуз, А. Даниленко, О. Дубас, О. Золотар, А. Зубко, В. Карпенко, О. Когут, Л. Кожура, М. Комова, І. Корж, І. Костенко, О. Коцовська, К. Кочман, Л. Кочубей, Д. Кошиков,

О. Кузьменко, К. Куркова, Д. Левченко, В. Лукашевич, А. Луцька, Г. Мелеганич, Ю. Мохова, В. Оксінь, П. Орлов, В. Пашкова, О. Пащенко, А. Пелещишин, Є. Петров, А. Приходько, О. Пугачов, Т. Савосько, М. Санакуєв, Л. Сорока, О. Соснін, В. Тимошенко, О. Токар, О. Тугарова, Г. Форос, І. Цимбалюк, О. Шарук, О. Шепета, М. Шиленко, Ю. Шпарага, О. Юдін, П. Яковлєв та багатьох інших.

Зв'язок роботи з науковими програмами, планами, темами. Дисертаційне дослідження узгоджується з основними положеннями Угоди про асоціацію між Україною та Європейським Союзом, ратифікованої Законом України від 16 вересня 2014 року № 1678-VII та плану заходів з її виконання, затвердженого постановою Кабінету Міністрів України від 25 жовтня 2017 року № 1106; Цілей сталого розвитку України на період до 2030 року, постановлених Указом Президента України від 30 вересня 2019 року № 722/2019; Стратегії національної безпеки України, затвердженої Указом Президента України від 14 вересня 2020 року № 392/2020; Стратегії інформаційної безпеки, затвердженої Указом Президента України від 28 грудня 2021 року № 685/2021 та плану заходів з її реалізації на період до 2025 року, затвердженого розпорядженням Кабінету Міністрів України від 30 березня 2023 року № 272-р; Стратегії кібербезпеки України, затвердженої Указом Президента України від 26 серпня 2021 року № 447/2021; Концепції забезпечення національної системи стійкості, затвердженої Указом Президента України від 27 вересня 2021 року № 479/202 та плану її реалізації до 2025 року, затвердженої розпорядженням Кабінету Міністрів України від 10 листопада 2023 року № 1025-р; Стратегії забезпечення державної безпеки, затвердженої Указом Президента України від 16 лютого 2022 року № 56/2022; Національного плану реагування на кіберінциденти, кібератаки та кіберзагрози, затвердженого постановою Кабінету Міністрів України від 26 листопада 2025 року № 1533.

Тема дисертаційного дослідження узгоджується з планом науково-дослідної роботи Науково-дослідного інституту публічного права «Правове

забезпечення прав, свобод та законних інтересів суб'єктів публічно-правових відносин» (номер державної реєстрації 0126U003901) та затверджена рішенням вченої ради Науково-дослідного інституту публічного права 21 листопада 2022 року (протокол № 15).

Мета і завдання дослідження. *Мета* роботи полягає у виявленні проблем та недоліків у діяльності органів публічної адміністрації у сфері захисту інформації, уточненні причин їхнього виникнення, а також наданні пропозицій щодо їхнього усунення з позиції поєднання організаційного та правового дискурсів.

Для досягнення поставленої мети в дисертації потрібно виконати такі *завдання*:

– розкрити явище «інформація» крізь призму об'єкту правового захисту;

– визначити зміст та сутність адміністративно-правового захисту інформації;

– з'ясувати правові засади діяльності органів публічної адміністрації у сфері захисту інформації;

– сформувати поняття та визначити структуру адміністративно-правового статусу органів публічної адміністрації у сфері захисту інформації;

– розкрити повноваження органів публічної адміністрації у сфері захисту інформації;

– виявити механізми взаємодії органів публічної адміністрації з іншими суб'єктами у сфері захисту інформації;

– схарактеризувати зарубіжний досвід адміністративно-правового захисту інформації;

– запропонувати способи удосконалення адміністративного законодавства щодо діяльності органів публічної адміністрації у сфері захисту інформації.

Об'єктом дослідження є суспільні відносини, що виникають у сфері реалізації публічною адміністрацією своїх функціональних обов'язків щодо забезпечення та здійснення захисту інформації.

Предмет дослідження – адміністративно-правовий захист інформації, що здійснюється органами публічної адміністрації.

Методи дослідження. У дисертаційному дослідженні використано сукупність загальнонаукових і спеціально-юридичних методів, що забезпечили комплексне розкриття проблематики адміністративно-правового захисту інформації в України.

За допомогою методів *наукової індукції* та *дедукції* здійснено узагальнення теоретичних підходів до розуміння інформації як об'єкта правового захисту, а також перехід від загальних положень до конкретизації особливостей адміністративно-правового захисту інформації (розділи 1–2). Методи *аналізу* та *синтезу* використано для дослідження змісту та сутності адміністративно-правового захисту інформації, а також для виокремлення його структурних елементів і формування цілісного уявлення про відповідний правовий інститут (підрозділи 1.2, 1.3).

Формально-юридичний метод застосовано для з'ясування змісту правових норм, що визначають засади діяльності органів публічної адміністрації у сфері захисту інформації, а також розкриття їх адміністративно-правового статусу і повноважень (підрозділ 1.3, розділ 2). *Системно-структурний* метод застосовано для визначення структури адміністративно-правового статусу органів публічної адміністрації та встановлення взаємозв'язків між його елементами, а також для аналізу механізмів взаємодії відповідних суб'єктів (розділ 2).

Логіко-семантичний метод використано для уточнення понятійно-категоріального апарату дослідження, зокрема при визначенні змісту понять «інформація», «адміністративно-правовий захист інформації», «адміністративно-правовий статус органів публічної адміністрації» (розділи 1–2).

Порівняльно-правовий метод використано при дослідженні зарубіжного досвіду реалізації адміністративно-правового захисту інформації, що дало змогу виявити ефективні моделі правового регулювання та оцінити можливість адаптації позитивних практик в Україні (підрозділ 3.1). Метод *правового моделювання* застосовано для розроблення пропозицій щодо удосконалення адміністративного законодавства у сфері діяльності органів публічної адміністрації щодо захисту інформації (підрозділ 3.2).

Крім того, на усіх етапах роботи застосовними були: 1) метод *узагальнення* для формулювання висновків і пропозицій за результатами дослідження; 2) *аксоматичний* метод, який забезпечив послідовне й несуперечливе вибудовування авторської думки; 3) метод *абстрагування*, що дозволив відмежувати суттєві ознаки досліджуваних правових явищ від другорядних характеристик.

Наукова новизна отриманих результатів полягає в тому, що дисертація є одним із перших комплексних досліджень у межах науки адміністративного права, що надає наукове обґрунтування теоретико-методологічних основ та розкриває практичні рекомендації щодо вирішення актуальних проблем реалізації адміністративної діяльності органів публічної адміністрації у сфері захисту інформації. За результатами проведеного аналізу сформульовано наукові положення та висновки, запропоновані особисто здобувачем. Основні з них такі:

вперше:

– запропоновано розглядати зміст адміністративно-правового захисту інформації через призму тріади «конфіденційність – цілісність – доступність» як концептуальної основи його побудови, що дозволило перейти від формально-юридичного до системно-функціонального розуміння цього явища;

– обґрунтовано дуалістичний характер сприяння як провідної форми взаємодії у сфері захисту інформації, що проявляється у взаємному

забезпеченні реалізації повноважень між Держспецзв'язку та іншими суб'єктами публічного права;

– сформовано систему ініціатив щодо удосконалення адміністративного законодавства в контексті діяльності органів публічної адміністрації у сфері захисту інформації, які об'єктивують необхідність нормативної уніфікації законодавчих положень у цій сфері, деталізації адміністративних процедур реагування на кіберінциденти, запровадження дієвого механізму юридичної відповідальності за порушення у сфері захисту інформації, інституційного та ресурсного посилення функціоналу органів публічної адміністрації, розвитку механізмів публічно-приватного партнерства у сфері кібербезпеки з чітким визначенням правового статусу приватних суб'єктів, імплементації ризик-орієнтованого підходу до управління кіберзагрозами, нормативного врегулювання використання сучасних цифрових технологій, зокрема штучного інтелекту та автоматизованих систем моніторингу, а також запровадження системи оцінки ефективності діяльності органів публічної адміністрації із встановленням чітких критеріїв її результативності;

удосконалено:

– доктринальне розуміння природи інформації як об'єкта правового захисту, яке поєднує її філософське (онтологічне) та юридичне трактування, що дозволяє розкрити її подвійний характер як універсальної характеристики реальності та специфічного об'єкта правовідносин;

– наукові підходи до визначення адміністративно-правового статусу органів публічної адміністрації у сфері захисту інформації шляхом обґрунтування необхідності його розгляду крізь призму функціональної диференціації їх діяльності, яка проявляється у розмежуванні цільового призначення відповідних суб'єктів – від формування та координації державної політики до безпосереднього здійснення заходів інформаційного захисту та протидії загрозам;

отримали подальший розвиток:

– авторське визначення правових засад діяльності органів публічної адміністрації у сфері захисту інформації як динамічної, функціонально орієнтованої системи правового регулювання, що не зводиться до сукупності нормативно-правових актів, а визначає зміст, межі та механізми реалізації державної інформаційної політики у напрямку забезпечення інформаційної безпеки в Україні;

– обґрунтування того, що профілювання безпеки (базові, галузеві, цільові профілі) є ключовою формою реалізації повноважень органів публічної адміністрації у сфері захисту інформації;

– результати компаративістичного аналізу європейської та американської адміністративно-правових моделей захисту інформації, що стало підставою для визначення доцільності вдосконалення окремих механізмів публічного адміністрування у сфері захисту інформації в Україні.

Особистий внесок здобувача. Дисертаційне дослідження здійснене автором самостійно, всі положення наукової новизни та висновки сформовано особисто. В науковому журналі Advanced Space Law у співавторстві з А. Даниленко, М. Сокираном та К. Слабко опубліковано наукову працю під назвою «Space Debris: Legal Status and Liability Regime», де автором розроблена загальна концепція статті, розкрито проблематику правового статусу та його особливостей, сформовано частину висновків.

Практичне значення отриманих результатів полягає в тому, що сформульовані й аргументовані в дисертаційному дослідженні висновки, теоретичні положення та конкретні пропозиції використовуються та можуть бути використані у:

– *науково-дослідній сфері* – для подальшого наукового вивчення теоретико-методологічних проблем науки адміністративного права і процесу (акт впровадження Науково-дослідного інституту публічного права);

– *практичній діяльності* – для вдосконалення чинного законодавства в частині підвищення результативності реалізації механізмів адміністративно-правового захисту інформації публічною адміністрацією України;

– *освітньому процесі* – під час розроблення та викладання навчальної дисципліни «Адміністративне право та процес: доктринальні та практичні проблеми» (акт впровадження Науково-дослідного інституту публічного права).

Апробація матеріалів дисертації. Підсумки розроблення проблеми загалом, окремі її аспекти, одержані узагальнення та висновки оприлюднено на трьох науково-практичних конференціях: «Інноваційні підходи до реформування сучасного законодавства» (м. Київ, 20–21 квітня 2023 року), «Актуальні проблеми імплементації наукових досягнень у практичну діяльність» (м. Київ, 4–5 червня 2024 року), «Актуальні питання розвитку правової системи в сучасній Україні» (м. Львів, 4 лютого 2025 року).

Публікації. Основні положення та висновки дисертації викладено у семи наукових працях, з яких три одноосібних статті опубліковані в журналах, включених МОН України до переліку наукових фахових видань з юридичних наук, одна стаття у співавторстві (з А. Даниленко, М. Сокираном та К. Слабко) у науковому фаховому виданні України з юридичних наук; три – тези доповідей на науково-практичних конференціях та круглих столах.

Структура та обсяг дисертації. Робота складається зі вступу, трьох розділів, що містять вісім підрозділів, висновків, списку використаних джерел і додатків. Загальний обсяг дисертації становить 206 сторінок. Робота містить список використаних джерел з 246 найменувань на 28 сторінках.

РОЗДІЛ 1
ТЕОРЕТИКО-ПРАВОВА ОСНОВА ДІЯЛЬНОСТІ ОРГАНІВ ПУБЛІЧНОЇ АДМІНІСТРАЦІЇ У СФЕРІ ЗАХИСТУ ІНФОРМАЦІЇ

1.1. Інформація як об’єкт правового захисту

У статті 3 Конституції України закріплено, що людина, її життя і здоров’я, честь, гідність визнаються найвищою соціальною цінністю в державі. При цьому серед зазначених благ першочергове значення надається життю та здоров’ю як невід’ємним характеристикам кожної особи [19, с. 126]. Зазначене обумовлює необхідність гарантування належного рівня їх захищеності. У цьому контексті безпека виступає не лише як фізичний чи матеріальний стан особи, а й як комплексне явище, забезпечення якого в усіх сферах суспільного життя стає державним пріоритетом [15].

Концепція безпеки як система поглядів на цілі, завдання, способи і засоби забезпечення безпечної діяльності повинна в загальному вигляді відповідати на три базові питання: 1) що захищати; 2) від чого (кого) захищати; 3) як захищати. Із питанням «що захищати» зв’язане поняття «об’єкт захисту» [107, с. 146].

Як справедливо зауважує Г. Козаченко, поняття «об’єкт захисту» належить до таких, що вважаються аксіоматичними і сприймаються за умовчанням як такі, зміст яких є загальновизнаним, тобто всі дослідники сприймають його однаково [67, с. 12]. Приміром, К. Бабенко у статті про конституційний захист прав людини об’єктом захисту вбачає явище, яке має фундаментальне значення для існування та розвитку суспільства і тому підлягає охороні державою [8].

Варто вказати, що у сучасних умовах розвитку інформаційного суспільства до кола таких об’єктів дедалі частіше відносять інформацію, яка набуває статусу самостійної соціальної та правової цінності. Пояснити

зазначене досить просто, – інформаційна сфера вже давно перетворилась не тільки в одну з найбільш прогресивних та перспективних наукових галузей, але й на фундаментальну складову частину всього процесу пізнання з точки зору науки, наукову базу для формування суспільства, що засноване на знаннях [170, с. 91].

Тому проблематика забезпечення безпеки інформаційних відносин вже тривалий час перебуває у центрі уваги як вітчизняних, так і зарубіжних науковців, адже суспільні відносини, що виникають у сфері створення, збирання, зберігання, використання та захисту інформації характеризуються динамічністю, багатовимірністю та підвищеним рівнем ризиків їх порушення в умовах цифровізації суспільного розвитку. Разом з тим окремі аспекти зазначеної проблематики залишаються недостатньо розробленими та потребують подальшого наукового осмислення. Зокрема в контексті визначення юридичної природи інформації через призму об’єкта правового захисту вченими наголошується на необхідності уточнення її статусу, видів та меж правового регулювання. Тим самим обґрунтовується доцільність застосування комплексного підходу до вивчення механізмів захисту інформаційних відносин, що передбачає послідовне та системне розкриття всіх аспектів проблеми [15].

Відповідно, розпочинаючи розгляд порушеної у межах цього дослідження проблематики, варто першочергово визначити значення інформації у правовій площині шляхом аналізу її природи як першого кроку до більш комплексного вивчення питань діяльності вітчизняних органів публічної адміністрації у сфері захисту інформації.

Так дослідження засвідчують, що інформація є основним фактором у процесах самоорганізації та еволюції складних систем [170, с. 93]. До середини 20-х років XX ст. під інформацією розумілись відомості та повідомлення, які передаються людьми усно, письмово або іншим способом. З середини XX ст. інформація перетворюється у загальнонаукове поняття, яке включає обмін повідомленнями між людьми, людиною та автоматом,

автоматом та автоматом; обмін сигналами у тваринному та рослинному світі. На побутово-життєвому рівні під інформацією розуміється сукупність певних відомостей, знань і повідомлень про будь-які об’єкти, явища і процеси. Як відмічає В. Лукашевич, суто наукове поняття інформації певною мірою відвертається від змістовної сторони повідомлень і бере їх кількісний аспект. Кількість інформації визначається як величина обернена пропорційна ступеню імовірності тієї події, про яку йде мова в повідомлені [89, с. 4; 113, с. 250].

Разом з тим існує безліч думок стосовно питання дефініції інформації, на що вказує масштаб досліджень цієї проблематики. Наприклад, у сучасних наукових джерелах міститься понад 200 визначень інформації [34, с. 16].

Зауважимо, що прихильники функціональної концепції стверджують, що інформація – лише одна з функцій людської свідомості і тому в неживій природі вона принципово існувати не може. Що ж стосується закономірностей функціонування та розвитку неживої природи, то вони доволі повно описуються у відповідних наукових дисциплінах (фізиці, хімії та ін.), в яких поняття інформації практично не використовується . Ця точка зору широко розповсюджена в науці і в наш час [170, с. 93]. Водночас, проаналізувавши підходи до визначення феномену інформації з точки зору представників природничих наук, О. Дзьобань справедливо констатує, що «свідомо або мимоволі, всі ці поспішні й погано продумані узагальнення, поширювані про інформацію й інформаційні процеси представниками точних наук, призвели до того, що в сучасній свідомості, у міркуваннях про інформацію, багато в чому вже стирається принципова грань між людиною й тваринами (і навіть машинами), що, як мінімум, є передчасним» [43, с. 10–11]. Це означає, що на інформацію як складову буття людини необхідно розглядати з точки зору онтології і гносеології цього феномену [34, с. 18–19].

Примітно, що винятковий онтологічний статус феномену інформації надихнув Л. Флоріді, італійського філософа, до розроблення нової філософської теорії, яка вивчає та обґрунтовує інформаційні концепти в

умовах глобального поширення комп'ютеризації та інформаційних технологій [220; 221; 222]. На думку Л. Флоріді, фундаментальність поняття інформації виявляється в тому, що в її термінах можуть бути визначені такі базові філософські категорії, як буття, знання, життя, розум, досвід, судження, правда, етика, творчість, значення, добро і зло. Учений визначає сутність нової філософської дисципліни на перетині потенціалу філософської методології і ресурсів інформаційних технологій. Трактує філософію інформації як нову філософську дисципліну, пов'язану з критичним дослідженням концептуальної природи і базових принципів інформації, із розробленням та застосуванням інформаційно-теоретичних та обчислювальних методологій філософських проблем [71, с. 19; 222].

Тобто, сучасна наукова думка демонструє поступовий перехід від вузького, антропоцентричного розуміння інформації до її більш широкого, універсального трактування як фундаментальної характеристики реальності.

Приміром, М. Санакуєв стверджує, що: 1) інформація в широкому розумінні – об'єктивна властивість реальності, яка проявляється в неоднорідності (асиметрії) розподілу матерії та енергії в просторі і часі, в нерівномірності протікання всіх процесів, що відбуваються у світі живої і неживої природи, а також у людському суспільстві і свідомості; 2) інформація пронизує всі рівні організації матерії та енергії в навколишньому світі, вона є першопричиною руху матерії та енергії і визначає напрямок цього руху в просторі і часі; 3) інформація є вирішальним фактором еволюції, вона визначає напрямок розвитку всіх еволюційних процесів у природі і суспільстві; 4) кількість інформації є мірою складності організованих систем будь-якої природи і дає можливість отримувати кількісні оцінки рівня цієї складності; 5) інформація – багатоплановий феномен реальності, який специфічним чином проявляє себе в різних умовах протікання інформаційних процесів у різноманітних інформаційних середовищах живої та неживої природи: у неживому природному середовищі, в технічних об'єктах і системах штучної природи, створених людиною, в біологічних системах, а

також у людському суспільстві і свідомості; 6) можна припустити, що існують деякі фундаментальні закономірності прояву інформації, які є загальними для інформаційних процесів, що реалізуються в об’єктах, процесах чи явищах будь-якої природи [170, с. 93–94].

Разом з тим, поряд із філософським осмисленням інформації як універсальної категорії, у науковому дискурсі сформувалися підходи, що прагнуть конкретизувати її зміст через виявлення сутнісних характеристик та функціональних проявів у різних сферах буття [182, с. 359]. Тому не дивно, що власне змістовне розуміння має «інформація» і в юриспруденції [182, с. 359].

О. Тугарова зауважує, що вперше правове визначення поняття інформації було закріплено в Законі України «Про інформацію» 1992 року: інформацією визнавалися документовані або публічно оголошені відомості про події та явища, що відбуваються у суспільстві, державі та навколишньому природному середовищі. Внесення змін до Закону у 2011 році суттєво спростило легальне визначення поняття інформації: інформацією є будь-які відомості та/або дані, які можуть бути збережені на матеріальних носіях або відображені в електронному вигляді (стаття 1 Закону) [182, с. 359].

Щодо інших нормативно-правових актів, залежно від предмета правового регулювання, буде різнитись нормативне визначення досліджуваної категорії. Наприклад, у межах положень Закону України «Про захист економічної конкуренції» інформація трактується як відомості в будь-якій формі й вигляді та збережені на будь-яких носіях (у тому числі листування, книги, помітки, ілюстрації (карти, діаграми, органіграми, малюнки, схеми тощо), фотографії, голограми, кіно-, відео-, мікрофільми, звукові записи, бази даних комп’ютерних систем або повне чи часткове відтворення їх елементів), пояснення осіб та будь-які інші публічно оголошені чи документовані відомості [148].

Однак варто погодитись з тим, що визначення, наведене у профільному законі, є найбільш застосовним, адже відзначається своєю універсальністю.

Разом з тим, законодавча «простота» визначення поняття інформації стала каталізатором наукової активності у формулюванні змісту означеної категорії [182, с. 359].

Приміром, І. Бочкова запропонувала підхід, відповідно до якого під інформацією повинні розумітись будь-які відомості та/або дані щодо дій, подій, закономірностей, взаємозв'язку, стану суб'єктів чи об'єктів суспільних відносин, які можуть бути збережені на матеріальних носіях або відображені в електронному вигляді, права на які можуть потребувати визнання та захисту. Така позиція стає передумовою визнання прав не на будь-які відомості, закріплені на носії, а лише ті, що містять певну об'єктивну чи суб'єктивну корисність, важливість, а отже, можуть порушуватись і тому потребують визнання і захисту. Нам імпонує такий підхід, адже він відмежовує інформацію як явище від інформації як правової категорії і детермінує встановлення різних правових режимів для різних відомостей [20, с. 89].

Доповнюючи тезу про необхідність диференціації загального та часткового, уточнимо, що в загальному контексті категорія «інформація» характеризується низкою взаємопов'язаних властивостей, які розкривають та репрезентують це поняття. До них у науковій літературі відносять: 1) наявність мети – інформування, оцінка, планування, контроль, пошук; 2) наявність адресата – за відсутності споживача інформації, говорити про неї недоцільно; 3) суб'єктивна цінність; 4) спосіб і форма подання; 5) повнота – повідомлення повинні охоплювати весь стан об'єкта за усіма керованими параметрами, при цьому додавання будь-яких інших відомостей не дає нових знань про об'єкт; 6) необхідність – повідомлення повинно надавати тальки необхідні знання, скорочення інформації в повідомленні зменшує знання стосовно об'єкта, надмірність припускається тільки для спеціальних цілей; 7) точність – кількісна характеристика параметрів, які визначають стан керованого об'єкта, і зменшення яких неприпустимо, а збільшення може бути зайвим; 8) надійність; 9) своєчасність і регулярність; 10) придатність –

синтезуюча властивість цінності, повноти, необхідності та надмірності, точності, надійності, своєчасності та регулярності [89, с. 6]; 11) споживча якість [113, с. 252].

Разом з тим у науковій літературі сформувалися такі основні ознаки інформації саме як правової категорії: 1) нематеріальний характер інформації – інформація, на відміну від предметів і речей матеріального світу, є певною субстанцією, яка не має фізичної форми. Отже, цінність інформації безпосередньо залежить від її змісту, а не форми закріплення; 2) фізична невідчужуваність інформації, яка заснована на тому, що знання не можуть бути відокремлені від людини як її творця – ця вимога сформулювала правило: разом з відчуженням інформації від одної особи до іншої і юридичного закріплення цього факту має відбуватися передача всіх прав на використання інформації; 3) відокремленість інформації характеризує інформацію як об'єкт, що знаходить свій вираз у вигляді символів, звуків, цифр тощо. Завдяки цьому інформація може відокремлена від її творця і існувати незалежно від нього. Ця ознака створює можливість передачі інформації від одного суб'єкта до іншого; 4) властивість інформаційної речі (інформаційного об'єкта) – право на інформацію і право власності на матеріальний носій інформації є різними правами і не залежать одне від одного. Звідси випливає правило: відчуження матеріального носія не означає відчуження права на інформацію і навпаки; 5) тиражованість інформації створює можливість розповсюдження інформації без зміни її змісту. Одна й та ж інформація може водночас належати необмеженому колу осіб, тому необхідно юридично закріплювати обсяг прав з використання інформації кожної особи, яка має доступ до конкретних відомостей або даних; 6) екземплярність інформації дозволяє вести облік інформації через облік носіїв, що містять інформацію – завдяки цій ознаці стає можливим забезпечувати механізм реєстрації інформації, виконувати умови обігу інформації з обмеженим доступом [77; 182, с. 359; 187, с. 24–26].

Також варто вказати, що з позиції інформаційної безпеки інформація характеризується своєю конфіденційністю, цілісністю та доступністю [4, с. 47]. Зокрема згідно з термінологією законодавства конфіденційність інформації – властивість інформації, яка полягає в тому, що інформація не може бути отримана неавторизованим користувачем інформаційно-комунікаційної системи та/або процесом [40]; цілісність інформації – умови, за яких інформація зберігається, передається та приймається без змін [134] або властивість інформації, яка полягає в тому, що інформація не може бути модифікована неавторизованим користувачем інформаційно-комунікаційної системи та/або процесом [40]; доступність інформації – властивість інформації бути захищеною від несанкціонованого блокування [156]. Міститься уточнення, що інформація зберігає конфіденційність, якщо дотримуються встановлені правила інформаційної безпеки відносно доступу до неї, а цілісність, – якщо дотримуються встановлені правила з інформаційної безпеки відносно її модифікації (видалення) [40].

Своєю чергою, саме необхідність забезпечення зазначених властивостей обумовлює формування змісту інформаційної безпеки. У цьому контексті інформаційна безпека розглядається як комплекс заходів, спрямованих на забезпечення захищеності інформації від несанкціонованого доступу, використання, оприлюднення, руйнування, внесення змін, ознайомлення, перевірки, запису чи знищення даних [4, с. 47].

Окремо зауважимо, що апелювання словосполученнями «інформаційна безпека» та «захист інформації» є оманливим, адже, постає цікаве питання про їхнє співвідношення. Зокрема існує думка, що перше має скоріше наукове, теоретичне поняття, а «захист інформації» звичайно використовується при описанні практичних заходів. Проте у цілому вони є синонімами і як правило, між ними не робитися якої-небудь різниці [88].

На нашу думку, це зумовлено тим, що сфера інформаційної безпеки історично формувалася як міждисциплінарне явище і вже на ранніх етапах свого розвитку набула дуалістичного характеру, поєднуючи юридичну та

філософську компоненти [31, с. 20]. Така подвійна природа обумовлена тим, що, з одного боку, інформаційна безпека пов’язана з правовим регулюванням суспільних відносин, а з іншого – із загальними уявленнями про цінність інформації, її роль у суспільстві та необхідність її збереження.

Щодо цього показовими є історичні витоки становлення підходів до захисту інформації. Так, О. Золотар, досліджуючи першоджерела інформаційної безпеки, зазначає, що «початок історії захисту інформації вчені пов’язують з появою можливості фіксації інформаційних повідомлень на твердих носіях, тобто з винаходом писемності, а першим видом інформації, що підлягала захисту, вважають державну таємницю» [59, с. 140]. На думку науковця, майже одночасно з винайденням писемності були відкриті методи і способи захисту інформації, а саме шифрування і приховування [31, с. 20–21].

Ілюстрацією цього є відомий історичний приклад, наведений ученим, що стосується одного з найдавніших способів захисту інформації від стороннього доступу: йдеться про зашифрований текст, прихований під рецептом глазурі на виробах гончарства в Месопотамії (близько 2000 р. до н. е.) [31, с. 20–21]. Такий приклад свідчить про те, що потреба у захисті інформації має глибинний історичний характер і передувала сучасному етапу розвитку правового регулювання у цій сфері.

Зокрема колектив науковців, серед яких А. Тоцький, О. Тимошенко, А. Гуз, вважають, що історія охорони і захисту інформації на території сучасної України також сягає ще додержавних часів. Першим видом інформації, яку потрібно було охороняти, була військова інформація. Спочатку охорону такої інформації забезпечував князь, потім особа, яку він призначав особисто. Війна була на той час головним і загальновизнаним способом ведення зовнішньої політики будь-якої держави, тому захист військової інформації був головним у політиці князів Олега, Ігоря, Святослава, Ярослава та княгині Ольги. Князі, йдучи в похід, намагалися приховати інформацію про кількість війська і напрям головного удару. Ворог не міг адекватно реагувати на

небезпеку, а заздалегідь розпущені чутки, перебільшення і неправдива інформація ще більше призводили до паніки [31, с. 23; 105, с. 11].

Сьогодні ж об'єктами інформаційної безпеки є держава, суспільство та особа [10, с. 30]. Тому в системі забезпечення інформаційної безпеки важливе місце посідають такі категорії, як «суспільна безпека», «особиста безпека», «державна безпека».

Зокрема термін «безпека суспільства» або «суспільна безпека» почав вживатися у науковій літературі на початку 90-их років XX ст. Залишаючи осторонь визначення поняття безпека, все ж варто констатувати, що найперше воно стосується безпеки окремої людини, а вже потім суспільства та держави. А оскільки за сьогоднішніх умов життя людини поза суспільством чи державою не можливо, то ці поняття тісно переплітаються [92, с. 40].

Як зауважує Г. Мелеганич в українському законодавстві з питань національної безпеки термін «суспільна безпека» («безпека суспільства») не застосовують. Окремими науковцями та міжнародними нормами цей термін звужується до протидії злочинності (Декларація Організації Об'єднаних Націй про злочинність і суспільну безпеку). В такому ж контексті зустрічається і поняття «громадська безпека». Наприклад, у п. 7 ст. 138 та деяких законодавчих актах Конституції України [72]. Сучасне українське законодавство надає дещо розширене трактування терміну «громадська безпека – захищеність життєво важливих для суспільства та особи інтересів, прав і свобод людини і громадянина від протиправних посягань, надзвичайних ситуацій, які створюють загрозу спричинення шкоди життю, здоров'ю та майну значної кількості осіб, тобто тут йде мова про безпеку, дотримання якої входить у компетенції правоохоронних органів» [121]. Саме в такому розуміння поняття «громадська безпека» вживається і в щорічному посланні Президента України [92, с. 41].

Водночас термін «особиста безпека» як правило, стосується фізичної особи. У такому контексті вітчизняне законодавство трактує його як

«поточний стан захищеності її життєдіяльності від безпосередніх загроз її життю, здоров'ю, тілесній неушкодженості, а також особистій свободі» [139].

Загалом вбачається, що особиста безпека – цілеспрямований процес забезпечення функціонування та стійкого розвитку особи [108, с. 30]. Зазвичай її розглядають як законодавчо закріплене та гарантоване державою соціальне благо, що дозволяє людині безпечно здійснювати свої права та свободи. Тобто ця правова категорія являє собою складне системне утворення, що охоплює правове забезпечення, захищеність і реалізацію усієї сукупності прав і свобод людини і громадянина. Вона передбачає відсутність будь-яких загроз для людини, використання громадянами всіх, передбачених конституцією, громадянських, політичних, економічних, соціальних та культурних прав, верховенство закону, юридичну рівність та справедливість [179, с. 65].

Своєю чергою, термін «безпека держави» може вживатися як у широкому, як синонім терміну «національна безпека», так і у вузькому розумінні цього слова. У цьому випадку ми маємо зважати на те, що об’єктом забезпечення безпеки є не все те сумарне, комплексне, що існує і функціонує в державі, не загальні інтереси тощо, а саме лише держава, її основні ознаки [73, с. 74]. Уточнимо, що йдеться, приміром, про такі ознаки держави як:

– територія – це територіальна організація влади, тобто влада держави поширюється в межах державних територіальних кордонів, надає регулятивний вплив на всіх осіб, що перебувають на території держави, незалежно від їх належності до громадянства, національної приналежності, професії та інших особливостей;

– народ – це населення, що проживає на певній території, має певний зв’язок із державою, наприклад громадянство, підданство;

– публічна влада – держава обов’язково формує публічну владу, що виділена суспільством, і не збігається з населенням країни;

– суверенітет, або суверенна організація влади. Державний суверенітет означає самостійність, незалежність держави в здійсненні ним своєї політики,

як у межах своєї території, наприклад, внутрішній суверенітет; і в міжнародних відносинах, наприклад, зовнішній суверенітет, за умови поваги до суверенітету інших держав. У широкому тлумаченні термін «суверенітет» означає верховенство та незалежність влади держави всередині країни від будь-якої іншої влади, а також незалежність від інших держав у міжнародних відносинах;

– регулятивний інститут суспільства, інструмент, за допомогою якого соціум організує та розвиває у потрібному напрямку відносини між людьми. Сенс існування державної організації – в управлінні життям суспільства. Ухвалюючи та реалізуючи на практиці необхідні закони, держава впливає на найбільш значущі суспільні відносини;

– формування права, тобто це видання нормативних правових актів, що виражають волю держави та обов'язкових для загального виконання в усіх сферах життя. Право здійснює державну владу та робить її легітимною, визначаючи юридичні межі та форми здійснення функцій держави;

– наявність спеціального апарату примусу, що складається із системи правоохоронних органів та установ, що забезпечують реалізацію волі держави, тому числі й примусовими засобами;

– система податків та зборів, позик, які виступають головною частиною надходження до бюджету будь-якої держави та необхідні для проведення певної політики та утримання державного апарату;

– володіння певними матеріальними засобами для проведення своєї політики, наприклад, державна власність, бюджет тощо [169].

Саме на захист зазначених вище ознак направлені усі зусилля утворених державою інституцій при забезпеченні її безпеки [73, с. 74].

Також існує думка, що поняття «національна безпека», «державна безпека» і «безпека держави» є семантично схожими, але не тотожними, категорія «національна безпека» є ширшою за категорію «державна безпека» і співвідносяться як ціле і складник. Треба погодитися з тезою, що під час формування сучасної концепції безпеки повинен бути здійснений

принциповий вибір між концепціями, орієнтованими тільки на захист інтересів осіб, нації чи окремих держав, і концепціями цілеспрямованого впливу в інтересах нації, осіб і держави для найбільш повного задоволення їх потреб як цілісного організму [183, с. 72–73].

Нам, до речі, імпонує думка, що вжиття терміну «безпека держави» одночасно у широкому і вузькому розумінні цього слова, є не цілком зручним. Тому є доцільним його поділ на термін «безпека України», що рівнозначно терміну «безпека держави» у широкому розумінні цього слова як «національна безпека», та на термін «державна безпека», що рівнозначно терміну «безпека держави» у вузькому розумінні цього слова. Крім того, зазначене буде відповідати положенням морфології української мови в частині творення та правопису присвійних прикметників, що вказує на належність безпеки до того, чи іншого його виду чи підвиду [73, с. 74].

Узагальнюючи наведений матеріал маємо, що безпека як правова категорія охоплює різні рівні – індивідуальний, колективний і національний, які перебувають у тісному взаємозв’язку та взаємозалежності. При цьому кожен із зазначених рівнів передбачає наявність власних об’єктів захисту, серед яких в умовах сучасного розвитку особливе місце посідає інформація. Її слід розглядати як особливий нематеріальний об’єкт, що характеризується сукупністю специфічних властивостей та набуває юридичного значення лише за умови її включення у сферу правового регулювання.

Відповідно, нам імпонує думка, що терміни «інформаційна безпека» та «захист інформації» повинні розмежовуватись та застосовуватись у правильних контекстах. Однак, є важливе застереження: захист інформації є частиною забезпечення інформаційної безпеки, а отже, поглинання останнім особливостей попереднього не слід розглядати як помилковість. Відповідно, інформаційна безпека є станом захищеності, яка досягається на основі створення і упровадження ефективних систем захисту інформації [12].

Отже, у результаті проведеного дослідження видається можливим визначити, що інформація у широкому значенні постає як універсальна

характеристика реальності, що забезпечує процеси організації, взаємодії та розвитку систем різної природи, тоді як у вузькому, юридичному розумінні вона набуває ознак специфічного об’єкта правовідносин, зокрема і захисного спрямування, адже її обіг, збирання, зберігання та поширення можуть як сприяти реалізації прав людини, так і створювати загрози їх порушення. Інший контекст порушеного питання, – загальнодержавний, оскільки інформація виступає стратегічним ресурсом розвитку держави, важливим чинником забезпечення її суверенітету, національної безпеки та ефективного функціонування публічної влади.

Таким чином, інформацію як об’єкт правового захисту варто характеризувати через призму стратегічного ресурсу, що зумовлює необхідність її охорони не лише як об’єкта приватних прав, але і як елемента національної безпеки.

1.2. Зміст та сутність адміністративно-правового захисту інформації

Варто погодитись з тим, що інформаційна сфера характеризується високими темпами розвитку, що обумовлено зростанням ролі інформації та інформаційних ресурсів у всіх процесах суспільної життєдіяльності. Політичні, економічні, соціальні та культурні інститути в значній мірі відчувають вплив інформаційно-комп’ютерних технологій та змісту інформаційних продуктів, що поширюються за їх допомогою. Така тенденція трансформації значення суспільного інформаційного обміну вимагає активної державної діяльності з метою впорядкування інформаційних процесів, а проведення ефективної державної інформаційної політики набуває надзвичайної актуальності [22, с. 37].

Уточнимо, що за влучними узагальненнями Т. Савосько визначаючи поняття «інформаційної політики» науковці переважно дотримуються двох основних підходів: у вужчому та ширшому значенні. Науковці, що є

представниками вужчого підходу визначають інформаційну політику як сукупність напрямів та способів діяльності держави для отримання, використання, збереження та поширення інформації. Однак дехто з науковців вважає такий підхід надто одностороннім [168, с. 30].

Зокрема О. Токар справедливо стверджує, що зведення інформаційної політики лише до збору, використання і безпеки інформації надто звужує її як об'єкт аналізу. Так, враховуючи розвиток інформаційних технологій, їх проникнення у найважливіші сфери життя суспільства, необхідно брати до уваги перехід від принципу безпеки інформації до принципу інформаційної безпеки. Розгляд останньої з позицій системного підходу дозволяє побачити різницю між науковим розумінням проблеми і розумінням «повсякденним». У практиці державного управління інформаційна безпека розуміється лише як необхідність боротьби з відтоком закритої (таємної) інформації, а також з розповсюдженням хибної і ворожої інформації. Осмислення інформаційної безпеки в суспільстві ще тільки розпочинається. Тому, на її думку, таке бачення інформаційної політики є дещо спрощеним і не враховує цілий спектр завдань держави в інформаційній сфері [180, с. 133].

Дещо ширше розглядає інформаційну політику В. Пашкова, зокрема як «сукупність законів і положень, присвячених створенню, виробництву, збиранню, зберіганню та організації розповсюдження інформації і доступу до неї». На думку науковиці, важливість поняття «інформаційна політика» заключається в тому, що вона має вплив на шляхи, якими людина здатна зробити вибір соціальний, політичний й економічний [110; 168, с. 30]. Суміжною до такої думки є позиція Ю. Мохової та А. Луцької, які вважать, що інформаційна політика – це сукупність всіх громадських законів, правил і політик, які заохочують, перешкоджають або регулюють створення, використання, зберігання, доступ і передачу і поширення інформації [95]. Разом з цим вчені також вказують, що: «сучасна інформаційна політика в розвинених країнах – це сукупність напрямів і способів діяльності компетентних органів держави з контролю, регулювання та планування

процесів у сфері одержання, зберігання, оброблення, використання та поширення інформації» [95].

Науковці, що розглядають інформаційну політику з більш широкої позиції вважають, що вона є більш складним і багатокомпонентним явищем. Наприклад, Г. Почепцов вважає, що «інформаційна політика визначає закони функціонування інформаційної сфери. До таких законів відносяться: закон ефективної роботи системи ЗМІ, закон адекватної взаємодії влади і населення». Вчений виділяє ще один важливий аспект державної інформаційної політики – посилення інформаційної безпеки [124, с. 12]. Дещо подібно визначає інформаційну політику й О. Дубас акцентуючи увагу на тому, що «така політика має забезпечувати взаєморозуміння та взаємодію влади з суспільством за допомогою засобів масової інформації та громадські зв'язки, координацію висвітлення діяльності органів влади, захист свободи слова, задоволення інформаційних потреб особи і суспільства, формування високої інформаційної культури громадян» [50, с. 100; 168, с. 30].

О. Юдін і В. Богуш визначають інформаційну політику як головні напрями діяльності держави в галузі інформації. Основною її метою є створення умов для ефективного і якісного інформаційного забезпечення стратегічних і оперативних завдань соціального та економічного розвитку держави [197, с. 209]. Такими завданнями в економічний сфері, наприклад, можуть бути збереження, розвиток та ефективне використання об'єктів національного інформаційного простору, які мають стратегічне значення для економіки і безпеки України; забезпечення всебічної підтримки і захисту вітчизняного виробника інформаційного продукту, сприяння виробленню і впровадженню новітніх інформаційних технологій; економічна підтримка державою розвитку інформаційної інфраструктури та інформаційної системи, сприяння розробці і впровадженню новітніх інформаційних технологій [180, с. 134]. Водночас В. Карпенко вважає, що державна інформаційна політика охоплює як внутрішні, так і зовнішні аспекти діяльності країни. Внутрішня політика спрямована на якомога ширше задоволення інформаційних потреб

свого суспільства; зовнішня – на створення позитивного образу держави у світі, інформування світової громадськості про політичний, економічний, духовний, культурний, інвестиційний клімат в Україні, експорт на світовий інформаційний ринок українського продукту тощо [62, с. 147–148]. Своєю чергою, О. Соснін поняття інформаційної політики держави ототожнює з державною політикою інформатизації – побудовою інформаційного суспільства. Він зауважує, що інформатизація – це глобальний процес, який супроводжується кардинальною зміною структури і характеру світового економічного і соціального розвитку, переходом до наукомісткого виробництва, нових видів інформаційного обміну і впливає на більшість сфер суспільної діяльності, змінюючи характер світового розвитку, соціально-економічні відносини, рівень і якість життя всіх членів суспільства [176, с. 35–38]. З таким розумінням інформаційної політики, на думку О. Токар, можна погодитись лише частково, адже інформаційна політика включає набагато ширший спектр проблем; політику інформатизації доцільніше вважати складовою державної інформаційної політики, яка, окрім того, включає в себе посилення інформаційної безпеки, захист інформаційного суверенітету держави, забезпечення незалежності ЗМІ, розвиток інформаційної інфраструктури, захист права на свободу слова, права на інформацію тощо [180, с. 135].

Сама ж О. Токар стверджує, що під державною інформаційною політикою слід розуміти сукупність напрямів діяльності держави в інформаційній сфері, які ґрунтуються на певній нормативній базі і передбачають, насамперед, посилення інформаційної безпеки держави, суспільства, особи та мають внутрішнє і зовнішнє спрямування [180, с. 139]. Водночас Т. Савосько вважає що державна інформаційна політика є інструментом державного управління інформаційною сферою суспільства, що дає можливість впливати на інформаційні процеси та діяльність суб’єктів інформаційного простору і виконує ряд важливих функцій [168, с. 31].

На нашу думку, наведений матеріал дає розуміння того, що інформаційна політика держави може бути схарактеризована через низку визначальних властивостей, однак провідною з таких варто вважати цілеспрямованість та системність державного впливу на інформаційну сферу, яка забезпечує баланс між свободою доступу до інформації та її захистом, формує нормативні та організаційні умови для стійкого розвитку інформаційного простору.

Згідно нормативних положень, основними напрямами державної інформаційної політики є: забезпечення доступу кожного до інформації; забезпечення рівних можливостей щодо створення, збирання, одержання, зберігання, використання, поширення, охорони, захисту інформації; створення умов для формування в Україні інформаційного суспільства; забезпечення відкритості та прозорості діяльності суб'єктів владних повноважень; створення інформаційних систем і мереж інформації, розвиток електронного урядування; постійне оновлення, збагачення та зберігання національних інформаційних ресурсів; забезпечення інформаційної безпеки України; сприяння міжнародній співпраці в інформаційній сфері та входженню України до світового інформаційного простору [151]. Однак варто враховувати, що за сучасних умов першочерговим завданням державної інформаційної політики України є стримування та протидія загрозам інформаційній безпеці України та нейтралізація інформаційної агресії, у тому числі спеціальних інформаційних операцій держави-агресора, спрямованих на підрив державного суверенітету, територіальної цілісності України, забезпечення інформаційної стійкості суспільства та держави, створення ефективної системи взаємодії між органами державної влади, органами місцевого самоврядування та суспільством, а також розвиток міжнародної співпраці у сфері інформаційної безпеки на засадах партнерства та взаємної підтримки [157].

Відповідно, маємо підтвердження того, що забезпечення стійкого інформаційного середовища в Україні неможливе без реалізації захисної

діяльності, як однієї зі складових комплексного механізму управління інформаційною сферою.

Так положеннями Закону України «Про інформацію» від 02 жовтня 1992 року № 2657-XII передбачено, що під категорію «захист інформації» варто розуміти «сукупність правових, адміністративних, організаційних, технічних та інших заходів, що забезпечують збереження, цілісність інформації та належний порядок доступу до неї» [151].

Ми поділяємо думку Т. Перуна, що головну роль в ефективності захисту інформації має відігравати адміністративне право як право, яке регламентує управлінську діяльність суб'єктів забезпечення інформаційної безпеки. Вчений зауважує, – «норми адміністративного права забезпечують реалізацію механізму управління в різних сферах життєдіяльності, встановлюють відповідні правові режими, які повинні стати ефективним інструментом державного управління в досліджуваній сфері» [111, с. 16].

Зауважимо, що з боку наукової доктрини термін «правовий захист» в адміністративному праві здебільшого зводиться до діяльності компетентних органів державної влади, органів управління і місцевого самоуправління [181, с. 116–117], яка об'єктивує реалізацію відповідних заходів. Спеціалізовано означена діяльність іменується як адміністративно-правовий захист [192, с. 25].

Однак варто зауважити, що національне законодавство та наукові джерела іноді використовують для позначення одного і того ж явища різні терміни. До таких термінів відносяться терміни «охорона» та «захист». Як зазначає О. Коцовська в законодавстві відсутнє тлумачення цих понять, тим більше, інколи видається, що законодавець використовує ці терміни в одних випадках як синоніми, в інших – як різні за змістом. Тлумачні словники української мови також не дають чіткого визначення згаданих вище понять і, переважно, не розмежовують їх за змістом та не дають нам відповіді на питання про конкретний зміст та співвідношення понять «охорона» та «захист» [29, с. 38; 78, с. 270–271]. Тому цілком зрозуміло, чому наукові праці

не містять єдиної точки зору щодо розуміння правової категорії «адміністративно-правовий захист». Л. Кожура уточнює, що часто вказане поняття ототожнюється з такими термінами, як «адміністративно-правове забезпечення» чи навіть «адміністративно-правова охорона», а також використовується у вузькому та широкому розумінні з різним змістовним навантаженням [66, с. 119]. Приміром М. Шиленко при досліджені одного з видів адміністративно-правової охорони ототожнює її із захистом [194, с. 1193]. К. Гарбузюк стверджує, що аналіз дозволяє виділити у його дефініції об'єкт охорони (захисту) – суб'єкт малого підприємництва, а в якості суб'єкта охорони (захисту) – публічну адміністрацію [29, с. 38]. Натомість вчена О. Єщук вважає, що адміністративно-правова охорона є широким поняттям, вона включає в себе дефініцію адміністративно-правового захисту [52, с. 53].

Варто вказати також те, що за загальним контекстом означений термін є застосовним до правовідносин захисту прав, свобод та законних інтересів особи (осіб) [192, с. 25]. Навіть законодавче визначення категорії «захист інформації» є тому підтвердженням. Проте його зміст виходить за межі лише інтересів окремих фізичних чи юридичних осіб, оскільки охоплює й публічний інтерес, безпосередньо пов'язаний з безпекою інформаційного середовища [11].

Тому нам імпонує твердження, що адміністративно-правовий захист, як і адміністративно-правова охорона чи адміністративно-правове забезпечення, логічніше розглядати з позиції самостійних врегульованих процесів, що мають різні завдання та механізми реалізації. Узагальнено та схематично їх співвідношення можна представити так: забезпечення спрямовується на охорону та захист, а охорона та захист – реалізовуються у тісній взаємодії. Причому саме визначення адміністративно-правового захисту має розглядатись з дуальної інтерпретації об'єктної складової. Мається на увазі, що окрім юридичного відношення особи до конкретного інтересу (як правило, права на щось) має враховуватись його безпосередній стан з позиції

убезпечення від зміни властивостей чи характеристик, руйнування або загалом знищення [192].

Така думка видається цілком обґрунтованою, адже за влучними твердженнями Т. Перуна як і будь-який інший товар, інформація має власника, який володіє правом розпоряджатися інформацією на свій розсуд, а її несанкціоноване використання тягне за собою матеріальні втрати для її правовласника, несанкціоновані дії з інформацією стають підставою для настання шкоди для держави, громадян, суб'єктів господарювання [111, с. 27]. Водночас, як зауважено попередньо, у сучасних умовах інформація стає стратегічним ресурсом, правий захист якої диктується необхідністю розвитку економіки, формування громадянського суспільства, забезпечення безпеки держави та громадян [111, с. 28].

Таким чином, адміністративно-правовий захист інформації визначаємо як різновид діяльності органів публічної адміністрації, що безпосередньо пов'язаний із забезпеченням стійкості інформаційного середовища індивідуального, колективного та національного рівнів через реалізацію заходів попереджувального та реагувального характеру, спрямованих на запобігання порушенням, відновлення порушених прав та інтересів суб'єктів інформаційних відносин, а також створення умов для безпечного використання інформації як стратегічного ресурсу в публічних цілях.

Нагадаємо, що індивідуальний, колективний та національний рівні інформаційного середовища є взаємопов'язаними. Тому об'єктами адміністративно-правового захисту інформації є будь-які види інформації, з приводу якої суб'єкти права вступають у певні правовідносини та здійснюють свої права та обов'язки. Слід зазначити, що усі види інформації в Україні згідно законодавства мають певний порядок доступу, що надає їй відповідний правовий статус. Так, відповідно до статті 20 Закону України «Про інформацію» за порядком доступу інформація поділяється на відкриту інформацію та інформацію з обмеженим доступом [16, с. 127; 151]. Відповідно, слід виокремлювати два базових різновиди адміністративно-

правового захисту інформації, зокрема об’єктом якого є відкрита інформація або інформація з обмеженим доступом.

Приміром, В. Бєлєвцева адміністративно-правовий захист інформації з обмеженим доступом визначає як сукупність засобів попередження, припинення та примусу, які вживаються власниками інформації з обмеженим доступом або іншими суб’єктами, які мають адміністративно-юрисдикційні повноваження з метою запобігання заподіянню шкоди інтересам власника інформації та її неконтрольованому використанню [16, с. 129]. Ми більш схильні до думки, що адміністративно-правовий захист інформації з обмеженим доступом має на меті гарантування прозорості діяльності держави та реалізацію права громадян на інформацію. Водночас адміністративно-правовий захист відкритої інформації стосується забезпечення реалізації конституційного права кожного на вільний доступ до інформації, а також на недопущення неправомірних обмежень чи ускладнень у користуванні нею.

Таким чином, за заявленим аспектом адміністративно-правовий захист інформації виступає ключовим механізмом реалізації державної інформаційної політики, забезпечуючи належне функціонування правового режиму доступу до відкритої та обмеженої інформації в безпековому контексті.

Однак, на нашу думку, це лише однин із варіантів розгляду змістової структури адміністративно-правового захисту інформації, адже, як з’ясовано нами попередньо, в правовому контексті категорії конфіденційності, цілісності та доступності виступають не лише характеристиками інформації, а й концептуальною основою формування системи її захисту. У цьому сенсі адміністративно-правовий захист виступає не просто набором окремих державних заходів чи механізмів, а цілісною системою інструментів, що спрямовані на підтримку стабільності інформаційного середовища на всіх рівнях – від індивідуального до національного.

Приміром, ще у 2018 році Л. Кочубей у контексті російсько-української війни відзначала, що інструментарій захисту українського інформаційного поля може включати [80]:

1) максимальне підвищення поінформованості населення про реальний стан подій на Сході України, зокрема, проведення PR-кампаній, створення роликів про ситуацію на Сході, відносини між різними національними меншинами (підвищення рівня критичного сприйняття інформації з боку активних верств суспільства задля мінімізації поширення чуток як фактора інформаційного впливу на розвиток конфліктів та загострення суперечностей у суспільстві);

2) боротьбу із розгалуженою мережею агентів впливу серед місцевого населення для поширення чуток;

3) пояснення діяльності армії має бути, особливо для населення прифронтових територій ворога. Обізнаність громадськості щодо реальної ситуації на фронтах формуватиме громадський тиск на владу, навести лад і забезпечити ефективність армії;

4) регулярне відстеження аналітиками з інформаційної безпеки (зокрема, діяльність такої групи фахівців запланована при Міністерстві інформаційної політики) інформації та новин із соціальних мереж, обговорення їх та вироблення пропозицій для формування «порядку денного» на місцях;

5) українські ЗМІ спрямувати свої зусилля протидії російській пропаганді не лише на зону небойових дій, а для громадян окупованих територій, які не отримують правдивої інформації. Тобто, створювати медіа-контент, спрямований на аудиторію окупованих територій. Асиметрична реакція на технології, що застосовуються на Донбасі, – максимально чесний діалог з власним народом. Щоб бути ефективними, необхідно уникати спроб змагатися з ворогами у брехні. Діяльність української влади мусить бути прозорою, адже саме закритість, кулуарність ухвалення рішень створюють сприятливий режим для локальних маніпуляторів;

6) PR-кампанії, спрямовані до російських журналістів із закликом дотримуватися «клятви Гіппократа для ЗМІ»; з метою підвищення відповідальності журналістів під час здійсненні своїх професійних обов'язків та дотримання етичних стандартів розробити та внести зміни до чинного законодавства України (наприклад, до статті 25 Закону України «Про інформацію»), передбачивши відповідальність за порушення професійних стандартів тощо;

7) діяльність «StopFake» в Україні. Громадські організації та рухи в межах своїх можливостей намагаються проводити певну діяльність, але ці можливості надто обмежені. Ініціативи на кшталт StopFake та «Не Формат» викривають пропаганду, і це має вплив на ситуацію в тилу;

8) створення сайту «Інформаційних військ України»: що дозволить досить оперативно надавати правдиві новини та спростовувати фейкові новини людям, які на неї підписалися. Завдання полягає у забезпеченні дуже швидкого донесення правди через Інтернет [80].

Звісно, не всі наведені заходи мають адміністративно-правову природу, адже з числа таких чітко виокремлюються державні, громадські та медійні інструменти. Однак, на нашу думку, адміністративно-правовий захист забезпечує правову основу і рамки для реалізації цих заходів, тоді як громадські ініціативи та медійні кампанії виконують роль оперативного реагування та соціальної мобілізації, підвищуючи ефективність державних рішень.

Суто адміністративні заходи захисту інформації, на нашу думку, представлені такою системою:

1) нормотворчі – передбачають розробку та прийняття нормативів, що встановлюють правила доступу до інформації, порядок її збирання, обробки, зберігання та поширення, а також визначають відповідальність за порушення режиму інформаційної безпеки. У цьому контексті йдеться як про нормативно-правові акти загальної та індивідуальної сили, так і про акти реагування та документи, якими оформлюються відповідні домовленості;

2) превентивні – спрямовані на запобігання порушенням прав на інформацію та загрозам інформаційній безпеці. До них належать контроль за дотриманням правил доступу до інформації, інструктажі та навчання працівників, проведення інформаційно-просвітницьких кампаній, аудит інформаційних систем, моніторинг інформаційного середовища та раннє виявлення потенційних загроз;

3) оперативні – реалізуються у разі фактичного порушення інформаційної безпеки та передбачають невідкладні дії щодо локалізації загроз і нейтралізації негативних наслідків. Це можуть бути тимчасові обмеження доступу до інформації, блокування неправомірних джерел, реагування на спроби несанкціонованого втручання або поширення дезінформації, а також координація між різними суб’єктами інформаційного простору;

4) відновлювальні – спрямовані на відновлення порушених прав та цілісності інформації, ліквідацію наслідків інформаційних порушень та забезпечення стійкості інформаційного середовища у майбутньому. Йдеться зокрема про відновлення доступу до обмеженої або заблокованої інформації, публічні спростування фейків, компенсаційні дії, а також впровадження додаткових заходів контролю для запобігання повторних порушень.

Разом з тим вбачаємо доречним уточнити питання щодо співвідношення превентивних інструментів адміністративно-правового захисту та адміністративно-правової охорони, оскільки на перший погляд їх змістовне наповнення є подібним.

Однак відмінність є. Вона полягає у цільовій спрямованості та функціональному контексті застосування. Так, превентивні інструменти адміністративно-правової охорони мають загально-регулятивний, стабілізаційний характер і спрямовані на формування належного правового режиму інформаційних відносин, у межах якого мінімізується сама можливість виникнення правопорушень. Натомість превентивні інструменти адміністративно-правового захисту, хоча і мають попереджувальний

характер, однак застосовуються вже в умовах наявності підвищених ризиків, загроз або передумов до порушення прав на інформацію чи інформаційної безпеки. Тобто їх превентивність є більш цільовою та ризик-орієнтованою, а не загальною.

Отже, враховуючи зазначене обґрунтовуємо тезис про те, що адміністративно-правовий захист інформації загалом є способом реалізації державної інформаційної політики, що здійснюється через комплекс заходів, спрямованих на гарантування балансу між правом на доступ до інформації та необхідністю її захисту від загроз.

Варто також уточнити, що такі загрози розглядаються як правило через призму національної безпеки. Їх трактують як сукупність умов та чинників, які становлять небезпеку життєво важливим інтересам держави, суспільства та особи через можливість негативного інформаційного впливу на свідомість та поведінку громадян, а також на інформаційні ресурси та інформаційно-технічну інфраструктуру [112, с. 2]. До числа таких з позиції вітчизняного законодавства відносяться:

– збільшення кількості глобальних дезінформаційних кампаній – глобальні дезінформаційні кампанії, що інспіруються авторитарними урядами та активістами радикальних рухів для маніпулювання свідомістю окремих людей та груп населення, стали повсякденною практикою, яка загрожує демократичному розвитку держав та міжнародній стабільності;

– інформаційна політика Російської Федерації – загроза не лише для України, але й для інших демократичних держав;

– соціальні мережі як суб'єкти впливу в інформаційному просторі – збільшення кількості соціальних мереж, їх інтегрованість з іншими соціальними сервісами повсякденного користування, а також специфіка організації всесвітньої мережі Інтернет ставлять під загрозу гарантії права особи на приватність;

– недостатній рівень медіаграмотності (медіакультури) в умовах стрімкого розвитку цифрових технологій – некритичне сприйняття

інформації створює загрози політичній та економічній стабільності демократичних держав;

– інформаційний вплив Російської Федерації як держави-агресора на населення України;

– інформаційне домінування Російської Федерації як держави-агресора на тимчасово окупованих територіях України;

– обмежені можливості реагувати на дезінформаційні кампанії – деструктивна пропаганда, поширення дезінформації як ззовні, так і всередині України застосовуються державою-агресором з метою підриву стійкості суспільства та інформаційної дестабілізації держави. Водночас ефективна система реагування на такі виклики в Україні досі не створена, не забезпечено функціонування розвиненої національної інформаційної інфраструктури, що обмежує можливість належним чином протидіяти інформаційній агресії з метою захисту національної безпеки та реалізації національних інтересів України;

– несформованість системи стратегічних комунікацій – органами державної влади України здійснено низку організаційних та практичних заходів зі зміцнення власної інституційної спроможності у сфері стратегічних комунікацій, однак не створено дієвого механізму координації і взаємодії між усіма органами державної влади, залученими до здійснення заходів із протидії загрозам в інформаційній сфері. Зазначене послаблює можливості до розбудови комплексного стратегічного планування інформаційного потоку, здійснення системної комунікативної діяльності Кабінету Міністрів України, об'єднання всіх ключових суб'єктів у сфері інформаційних відносин, суб'єктів формування і реалізації державної політики щодо ефективного захисту національного інформаційного простору, утвердження позитивного іміджу України, реалізації цілей захисту національної безпеки України в інформаційній сфері;

– недосконаліть регулювання відносин у сфері інформаційної діяльності та захисту професійної діяльності журналістів – є непоодинокі

випадки втручання в професійну організаційно-творчу діяльність засобів масової інформації та в індивідуальну професійну творчу діяльність журналістів, інші посягання на свободу інформаційної діяльності, зокрема перешкоджання їх професійній діяльності, погрози, насильство щодо них, посягання на їх життя та власність. Зазначене позбавляє журналістів можливості належним чином інформувати суспільство про суспільно важливі події та явища;

– спроби маніпуляції свідомістю громадян України щодо європейської та євроатлантичної інтеграції України – здійснюються спроби маніпуляції свідомістю громадян України шляхом поширення міфів та дезінформаційних (деструктивних) стереотипів щодо ЄС і НАТО з метою послаблення консолідації суспільства щодо зовнішньополітичного курсу України, гальмування проведення реформ, що негативно впливає на загальну суспільно-політичну ситуацію в державі;

– доступ до інформації на місцевому рівні – інформаційні потреби на місцевому рівні належним чином не задовольняються, зокрема через низьку спроможність забезпечення населення послугами з доступу до Інтернету;

– недостатній рівень інформаційної культури та медіаграмотності в суспільстві для протидії маніпулятивним та інформаційним впливам – відсутність належного рівня інформаційної культури та медіаграмотності в суспільстві в умовах стрімкого розвитку цифрових технологій створює підґрунтя для маніпулювання громадською думкою, проведення стрімких деструктивних інформаційних операцій, що зумовлює існування потенційних та реальних загроз інформаційній безпеці України [157].

Суттєвого негативного впливу на інформаційну безпеку додає й широке використання терористичними і екстремістськими організаціями світових інформаційних ресурсів і механізмів інформаційного впливу для поширення ідеології тероризму, нагнітання міжнаціональної і соціальної напруженості і т. д. Діяльність терористів також перемістилася в інформаційний простір, дане напрямок названо «інформаційний тероризм», або «кібертероризм»

[173]. Тому наразі однією з основних загроз інформаційної безпеки України є загроза комп'ютерних атак (хакерських операцій) на інформаційні мережі, інформаційні державні системи та інформаційні системи персональних даних, кредитно-фінансову сферу [46].

Таким чином, у результаті проведеного дослідження видається можливим визначити такі ключові тези:

– адміністративне право в механізмі формування стійкого інформаційного середовища в Україні відіграє одну із ключових ролей, адже з-поміж того, що визначає порядок організації та функціонування органів публічної адміністрації, що здійснюють адміністративно-правовий захист інформації, також забезпечує організаційну основу для реалізації інших важливих заходів, пов'язаних із протидією інформаційним загрозам, безперервністю перебігу важливих інформаційних процесів, впровадженням цифрових рішень в буденність тощо;

– адміністративно-правовий захист інформації слід розглядати як самостійний різновид діяльності органів публічної адміністрації, спрямований на забезпечення стійкості інформаційного середовища різних рівнів. Його зміст охоплює комплекс нормативних, превентивних, оперативних та відновлювальних інструментів, реалізація яких забезпечує як гарантування інформаційних прав особи, так і захист національних інтересів у інформаційній сфері;

– максимально узагальнено адміністративно-правовий захист інформації можемо визначити як систему заходів, застосовних уповноваженими представниками публічної адміністрації задля забезпечення захищеності інформації, що є об'єктом адміністративно-правового захисту. Водночас об'єктами адміністративно-правового захисту виступають усі види інформації, правовий режим доступу до яких визначений чинним законодавством.

1.3. Правові засади діяльності органів публічної адміністрації у сфері захисту інформації

Посилення спроможностей щодо забезпечення інформаційної безпеки держави, її інформаційного простору, підтримки інформаційними засобами та заходами соціальної та політичної стабільності, оборони держави, захисту державного суверенітету, територіальної цілісності України, демократичного конституційного ладу, забезпечення прав та свобод кожного громадянина є однією з найважливіших функцій держави [157]. Щонайменше про це йдеться у Стратегії інформаційної безпеки, яка визначає, що захист і протидія нанесенню шкоди через поширення негативних інформаційних впливів, у тому числі скоординоване поширення недостовірної інформації, деструктивної пропаганди, інших інформаційних операцій, несанкціоноване розповсюдження, використання й порушення цілісності інформації з обмеженим доступом [157] є державним пріоритетом.

Зазначене свідчить про те, що держава, усвідомлюючи потребу в реалізації такої діяльності, уповноважує на здійснення відповідних заходів забезпечення інформаційної безпеки різних рівнів конкретних виконавців.

З попередньо висвітленого матеріалу стає зрозумілим, що йдеться безпосередньо про органи публічної адміністрації у сфері захисту інформації. Однак для повноти та ґрунтовності розкриття порушених питань варто уточнити, що досі адміністративно-правова галузь наукових знань не визначилась досконально з тим, представники якого рівня влади та яких структур формують систему публічної адміністрації загалом, зокрема і у досліджуваній сфері.

Уточнимо, що з доктринального дискурсу публічною адміністрацією іменується сукупність органів виконавчої влади та органів виконавчого самоврядування, підпорядкованих політичній владі, які забезпечують виконання закону та здійснюють інші публічно-управлінські функції [1].

Означене визначення запропонував В. Авер'янов, який нині вбачається одним з основних фундаментаторів розвитку вітчизняного адміністративного права.

Окремими адміністративістами його думка піддається критиці щодо суб'єктного складу публічної адміністрації, однак вчені погоджуються з тим, що означена категорія є репрезентацією системи органів влади, які виконують адміністративно-виконавчі функції, основне призначення яких полягає у забезпеченні публічних інтересів та вирішені індивідуальних адміністративних справ [13].

Маємо враховувати, що Україна здобула незалежність у 1991 році. Особливістю становлення публічної адміністрації в Україні було те, що, перебуваючи у складі СРСР, республіка не мала досвіду самостійного прийняття рішень та навіть повноцінної мережі адміністративних органів. Адже в СРСР рішення на усіх рівнях (від центрального до місцевого) приймалися компартійними органами [161]. Тому не викликає подиву той факт, що суб'єктний склад публічної адміністрації України вченими визначається з позиції варіативності.

Законодавча доктрина щодо означеного теж мало інформативна. Вітчизняні нормативно-правові акти не апелюють цим терміном, у зв'язку з чим його характеристика вченими об'єктивується через положення КАС України, який передбачає, що суб'єктом владних повноважень (а отже, органом чи посадовою особою, що безпосередньо вирішує питання публічного та одиничного інтересу у спосіб реалізації відповідних дій) є орган державної влади (у тому числі без статусу юридичної особи), орган місцевого самоврядування, орган військового управління, їх посадова чи службова особа, інший суб'єкт при здійсненні ними публічно-владних управлінських функцій на підставі законодавства, в тому числі на виконання делегованих повноважень, або наданні адміністративних послуг [65].

Тому вважаємо, що суб'єктний склад досліджуваної публічної адміністрації варто визначати враховуючи нормативний контекст, тобто на підставі аналізу вітчизняного законодавства, що безпосередньо регламентує

повноваження органів державної влади та місцевого самоврядування у сфері захисту інформації.

При цьому варто зауважити, що за загальним контекстом з боку нормотворців, окремих представників публічної влади, а також деяких науковців масив відповідних актів іменується як «правові засади». Наприклад, Ю. Шпарага вбачає, що правові засади є сукупністю чинних нормативно-правових актів, розкриття яких здійснюється з урахуванням юридичної сили правових актів, що врегульовують певні відносини [196, с. 134]. Однак є і виключення із зазначеного правила, адже окремі вчені вбачають, що правовими засадами є:

– нормативно закріплені вихідні положення, які визначають організацію та функціонування державних інститутів (М.П. Орзіх, 2003) [106];

– сукупність правових норм і принципів, що встановлюють основи діяльності органів виконавчої влади та інших суб'єктів публічного адміністрування (В.Б. Авер'янов, 2007) [2];

– закріплені в нормативно-правових актах вихідні ідеї, принципи та правила, які визначають мету, завдання і механізм правового регулювання відповідної сфери (Ю.П. Битяк, 2012) [17];

– комплекс нормативно закріплених принципів, цілей і правових інструментів, які забезпечують регулювання певної сфери суспільних відносин (О.В. Кузьменко, 2019) [84].

Тож влучним є узагальнення Д. Кошикова, який зазначає, що поняття «правові засади» науковцями розуміються у декількох аспектах: 1) як система нормативно-правових актів, що регулює певну сферу суспільних відносин або функціонування їх суб'єктів; 2) як норми права, що встановлюють певні правила діяльності суб'єктів суспільних відносин, що містяться в законодавчих актах; 3) як керівні начала (принципи) відповідної діяльності окремих органів, що закріплені нормами відповідних законодавчих та підзаконних актів [81, с. 165; 166, с. 39]. Ми ж прибічники ж прибічники

думки, що це нормативна основа (система нормативно-правових актів), що окреслює: 1) цілі та завдання адміністративно-правового захисту інформації; 2) принципи здійснення такої діяльності; 3) повноваження органів публічної адміністрації у цій сфері; 4) правові механізми реалізації їхньої компетенції у цій сфері.

Зауважимо, що наукова спільнота визначає, що у широкому сенсі правовим фундаментом для правового захисту інформації виступає національне інформаційне право, предметом якого саме і є «суспільні відносини, що виникають з приводу встановлення режимів та форм обігу інформації, реалізації інформаційних прав і правового статусу суб'єктів інформаційних процесів і формування їх правомірної поведінки і зв'язків [74]. У вузькому сенсі мова йде про необхідність створення підсистеми організаційно-правового захисту інформації, яка ґрунтується на базі різних документів [87].

На нашу думку, з урахуванням специфіки сфери захисту інформації, варто запропонувати таку класифікацію нормативно-правових актів, що регулюють діяльність органів публічної адміністрації у цій сфері.

1. Конституційні та базові акти – йдеться про ті, що визначають загальні принципи функціонування та розвитку інформаційних відносин, а також гарантії прав людини і громадянина в інформаційній сфері. До числа таких відносяться:

а) Конституція України, в якій закладено фундамент інформаційних відносин через: а) гарантії доступу до інформації (стаття 32, право особи на доступ до інформації про себе; стаття 50, гарантує право на доступ до інформації про стан довкілля, якість продуктів тощо; стаття 57, закріплює право знати свої права і обов'язки – тобто доступності нормативно-правової інформації; б) захист приватності та персональних даних (стаття 32, гарантує право на невтручання в особисте і сімейне життя, а також: забороняє збирання, зберігання, використання та поширення конфіденційної інформації без згоди особи); в) свободу інформаційної діяльності (стаття 34, гарантує

свободу думки і слова; закріплює право вільно збирати, зберігати, використовувати і поширювати інформацію; визначає можливість обмеження цього права в інтересах національної безпеки, територіальної цілісності, громадського порядку тощо; стаття 31, забезпечує таємницю листування, телефонних розмов, телеграфної та іншої кореспонденції); г) обов'язок держави забезпечувати інформаційну безпеку (стаття 17, визначає забезпечення інформаційної безпеки як одну з найважливіших функцій держави) [72];

б) Закони України:

– «Про інформацію», цей закон визначає загальні правові засади інформаційних відносин, види інформації та принципи її обігу. Так, стаття 5 цього Закону закріплює право кожного на інформацію, що зобов'язує органи публічної адміністрації забезпечувати доступ до неї; стаття 6 – визначає основні принципи інформаційних відносин (відкритість, доступність, достовірність); стаття 21 – встановлює види інформації з обмеженим доступом (конфіденційна, таємна, службова), що є основою для її захисту [151]. Таким чином, закон формує загальну нормативну основу інформаційної діяльності (створення, збирання, одержання, зберігання, використання, поширення, охорона та захист інформації);

– «Про доступ до публічної інформації», що регулює порядок доступу до інформації, якою володіють органи публічної влади. Наприклад, стаття 3 визначає гарантії забезпечення права на доступ до публічної інформації; стаття 5 – засади доступу до інформації; стаття 22 передбачає підстави для відмови в доступі до інформації [132]. Загалом зазначений закон визначає обов'язки органів публічної адміністрації щодо надання інформації, забезпечуючи баланс між відкритістю і обмеженнями;

– «Про захист персональних даних», який регулює правові відносини, пов'язані із захистом і обробкою персональних даних, і спрямований на захист основоположних прав і свобод людини і громадянина, зокрема права на невтручання в особисте життя, у зв'язку з обробкою персональних даних.

Так стаття 6 встановлює принципи обробки персональних даних (законність, цільове призначення, пропорційність); стаття 10 визначає права суб'єкта персональних даних; стаття 24 – покладає на органи публічної адміністрації обов'язок забезпечувати захист персональних даних [150]. Окремо варто звернути увагу на те, що стаття 23 Закону визначає повноваження Уповноваженого Верховної Ради України з прав людини у сфері захисту персональних даних.

2. Спеціальні акти у сфері захисту інформації. Йдеться про акти, які а) безпосередньо регулюють питання забезпечення безпеки інформації, а також інші акти, що б) встановлюють вимоги до технічного та криптографічного захисту інформації.

До першої групи актів можна віднести закони України:

– «Про захист інформації в інформаційно-комунікаційних системах». Цей закон визначає правові та організаційні засади забезпечення захисту інформації в інформаційно-комунікаційних системах (ІКС), зокрема тих, що використовуються органами публічної адміністрації. Наприклад, стаття 1 визначає основні терміни, зокрема поняття захисту інформації в ІКС як діяльності, спрямованої на запобігання несанкціонованому доступу, втраті чи спотворенню інформації; стаття 9 встановлює обов'язок власників і розпорядників систем забезпечувати захист інформації відповідно до встановлених вимог; стаття 10 визначає повноваження державних органів у сфері захисту інформації в системах [149]. Міститься також норма про те, що органи державної влади, державні органи, органи місцевого самоврядування з урахуванням набору мінімальних вимог щодо заходів захисту (базового профілю безпеки), відповідних стандартів, політик безпеки, призначення системи, її структурно-функціональних характеристик, результатів аналізу ризиків безпеки та особливостей функціонування системи розробляють та затверджують цільові профілі безпеки для інформаційних, електронних комунікаційних, інформаційно-комунікаційних та технологічних систем, власником або розпорядником яких вони є [149]. Тобто закон регламентує не

тільки технічний, а й організаційний аспект діяльності органів публічної адміністрації, зобов'язуючи їх забезпечувати належний рівень захисту інформаційних систем, власником або розпорядником яких вони є;

– «Про державну таємницю» – закон, що встановлює правові засади віднесення інформації до державної таємниці, порядок її охорони та доступу до неї. Стаття 1 Закону визначає поняття державної таємниці як виду інформації з обмеженим доступом, розголошення якої може завдати шкоди національній безпеці; стаття 8 – встановлює категорії інформації, що може бути віднесена до державної таємниці; стаття 18 визначає основні організаційно-правові заходи щодо охорони державної таємниці; стаття 22 регулює допуск громадян до державної таємниці, а стаття 31 регулює питання обмеження на оприлюднення секретної інформації [130]. Отже, закон визначає спеціальний правовий режим інформації, що має підвищений рівень захисту та встановлює обов'язки органів публічної адміністрації щодо забезпечення її схоронності;

– «Про основні засади забезпечення кібербезпеки України», що визначає правові та організаційні основи забезпечення захисту життєво важливих інтересів людини і громадянина, суспільства та держави, національних інтересів України у кіберпросторі, основні цілі, напрями та принципи державної політики у сфері кібербезпеки, повноваження державних органів, підприємств, установ, організацій, осіб та громадян у цій сфері, основні засади координації їхньої діяльності із забезпечення кібербезпеки [154]. Стаття 1 містить визначення кіберзахисту як сукупності організаційних, правових, інженерно-технічних заходів, а також заходів криптографічного та технічного захисту інформації, спрямованих на захист від кіберзагроз, забезпечення кібербезпеки, стійкості, цілісності, доступності та конфіденційності інформаційних ресурсів у кіберпросторі, а також здатності інфраструктури до їх обробки; стаття 5 суб'єктами забезпечення кібербезпеки визначає Президента України, Національний координаційний центр кібербезпеки як робочий орган Ради національної безпеки і оборони

України, Кабінет Міністрів України, а також: 1) міністерства та інші центральні органи виконавчої влади; 2) місцеві державні адміністрації; 3) органи місцевого самоврядування; 4) правоохоронні, розвідувальні і контррозвідувальні органи, суб'єктів оперативно-розшукової діяльності; 5) Збройні Сили України, інші військові формування, утворені відповідно до закону; 6) Національний банк України; 7) операторів критичної інфраструктури та власників або розпорядників об'єктів критичної інформаційної інфраструктури; 8) суб'єктів господарювання, громадян України та об'єднань громадян, інших осіб, які провадять діяльність та/або надають послуги, пов'язані з національними інформаційними ресурсами, інформаційними електронними послугами, здійсненням електронних правочинів, електронними комунікаціями, захистом інформації та кіберзахистом [154].

Щодо другої групи нормативно-правових актів, в якості прикладу можна навести наказ Адміністрації Державної служби спеціального зв'язку та захисту інформації України від 16 грудня 2025 року № 832, яким було затверджено «Порядок формування програми робіт із стандартизації криптографічного та технічного захисту інформації, кіберзахисту, протидії технічним розвідкам, технічної перевірки проєкту стандарту криптографічного та технічного захисту інформації, кіберзахисту, протидії технічним розвідкам, розсилання, перевірки та перегляду стандартів криптографічного та технічного захисту інформації, кіберзахисту, протидії технічним розвідкам, ведення їх каталогу». Цей Порядок визначає процедури з формування програми робіт із стандартизації криптографічного та технічного захисту інформації, кіберзахисту, протидії технічним розвідкам, технічної перевірки проєкту стандарту криптографічного та технічного захисту інформації, кіберзахисту, протидії технічним розвідкам, розсилання, перевірки та перегляду стандартів криптографічного та технічного захисту інформації, кіберзахисту, протидії технічним розвідкам, ведення їх каталогу [147].

3. Акти стратегічного планування, які визначають основи державної політики у сфері захисту інформації в Україні. До таких можна віднести, приміром: Стратегію кібербезпеки України» та план заходів на 2025 рік з реалізації Стратегії кібербезпеки України», що передбачають координацію діяльності органів публічної адміністрації, розподіл повноважень між ними та впровадження сучасних механізмів реагування на кіберзагрози. Також можна вести мову про: а) Стратегію інформаційної безпеки, яка визначає основні загрози національній безпеці в інформаційній сфері, окреслює пріоритетні напрями державної політики щодо протидії дезінформації, інформаційним операціям та іншим формам деструктивного інформаційного впливу, а також встановлює засади формування стійкості інформаційного простору держави; б) Стратегію національної безпеки України, якою окреслено загрози інформаційному суверенітету та напрями їх нейтралізації; в) Стратегію розвитку інформаційного суспільства в Україні, яка визначає мету, базові принципи, стратегічні цілі розвитку інформаційного суспільства в Україні, завдання, спрямовані на їх досягнення; г) Концепцію розвитку електронного урядування в Україні, що покликана забезпечити модернізацію публічних послуг та розвиток взаємодії влади, громадян і бізнесу за допомогою інформаційно-комунікаційних технологій; модернізацію державного управління за допомогою інформаційно-комунікаційних технологій; управління розвитком електронного урядування.

4. Акти інституційного характеру – визначають правовий статус і повноваження органів публічної адміністрації у сфері захисту інформації, а також забезпечують права працівників вказаних органів. Наприклад, Закон України «Про Кабінет Міністрів України» встановлює повноваження уряду, зокрема й у сфері регулювання інформаційний відносин; Закон України «Про центральні органи виконавчої влади» визначає систему, статус і компетенцію міністерств та інших ЦОВВ в загальних контекстах; Закон України «Про Службу безпеки України» окреслює повноваження цього суб’єкта у сфері інформаційної безпеки та захисту державної таємниці; Закон України «Про

Державну службу спеціального зв'язку та захисту інформації України» встановлює статус органу, що забезпечує технічний і криптографічний захист інформації; Закон України «Про Уповноваженого Верховної Ради України з прав людини» визначає правовий статус, завдання та повноваження цього суб'єкта у сфері парламентського контролю за додержанням прав і свобод людини, зокрема права на інформацію та захист персональних даних; Закон України «Про місцеве самоврядування в Україні» регламентує повноваження органів місцевого самоврядування щодо формування і реалізації інформаційної політики місцевого рівня; Закон України «Про місцеві державні адміністрації» визначає компетенцію відповідних органів у частині реалізації державної інформаційної політики на регіональному рівні.

У контексті підзаконних актів можна вести мову, наприклад, про постанови Кабінету Міністрів України: а) від 3 вересня 2014 р. № 411 «Про затвердження Положення про Адміністрацію Державної служби спеціального зв'язку та захисту інформації України» в якій встановлено, що «Адміністрація Державної служби спеціального зв'язку та захисту інформації України (Адміністрація Держспецзв'язку) є спеціально уповноваженим центральним органом виконавчої влади з питань організації спеціального зв'язку та захисту інформації; центральним органом виконавчої влади, який забезпечує здійснення Держспецзв'язку повноважень уповноваженого органу у сфері захисту критичної інфраструктури під час воєнного стану, а також протягом 12 місяців після його припинення чи скасування, передбачених Законом України «Про критичну інфраструктуру України»; центральним органом виконавчої влади, який забезпечує здійснення Держспецзв'язку повноважень уповноваженого органу, що забезпечує функціонування національної системи обміну інформацією про кіберінциденти, кібератаки, кіберзагрози; центральним органом виконавчої влади, який забезпечує здійснення Держспецзв'язку повноважень уповноваженого органу, що забезпечує функціонування національної системи реагування на кіберінциденти, кібератаки, кіберзагрози; регулятором комунікаційних

послуг» [141]; б) від 18 вересня 2019 р. № 856 «Питання Міністерства цифрової трансформації», що визначає Мінцифри головним органом у системі центральних органів виконавчої влади, що забезпечує формування та реалізацію державної політики: у сферах цифровізації, цифрового розвитку, цифрової економіки, цифрових інновацій та технологій, робототехніки та роботизації, розвитку штучного інтелекту, розвитку напівпровідникових технологій, електронного урядування та електронної демократії, розвитку інформаційного суспільства, інформатизації; у сфері впровадження електронного документообігу; у сфері розвитку цифрових навичок та цифрових прав громадян; у сферах відкритих даних, публічних електронних реєстрів, розвитку національних електронних інформаційних ресурсів та інтероперабельності, електронних комунікацій та радіочастотного спектра, розвитку інфраструктури широкосмугового доступу до Інтернету, електронної комерції та бізнесу; у сфері надання електронних та адміністративних послуг; у сферах електронної ідентифікації та електронних довірчих послуг; у сфері розвитку ІТ-індустрії; у сфері розвитку та функціонування правового режиму Дія Сіті; у сфері хмарних послуг; у сфері організації та проведення азартних ігор та лотерейній сфері [116]; Указ Президента України від 7 червня 2016 року № 242/2016, яким затверджено Положення про Національний координаційний центр кібербезпеки, що є робочим органом Ради національної безпеки і оборони України, утвореним відповідно до рішення Ради національної безпеки і оборони України від 27 січня 2016 року «Про Стратегію кібербезпеки України», уведеного в дію Указом Президента України від 15 березня 2016 року № 96 [153].

Водночас з внутрішньоорганізаційного боку це може бути, приміром, Указ Президента України від 31 липня 2015 року № 463/2015 «Про Положення про проходження військової служби (навчання) військовослужбовцями Державної служби спеціального зв'язку та захисту інформації України», яким затверджено порядок проходження громадянами України військової служби (навчання) в Державній службі спеціального

зв'язку та захисту інформації України [155] або наказ Адміністрації Державної служби спеціального зв’язку та захисту інформації України від 30 серпня 2018 року № 527, яким затверджено «Порядок та умови виплати надбавки за особливий характер роботи працівникам Державної служби спеціального зв’язку та захисту інформації України, які обіймають посади, пов’язані з безпосереднім виконанням завдань із забезпечення кібербезпеки та кіберзахисту». Зокрема останнім наказом встановлена надбавка за особливий характер роботи, яка виплачується працівникам Держспецзв’язку щомісяця у розмірі до 50 відсотків посадового окладу [146].

5. Акти процедурного характеру, які встановлюють процедури захисту інформації, доступу до неї, її обробки, зберігання тощо. Наприклад, постанова Кабінету Міністрів України від 29 березня 2006 р. № 373 встановлює мінімальні вимоги до захисту інформаційних і технологічних систем, які застосовуються органами державної влади [140]; від 29 грудня 2021 р. № 1426 «Про затвердження Положення про організаційно-технічну модель кіберзахисту» – затвердила комплекс заходів, сил і засобів кіберзахисту, спрямованих на оперативне (кризове) реагування на кібератаки та кіберінциденти, впровадження контрзаходів, спрямованих на мінімізацію вразливостей комунікаційних систем [144]; від 18 червня 2025 р. № 712 «Деякі питання захисту інформаційних, електронних комунікаційних, інформаційно-комунікаційних, технологічних систем» – визначає процедури проведення авторизації з безпеки інформаційних, електронних комунікаційних, інформаційно-комунікаційних, технологічних систем, в яких обробляються державні інформаційні ресурси або інформація з обмеженим доступом, вимога щодо захисту якої встановлена законом, об’єктів критичної інформаційної інфраструктури, власниками або розпорядниками яких є органи державної влади, інші державні органи, державні підприємства, установи та організації, органи місцевого самоврядування, а також підтвердження дотримання вимог з безпеки щодо таких систем протягом їх життєвого циклу [41]. Це також може бути наказ Адміністрації Державної

служби спеціального зв'язку та захисту інформації України від 02 грудня 2014 р. № 660 «Про затвердження Порядку оцінки стану захищеності державних інформаційних ресурсів в інформаційних, електронних комунікаційних та інформаційно-комунікаційних системах», який визначає правові та організаційні засади проведення оцінки стану захищеності державних інформаційних ресурсів в інформаційних, електронних комунікаційних та інформаційно-комунікаційних системах державних органів, органів місцевого самоврядування, військових формувань, утворених відповідно до законів України, підприємств, установ і організацій незалежно від форм власності» [145].

Також варто вказати про відомчі нормативно-правові акти (підзаконні акти міністерств та інших центральних органів виконавчої влади), що деталізують та конкретизують загальні процедурні положення у сфері захисту інформації. Приміром, наказ Міністерства внутрішніх справ України від 27 липня 2015 р. № 906 «Про затвердження Інструкції з технічного забезпечення засобами технічного захисту інформації і комплексами технічного контролю Національної гвардії України» в якому регулюються питання щодо організації забезпечення структурних підрозділів Головного управління Національної гвардії України, територіальних управлінь, управлінь корпусів, військових частин і підрозділів, вищих навчальних закладів, навчальних військових частин (центрів), баз, установ та закладів Національної гвардії України засобами технічного захисту інформації, які застосовуються на об'єктах інформаційної діяльності, та комплексами технічного контролю [136].

6. Акти контрольно-наглядового характеру – регламентують здійснення державного нагляду (контролю) у сфері захисту інформації, визначають механізми перевірок, відповідальність за відповідні порушення. Наприклад, це наказ Міністерства внутрішніх справ України від 29 лютого 2016 р. № 139 «Про затвердження Положення про контроль за станом технічного захисту інформації в органах і підрозділах Національної поліції України», який встановив порядок організації та здійснення Національною поліцією України

контролю за станом технічного захисту державних інформаційних ресурсів та інформації, вимога щодо захисту якої встановлена законом, у структурних підрозділах центрального органу управління поліції, територіальних (у тому числі міжрегіональних) органах поліції та їх територіальних (відокремлених) підрозділах, а також в установах, закладах та організаціях, що належать до сфери управління Національної поліції України [143]. Або наказ Центрального управління Служби безпеки України від 18 серпня 2017 р. № 471, що затвердив інструкцію, яка визначає порядок організації і здійснення органами Служби безпеки України контролю за додержанням в органах державної влади, інших державних органах, органах влади Автономної Республіки Крим порядку обліку, зберігання і використання документів та інших матеріальних носіїв інформації, що містять службову інформацію, зібрану у процесі оперативно-розшукової, контррозвідувальної діяльності, у сфері оборони країни [143].

Разом з тим, варто вказати, що загального чинного нормативно-правового акту, який має регламентувати порядок проведення державного контролю у сфері захисту інформації наразі немає. До 2021 року [127] був чинний наказ Адміністрації Державної служби спеціального зв'язку та захисту інформації України від 16 травня 2007 р. № 87 «Про затвердження Положення про державний контроль за станом технічного захисту інформації», яким як раз і були встановлені загальні правила щодо державного контролю у сфері захисту державних інформаційних ресурсів та інформації, вимога щодо захисту якої встановлена законом, і який здійснюється в органах державної влади, органах місцевого самоврядування, утворених відповідно до законодавства військових формуваннях, на підприємствах, в установах і організаціях незалежно від форми власності, у тому числі в закордонних дипломатичних установах України, а також місцях постійного і тимчасового перебування вищих посадових осіб держави [142].

Як бачимо, нормативне закріплення цілей, принципів, завдань, способів та методів захисту інформації об’єктивоване через конституційні положення,

базові та спеціальні закони, акти стратегічного планування, інституційні, процедурні та контрольно-наглядові акти. У межах таких органічно знаходять свій вияв загальні та конкретні правила діяльності органів публічної адміністрації, покликані забезпечити як схоронне функціонування інформаційної сфери, так і сформувати ефективні спеціалізовані механізми реагування на сучасні загрози.

Тож маємо констатувати, що схематично органами публічної адміністрації у сфері захисту інформації є:

1) органи стратегічного управління – Рада національної безпеки і оборони України та її робочі органи (Національний координаційний центр кібербезпеки, Центр протидії дезінформації), Кабінет Міністрів України;

2) органи виконавчої влади спеціальної компетенції – Міністерство цифрової трансформації України, Державна служба спеціального зв'язку та захисту інформації України, Служба безпеки України;

3) органи виконавчої влади секторальної компетенції – міністерства, правоохоронні органи, розвідувальні та контррозвідувальні органи, Національний банк України тощо;

4) органи влади регіонального та місцевого рівня – місцеві державні адміністрації та органи місцевого самоврядування;

5) інші інституції публічно-владного та правозахисного характеру – Уповноважений Верховної Ради України з прав людини, уповноважені підрозділи Національної поліції та інших органів.

При цьому окремо варто вказати, що суб'єкти та органи публічної адміністрації не є тотожними категоріями, а отже і правовими явищами. Зокрема остання є вужчою за змістом, адже суб'єктний склад публічної адміністрації представлений також допоміжними та залученими суб'єктами, які здійснюють захист інформації у власних інформаційно-комунікаційних системах та беруть участь у забезпеченні інформаційної безпеки у межах делегованих або покладених на них законом повноважень, не набуваючи при цьому статусу органів публічної влади у класичному розумінні (оператори

критичної інфраструктури, державні підприємства, установи та організації, суб'єкти господарювання та громадяни).

Таким чином, можна узагальнити, що правові засади діяльності органів публічної адміністрації у сфері захисту інформації є нормативною основою для реалізації процедур та механізмів адміністративно-правового захисту інформації в Україні. Ця нормативна основа з-поміж того, що визначає суб'єктний склад публічної адміністрації у цій сфері, вона також забезпечує системну регламентацію їх компетенції, виконуючи інтегруючу функцію, оскільки поєднує різнорівневі правові приписи – від конституційних положень до відомчих інструкцій – у цілісну систему, спрямовану на досягнення єдиної мети.

Отже, маємо всі підстави вбачати, що правові засади діяльності органів публічної адміністрації у сфері захисту інформації – це не лише сукупність нормативно-правових актів, а динамічна функціонально орієнтована система правового регулювання, що визначає зміст, межі та механізми реалізації державної інформаційної політики у напрямку забезпечення інформаційної безпеки в Україні.

Висновки до Розділу 1

1. Зауважено, що у сучасних умовах розвитку інформаційного суспільства до кола об'єктів захисту дедалі частіше відносять інформацію, яка набуває статусу самостійної соціальної та правової цінності. Тому проблематика забезпечення безпеки інформаційних відносин вже тривалий час перебуває у центрі уваги як вітчизняних, так і зарубіжних науковців.

2. Визначено, що безпека як правова категорія в контексті держави охоплює різні рівні – індивідуальний, колективний та національний, які перебувають у тісному взаємозв'язку та взаємозалежності. При цьому кожен із зазначених рівнів передбачає наявність власних об'єктів захисту, серед

яких в умовах сучасного розвитку особливе місце посідає інформація. Її слід розглядати як особливий нематеріальний об’єкт, що характеризується сукупністю специфічних властивостей та набуває юридичного значення лише за умови її включення у сферу правового регулювання.

3. З’ясовано, що сучасна наукова думка демонструє поступовий перехід від вузького, антропоцентричного розуміння інформації до її більш широкого, універсального трактування як фундаментальної характеристики реальності. Тому узагальнюється, що інформація у широкому значенні постає як універсальна характеристика реальності, що забезпечує процеси організації, взаємодії та розвитку систем різної природи, тоді як у вузькому, юридичному розумінні вона набуває ознак специфічного об’єкта правовідносин, зокрема і захисного спрямування, адже її обіг, збирання, зберігання та поширення можуть як сприяти реалізації прав людини, так і створювати загрози їх порушення. Інший контекст порушеного питання, – загальнодержавний, оскільки інформація виступає стратегічним ресурсом розвитку держави, важливим чинником забезпечення її суверенітету, національної безпеки та ефективного функціонування публічної влади.

4. Констатується, що інформацію як об’єкт правового захисту варто характеризувати через призму стратегічного ресурсу, що зумовлює необхідність її охорони не лише як об’єкта приватних прав, але і як елемента національної безпеки.

5. Визначено, що адміністративне право в механізмі формування стійкого інформаційного середовища в Україні відіграє одну із ключових ролей, адже з-поміж того, що визначає порядок організації та функціонування органів публічної адміністрації, що здійснюють адміністративно-правовий захист інформації, також забезпечує організаційну основу для реалізації інших важливих заходів, пов’язаних із протидією інформаційним загрозам, безперервністю перебігу важливих інформаційних процесів, впровадженням цифрових рішень в буденність тощо.

6. Визначено, що адміністративно-правовий захист інформації є різновидом діяльності органів публічної адміністрації, що безпосередньо пов'язаний із забезпеченням стійкості інформаційного середовища індивідуального, колективного та національного рівнів через реалізацію заходів попереджувального та реагувального характеру, спрямованих на запобігання порушенням, відновлення порушених прав та інтересів суб'єктів інформаційних відносин, а також створення умов для безпечного використання інформації як стратегічного ресурсу в публічних цілях. Зауважено, що індивідуальний, колективний та національний рівні інформаційного середовища є взаємопов'язаними.

7. Запропоновано виокремлювати два базових різновиди адміністративно-правового захисту інформації, виходячи з об'єкта захисту: відкрита інформація або інформація з обмеженим доступом.

8. Визначено, що адміністративно-правовий захист інформації з обмеженим доступом має на меті гарантування прозорості діяльності держави та реалізацію права громадян на інформацію. Водночас адміністративно-правовий захист відкритої інформації стосується забезпечення реалізації конституційного права кожного на вільний доступ до інформації, а також на недопущення неправомірних обмежень чи ускладнень у користуванні нею.

9. Констатується, що за заявленим аспектом адміністративно-правовий захист інформації виступає ключовим механізмом реалізації державної інформаційної політики, забезпечуючи належне функціонування правового режиму доступу до відкритої та обмеженої інформації в безпековому контексті. Проте уточнюється, що це лише однин із варіантів розгляду змістової структури адміністративно-правового захисту інформації, адже в правовому контексті категорії конфіденційності, цілісності та доступності виступають не лише характеристиками інформації, а й концептуальною основою формування системи її захисту. У цьому сенсі адміністративно-правовий захист виступає не просто набором окремих заходів чи механізмів,

а цілісною системою інструментів, що спрямовані на підтримку стабільності інформаційного середовища на всіх рівнях – від індивідуального до національного.

10. Інструментами адміністративно-правового захисту названо: а) нормотворчі – передбачають розробку та прийняття нормативів, що встановлюють правила доступу до інформації, порядок її збирання, обробки, зберігання та поширення, а також визначають відповідальність за порушення режиму інформаційної безпеки. У цьому контексті йдеться як про нормативно-правові акти загальної та індивідуальної сили, так і про акти реагування та документи, якими оформлюються відповідні домовленості; б) превентивні – спрямовані на запобігання порушенням прав на інформацію та загрозам інформаційній безпеці. До них належать контроль за дотриманням правил доступу до інформації, інструктажі та навчання працівників, проведення інформаційно-просвітницьких кампаній, аудит інформаційних систем, моніторинг інформаційного середовища та раннє виявлення потенційних загроз; в) оперативні – реалізуються у разі фактичного порушення інформаційної безпеки та передбачають невідкладні дії щодо локалізації загроз і нейтралізації негативних наслідків. Це можуть бути тимчасові обмеження доступу до інформації, блокування неправомірних джерел, реагування на спроби несанкціонованого втручання або поширення дезінформації, а також координація між різними суб’єктами інформаційного простору; г) відновлювальні – спрямовані на відновлення порушених прав та цілісності інформації, ліквідацію наслідків інформаційних порушень та забезпечення стійкості інформаційного середовища у майбутньому. Йдеться зокрема про відновлення доступу до обмеженої або заблокованої інформації, публічні спростування фейків, компенсаційні дії, а також впровадження додаткових заходів контролю для запобігання повторних порушень.

11. Уточнено питання щодо співвідношення превентивних інструментів адміністративно-правового захисту та адміністративно-правової охорони, оскільки на перший погляд їх змістовне наповнення є подібним. Зауважено,

що відмінність є. Вона полягає у цільовій спрямованості та функціональному контексті застосування. Так, превентивні інструменти адміністративно-правової охорони мають загально-регулятивний, стабілізаційний характер і спрямовані на формування належного правового режиму інформаційних відносин, у межах якого мінімізується сама можливість виникнення правопорушень. Натомість превентивні інструменти адміністративно-правового захисту, хоча і мають попереджувальний характер, однак застосовуються вже в умовах наявності підвищених ризиків, загроз або передумов до порушення прав на інформацію чи інформаційної безпеки. Тобто їх превентивність є більш цільовою та ризик-орієнтованою, а не загальною.

13. Узагальнено, що адміністративно-правовий захист інформації є системою заходів, застосовних уповноваженими представниками публічної адміністрації задля забезпечення захищеності інформації, що є об’єктом адміністративно-правового захисту. Водночас об’єктами адміністративно-правового захисту виступають усі види інформації, правовий режим доступу до яких визначений чинним законодавством.

14. Зауважено, що держава, усвідомлюючи потребу в реалізації адміністративно-правового захисту інформації, уповноважує на здійснення відповідних заходів забезпечення інформаційної безпеки різних рівнів конкретних виконавців. Уточнено, що йдеться про органи публічної адміністрації. Однак констатується, що досі адміністративно-правова галузь наукових знань не визначилась досконально з тим, представники якого рівня влади та яких структур формують систему публічної адміністрації загалом, зокрема і у досліджуваній сфері. Підтримано науковий підхід, який визначає, що означена категорія є репрезентацією системи органів влади, які виконують адміністративно-виконавчі функції, основне призначення яких полягає у забезпеченні публічних інтересів та вирішені індивідуальних адміністративних справ.

15. Правовими засадами діяльності органів публічної адміністрації у сфері захисту інформації названо нормативну основу (систему нормативно-правових актів), що окреслює: 1) цілі та завдання адміністративно-правового захисту інформації; 2) принципи здійснення такої діяльності; 3) повноваження органів публічної адміністрації у цій сфері; 4) правові механізми реалізації їхньої компетенції у цій сфері.

16. Запропоновано класифікувати нормативно-правові акти, що регулюють діяльність органів публічної адміністрації у сфері захисту інформації за такими критеріями:

– конституційні та базові акти (визначають загальні принципи функціонування та розвитку інформаційних відносин, а також гарантії прав людини і громадянина в інформаційній сфері – Конституція України, Закони України «Про інформацію», «Про доступ до публічної інформації», «Про захист персональних даних» та ін.);

– спеціальні акти у сфері захисту інформації (акти, які безпосередньо регулюють питання забезпечення безпеки інформації, а також інші акти, що встановлюють вимоги до технічного та криптографічного захисту інформації – Закони України «Про захист інформації в інформаційно-комунікаційних системах», «Про державну таємницю», «Про основні засади забезпечення кібербезпеки України», наказ Адміністрації Державної служби спеціального зв’язку та захисту інформації України від 16 грудня 2025 року № 832, яким було затверджено «Порядок формування програми робіт із стандартизації криптографічного та технічного захисту інформації, кіберзахисту, протидії технічним розвідкам, технічної перевірки проєкту стандарту криптографічного та технічного захисту інформації, кіберзахисту, протидії технічним розвідкам, розсилання, перевірки та перегляду стандартів криптографічного та технічного захисту інформації, кіберзахисту, протидії технічним розвідкам, ведення їх каталогу» тощо);

– акти стратегічного планування, які визначають основи державної політики у сфері захисту інформації в Україні (Стратегія кібербезпеки

України, Стратегія інформаційної безпеки, Стратегія національної безпеки України, Стратегія розвитку інформаційного суспільства в Україні, Концепція розвитку електронного урядування в Україні та ін.);

– акти інституційного характеру (визначають правовий статус і повноваження органів публічної адміністрації у сфері захисту інформації, а також забезпечують права працівників вказаних органів – Закони України «Про Кабінет Міністрів України», «Про центральні органи виконавчої влади», «Про Службу безпеки України», «Про Державну службу спеціального зв'язку та захисту інформації України», «Про Уповноваженого Верховної Ради України з прав людини», «Про місцеве самоврядування в Україні», «Про місцеві державні адміністрації», постанови Кабінету Міністрів України від 3 вересня 2014 р. № 411 «Про затвердження Положення про Адміністрацію Державної служби спеціального зв'язку та захисту інформації України», від 18 вересня 2019 р. № 856 «Питання Міністерства цифрової трансформації, Укази Президента України від 7 червня 2016 року № 242/2016, яким затверджено Положення про Національний координаційний центр кібербезпеки, від 31 липня 2015 року № 463/2015 «Про Положення про проходження військової служби (навчання) військовослужбовцями Державної служби спеціального зв'язку та захисту інформації України» тощо);

– акти процедурного характеру (встановлюють процедури захисту інформації, доступу до неї, її обробки, зберігання тощо – постанови Кабінету Міністрів України від 29 березня 2006 р. № 373 «Про затвердження Мінімальних вимог до захисту інформаційних, електронних комунікаційних, інформаційно-комунікаційних та технологічних систем», від 29 грудня 2021 р. № 1426 «Про затвердження Положення про організаційно-технічну модель кіберзахисту», від 18 червня 2025 р. № 712 «Деякі питання захисту інформаційних, електронних комунікаційних, інформаційно-комунікаційних, технологічних систем», наказ Адміністрації Державної служби спеціального зв'язку та захисту інформації України від 02 грудня 2014 р. № 660 «Про затвердження Порядку оцінки стану захищеності державних інформаційних

ресурсів в інформаційних, електронних комунікаційних та інформаційно-комунікаційних системах», наказ Міністерства внутрішніх справ України від 27 липня 2015 р. № 906 «Про затвердження Інструкції з технічного забезпечення засобами технічного захисту інформації і комплексами технічного контролю Національної гвардії України» та ін.);

– акти контрольно-наглядового характеру (регламентують здійснення державного нагляду (контролю) у сфері захисту інформації, визначають механізми перевірок, відповідальність за відповідні порушення – наприклад, наказ Міністерства внутрішніх справ України від 29 лютого 2016 р. № 139 «Про затвердження Положення про контроль за станом технічного захисту інформації в органах і підрозділах Національної поліції України» або наказ Центрального управління Служби безпеки України від 18 серпня 2017 р. № 471 «Про затвердження Інструкції про порядок здійснення Службою безпеки України контролю за додержанням порядку обліку, зберігання і використання документів та інших матеріальних носіїв інформації, що містять службову інформацію, зібрану у процесі оперативно-розшукової, контррозвідувальної діяльності, у сфері оборони країни»).

17. Констатується, що нормативне закріплення цілей, принципів, завдань, способів та методів захисту інформації об’єктивоване через конституційні положення, базові та спеціальні закони, акти стратегічного планування, інституційні, процедурні та контрольно-наглядові акти. У межах таких органічно знаходять свій вияв загальні та конкретні правила діяльності органів публічної адміністрації, покликані забезпечити як схоронне функціонування інформаційної сфери, так і сформувати ефективні спеціалізовані механізми реагування на сучасні загрози.

18. Органами публічної адміністрації у сфері захисту інформації названо: 1) органи стратегічного управління – Рада національної безпеки і оборони України та її робочі органи (Національний координаційний центр кібербезпеки, Центр протидії дезінформації), Кабінет Міністрів України; 2) органи виконавчої влади спеціальної компетенції – Міністерство цифрової

трансформації України, Державна служба спеціального зв'язку та захисту інформації України, Служба безпеки України; 3) органи виконавчої влади секторальної компетенції – міністерства, правоохоронні органи, розвідувальні та контррозвідувальні органи, Національний банк України тощо; 4) органи влади регіонального та місцевого рівня – місцеві державні адміністрації та органи місцевого самоврядування; 5) інші інституції публічно-владного та правозахисного характеру – Уповноважений Верховної Ради України з прав людини, уповноважені підрозділи Національної поліції та інших органів.

19. Окремо уточнено, що суб'єкти та органи публічної адміністрації не є тотожними категоріями, а отже і правовими явищами. Зокрема остання є вужчою за змістом, адже суб'єктний склад публічної адміністрації представлений також допоміжними та залученими суб'єктами, які здійснюють захист інформації у власних інформаційно-комунікаційних системах та беруть участь у забезпеченні інформаційної безпеки у межах делегованих або покладених на них законом повноважень, не набуваючи при цьому статусу органів публічної влади у класичному розумінні (оператори критичної інфраструктури, державні підприємства, установи та організації, суб'єкти господарювання та громадяни).

20. Узагальнено, що правові засади діяльності органів публічної адміністрації у сфері захисту інформації є нормативною основою для реалізації процедур та механізмів адміністративно-правового захисту інформації в Україні. Ця нормативна основа з-поміж того, що визначає суб'єктний склад публічної адміністрації у цій сфері, вона також забезпечує системну регламентацію їх компетенції, виконуючи інтегруючу функцію, оскільки поєднує різнорівневі правові приписи – від конституційних положень до відомчих інструкцій – у цілісну систему, спрямовану на досягнення єдиної мети.

21. Констатується, що правові засади діяльності органів публічної адміністрації у сфері захисту інформації – це не лише сукупність нормативно-правових актів, а динамічна функціонально орієнтована система

правового регулювання, що визначає зміст, межі та механізми реалізації державної інформаційної політики у напрямку забезпечення інформаційної безпеки в Україні.

РОЗДІЛ 2
АДМІНІСТРАТИВНО-ПРАВОВИЙ СТАТУС ОРГАНІВ ПУБЛІЧНОЇ АДМІНІСТРАЦІЇ У СФЕРІ ЗАХИСТУ ІНФОРМАЦІЇ

2.1. Поняття та структура адміністративно-правового статусу органів публічної адміністрації у сфері захисту інформації

Варто зауважити, що категорія «статус» є широко застосовною у різних тлумаченнях [204, с. 6]. Її розуміння є таким:

– становище або ранг у відношенні до інших;

– відносний ранг в ієрархії престижу;

– стан особи або речі з погляду права;

– стан або положення залежно від обставин [238].

Деякі науковці вважають, що це поняття визначає кількісні та якісні характеристики явища чи об’єкта [227, с. 58]. Однак у загальному розумінні під статусом розуміється правове положення (сукупність прав і обов’язків) фізичної чи юридичної особи [18, с. 23; 30]. Тому цілком зрозуміло чому статус визначається як основний елемент соціальної структури суспільства; соціальний стан людини в суспільстві, у певній соціальній групі, пов’язаний з іншими соціальними позиціями через систему ролей, прав і обов’язків, норм і звичаїв [90; 100].

На основі аналізу зазначеного А. Зубко акцентує, що категорія «статус» є історично сформованою та модернізованою під впливом зміни суспільно-політичних процесів у світі та наразі наділена соціологічним чинником інтерпретування [27; 60, с. 48]. Своєю чергою, В. Терещук додає, що синонімічними словами для вказаного слова є «становище», «стан», «модальність» чи «індигенат» (для іноземної особи) [100; 178].

У справі May v. Daniels, 359 Ark. 100, 108 (Ark. 2004), Верховний суд Арканзасу зазначив, що той факт, що термін може мати більше одного

значення, не робить його беззмістовним, якщо його значення можна правильно встановити з контексту, в якому він використовується [239].

Зокрема в офіційних правових документах ця категорія часто застосовується для визначення певного стану, зокрема правового. Однак у більшості випадків категорія «правовий статус» використовується для позначення становища особи в системі правових відносин. Вона ґрунтується на фактичному соціальному статусі, реальному становищі особи в цій системі суспільних відносин [245] як за формою, так і за змістом [228].

Отже, як загальне правило, правовий статус є складовою загальної проблеми прав людини. Належне та комплексне його правове регулювання дозволяє громадянам реалізовувати свої права та захищати законні інтереси [200]. Наприклад, термін «правовий статус» широко використовується у праві штату Арканзас для класифікації особи та визначення її прав і обов'язків, як-от правовий статус відвідувача або вітчима [239]. У законодавстві України цей термін характеризує належність особи до певної категорії (наприклад, правовий статус ветерана війни [159] або стан правомірності певної дії (наприклад, набрання юридичної сили електронними даними [133]).

Разом з цим, у межах наукових кіл заведено вважати, що з поняттям «статус» пов'язано правове положення юридичних осіб, які залежно від порядку їх створення поділяються на юридичних осіб приватного права та юридичних осіб публічного права. Нас цікавлять останні. Юридичні особи публічного права – це ті юридичні особи, які створюються безпосередньо законом або адміністративним актом як носії публічних завдань, їх організація регулюється приписами законів публічних інтересів, і вони виконують відповідні публічні функції. Такі юридичні особи створюються розпорядчим способом державними органами та органами місцевого самоврядування або організаціями, які віднесені до публічних за іншими підставами, визначеними в законі чи іншому нормативно-правовому акті, і порядок їх створення, організаційно-правові форми, правове становище не є

предметом цивільно-правового регулювання, а отже, вони визначаються публічними законами [75, с. 115; 83, с. 216].

Тобто, цей термін також використовується для розкриття місця та ролі конкретних юридичних осіб публічного права у певному механізмі регулювання суспільних відносин. На відміну від фізичних осіб, юридичні особи не є живими істотами і, відповідно, не мають природної волі, однак вони мають об'єднану людську волю та спільну діяльнісну спрямованість, визначену метою створення юридичної особи. У результаті юридична особа визнається суб'єктом права. Варто зазначити, що юридична особа є самостійним суб'єктом правовідносин і існує незалежно від осіб, які її створили, і хоча це колективне утворення визнається суб'єктом правовідносин, як юридична особа воно може мати лише ті права та обов'язки, які не пов'язані з природними властивостями людини [122].

Таким чином, можемо визначити, що категорія «правовий статус»: 1) у контексті фізичних осіб окреслює їх законодавчо встановлені права та обов'язки; 2) у контексті юридичних осіб публічного права характеризує їх роль і призначення в механізмі реалізації функцій держави як сукупність нормативних, інформаційно-аналітичних, реалізаційних, оптимізаційних, експертних, погоджувальних, організаційних, контрольно-наглядових, адміністративних та інших активних управлінських дій. Тобто кожен такий суб'єкт, діючи від імені та в інтересах держави, є носієм владних повноважень, виконує визначені завдання та має власні функції, належне виконання яких забезпечується обов'язком нести юридичну відповідальність [204, с. 6].

Наведені підходи до розуміння правового статусу, на нашу думку, є теоретично цінними, адже дозволяють сформувати загальнотеоретичне підґрунтя для подальшого дослідження його галузевих різновидів, зокрема і адміністративно-правового статусу як спеціалізованого різновиду останнього.

Уточнимо, що визначаючи зміст поняття адміністративно-правового статусу, у тому числі органів публічного адміністрування, вітчизняні вчені зауважують на такому:

– В. Авер'янов – вважає, що це комплекс конкретно визначених суб'єктивних прав й обов'язків, які закріплені за відповідним суб'єктом нормами адміністративного права [2, с. 194];

– О. Панфілов, А. Калімбет – стверджують, що адміністративно-правовий статус це сукупність конкретно визначених суб'єктивних прав і обов'язків, які закріплюються за відповідним суб'єктом визначеними нормативно-правовими актами та гарантовані державою [109, с. 79];

– Т. Коломоєць – переконана, що це сукупність суб'єктивних прав й об'єктивних обов'язків, закріплених нормами адміністративного права за певним органом [69, с. 64];

– С. Стеценко – розуміє адміністративно-правовий статус органу влади як сукупність прав, обов'язків та гарантій їх реалізації, що визначені в нормативних актах [177, с. 90];

– С. Обрусна, І. Іванова, Ю. Панімаш, К. Пасинчук – визначають, що це наявність та сукупність їхньої компетенції (мети створення, цілей діяльності, завдань, функцій), повноважень (права та обов'язки у визначеній сфері діяльності) та юридична відповідальність [99, с. 93];

– А. Замрига – стверджує, що адміністративно-правовий статус суб'єктів публічної адміністрації – це юридична конструкція адміністративного права зокрема, та надбання правознавства в цілому, що характеризується органічним поєднанням певних правових елементів. Ця конструкція: а) своїм структурним аспектом поєднує декілька самостійних юридичних складових, які сукупно формують дефінітивні та змістові чинники статики [55] адміністративної діяльності; б) наділяє суб'єктів публічної адміністрації адміністративною правосуб'єктністю – можливістю брати участь у адміністративно-правових відносинах. Він також визначає, що: 1) адміністративні обов'язки та задля їх виконання адміністративні права

уповноважених суб'єктів за своєю юридичною природою є потенційними засобами реалізації завдань і функцій публічної адміністрації; 2) компетенції суб'єктів публічної адміністрації можуть бути використанні виключно з метою реалізації публічного інтересу; 3) невід'ємним елементом адміністративно-правового статусу суб'єктів публічної адміністрації є їх адміністративна відповідальність [55]. Цікавими також є його розмірковування, що правовий статус окремого суб'єкта публічної адміністрації визначається за принципом головних, характерних йому особливостей як представника певного типу публічного утворення. На основі загального розуміння даного терміну необхідно досліджувати адміністративно-правовий статус зазначених суб'єктів [55];

– А. Приходько – визначає, що адміністративно-правовий статус суб'єктів публічної адміністрації – це абстрактне поняття, яким представники доктрини адміністративного права намагаються означити сукупність необхідних передумов, за допомогою яких з'являється змога описати практичне значення конкретного уповноваженого суб'єкта в певному публічно забезпечувальному процесі. З теоретичної точки зору, адміністративно-правовий статус публічної адміністрації у сфері запобігання та протидії корупції в Україні – це роль, значення та цінність її представників у цьому механізмі; з практичної – надання їм можливості вчиняти адміністративні дії, що спричиняють настання юридичних наслідків як індивідуального, так і публічного характеру. Практична цінність публічної адміністрації у сфері запобігання та протидії корупції у відповідному механізмі є різною, що обумовлюється як самим різновидом їхнього адміністративно-правового статусу (наприклад, публічні органи влади, їхні структурні підрозділи та делеговані ними представники мають класичний статус як особи, уповноважені на виконання функцій держави або місцевого самоврядування (та прирівняних до них); приватні особи та структури громадського спрямування – спеціальний, тобто як індивідуальний або, у встановлений законодавством випадках, класичний; представники

міжнародних інституцій – специфічний, у межах співпраці та технічної допомоги), так і сукупністю їхньої законодавчої та нормативної правової можливості вчиняти адміністративні дії, що має індивідуальне чи публічне значення. При цьому він зауважує, що для всіх суб'єктів досліджуваної публічної адміністрації головним критерієм визначення їхнього статусу є, по-перше, завдання, з метою виконання якого їх було утворено; по-друге, комплекс адміністративних обов'язків і прав за допомогою яких це завдання втілюється в дійсність; по-третє, юридичне значення результату діяльності – ефективність, необхідність і доцільність існування конкретного уповноваженого суб'єкта та безпосередньо діяльності, яку він реалізовує в рамках запобігання чи протидії корупції в Україні [126, с. 93];

– О. Дрозд, Л. Сорока, Л. Миськів – обґрунтовують, що адміністративно-правовий статус органів виконавчої влади є різновидом правового статусу, який визначає права, обов'язки, повноваження та відповідальність конкретного суб'єкта цієї системи (міністерство, служба, агентство, інспекція, центральний орган виконавчої влади зі спеціальним статусом, колегіальний орган, інший центральний орган виконавчої влади, місцевий орган влади [49]) у сфері публічного адміністрування та конкретних адміністративних відносин. Вчені уточнюють, що він встановлюється законами або іншими нормативно-правовими актами, однак здебільшого – положеннями про засади та організацію їхньої діяльності. Загалом їхня думка є такою: «концепт адміністративно-правового статусу є похідним, а отже – ґрунтується на теоретичних підходах загального та спеціального спрямування; по-друге, у дискурсі обмеження його змісту приналежністю конкретного суб'єкта до сфери функціонування такого (у цьому випадку – публічного адміністрування) слід з особливою обачністю розкривати елементний склад адміністративно-правового статусу, адже іменування публічного суб'єкта не завжди відповідає його організаційно-правовій формі [49, с. 507–508].

Як приклад, О. Бригінець, до структури адміністративно-правового статусу органу державної влади включала такі складники: 1) цільове призначення, що охоплює принципи, цілі, завдання і функції органу державної влади; 2) структурно-організаційну форму побудови органу державної влади, що включає в себе регулювання порядку створення, реорганізації, ліквідації, процедури діяльності, право на офіційні символи, лінійну і функціональну підпорядкованість; 3) компетенцію, яка передбачає сукупність владних повноважень стосовно: а) прав і обов'язків, пов'язаних зі здійсненням влади, участю в управлінських відносинах, а також правом видавати певні адміністративні акти; б) підпорядкованості, правового закріплення об'єктів, предметів і справ, на яких поширюються владні повноваження [21, с. 172; 101].

Водночас свого часу В. Авер'янов визначав, що адміністративно-правовий статус складається з трьох блоків елементів, а саме: а) цільовий блок, б) структурно-організаційний блок, в) компетенційний блок (компетенцію) [26]. Як зауважує щодо цього вчена С. Подоляка, з цим повною мірою можливо погодитись, однак усі ці блоки певною мірою випливають із повноважень суб'єктів, статус яких досліджується. Навіть структурно-організаційний блок статусу зумовлений ієрархічними зв'язками, що випливають із повноважень суб'єктів у системі ієрархії [27, с. 66; 101; 119, с. 161].

Окремо зазначимо, що деякі вчені як елементи аналізованого статусу розглядають правове зобов'язання, законність, правопорядок, правосвідомість, гуманізм, справедливість [68; 167, с. 27], тобто в занадто широкому елементному трактуванні [125, с. 178].

З означеного маємо, що категорійно-понятєва визначеність правового концепту «адміністративно-правовий статус органів публічної адміністрації» у вітчизняній науковій думці сформована через подвійний інтерпретаційний підхід: 1) через зміст як репрезентації елементів внутрішньої структури його складу, що ідентифікує суб'єкта у межах потенційно та фактично існуючих

адміністративних правовідносин; 2) через сутність, яка окреслює місце і роль органів публічної адміністрації в механізмі виконання адміністративних функцій держави [14].

Таким чином, на нашу думку, під адміністративно-правовим статусом органів публічної адміністрації у сфері захисту інформації слід розуміти сукупність нормативно визначених універсальних характеристик, які детермінують правове положення цих органів як суб’єктів публічної адміністрації в колі адміністративно-правових взаємозв’язків, пов’язаних із реалізацією ними повноважень під час забезпечення інформаційної безпеки та здійснення адміністративно-правового захисту прав громадян, юридичних осіб і держави в інформаційній сфері [14].

При цьому нам імпонує науковий підхід, який визначає, що існує певна сукупність правових елементів, які становлять його системну характеристику. Йдеться про сукупність характерних особливостей досліджуваних органів як представників влади та суб’єктів адміністративного права [85, с. 8] – осіб й організацій, за якими законом визнана особлива юридична властивість (якість) правосуб'єктності, що дає можливість брати участь у правовідносинах. При чому, ми долучаємось до думки Є. Додіна, що правосуб'єктність включає їх правоздатність і дієздатність, а також правовий статус. Вони стають суб'єктами адміністративно-правових відносин тоді, коли вони мають практичну можливість реалізувати свою адміністративну правоздатність у рамках конкретних адміністративних правовідносин [48, с. 5–6; 55].

Зокрема згідно зі статтею 4 Закону України «Про центральні органи виконавчої влади» міністерства, інші центральні органи виконавчої влади набувають статусу юридичної особи з дати внесення до Єдиного державного реєстру юридичних осіб, фізичних осіб - підприємців та громадських формувань запису про їх державну реєстрацію як юридичної особи [160].

Приміром, Державна служба спеціального зв'язку та захисту інформації України утворена 23 лютого 2006 року [128]. Так 7 листопада 2005 року

Президентом України був підписаний Указ № 1556/2005 «Про додержання прав людини під час проведення оперативно-технічних заходів» [131]. Відповідно до абзацу 2 пункту 1 цього документа Кабінету Міністрів України доручалося у чотиримісячний термін ужити заходів щодо утворення Державної служби спеціального зв’язку та захисту інформації України як центрального органу виконавчої влади із спеціальним статусом, визначивши основними її завданнями реалізацію державної політики у сфері захисту державних інформаційних ресурсів у мережах передачі даних, забезпечення функціонування державної системи урядового зв’язку, Національної системи конфіденційного зв’язку, криптографічного та технічного захисту інформації [35; 129].

Сьогодні Служба є спеціалізованим органом центральної виконавчої влади в галузі спеціального зв'язку та захисту інформації, суб'єктом сектору оборони і безпеки, основним суб'єктом національної системи кібербезпеки, що здійснює координацію діяльності суб’єктів забезпечення кібербезпеки в галузі кіберзахисту, та адміністратором зв'язку [128]. Вона виконує 93 завдання й функції та формує державну політику в 16 сферах. Узагальнено функції Держспецзв’язку – це захищені урядові комунікації, до яких також входить фельд’єгерська служба, захист інформації та кіберзахист [128]. У досліджуваному нами контексті йдеться, наприклад, про кіберзахист критичної інформаційної інфраструктури, захист критичної технологічної інформації, криптографічний і технічний захист інформації, захист державних інформаційних ресурсів та інформації, вимога щодо захисту якої встановлена законом, в інформаційних, електронних комунікаційних та інформаційно-комунікаційних системах і на об’єктах інформаційної діяльності, а також у сферах використання державних інформаційних ресурсів в частині захисту інформації, протидії технічним розвідкам, функціонування, безпеки та розвитку Національної телекомунікаційної мережі, державної системи урядового зв’язку, Національної системи конфіденційного зв’язку [141] тощо.

З означеного маємо, що адміністративно-правовий статус Держспецзв'язку характеризується чітко визначеною законодавством правосуб'єктністю, спеціальною компетенцією та функціональною спрямованістю діяльності. При цьому специфіка адміністративно-правового статусу цього суб'єкта полягає у його подвійному інституційному призначенні: з одного боку, як центрального органу виконавчої влади зі спеціальним статусом, що формує та реалізує державну політику у сфері захисту інформації, а з іншого – як суб'єкта сектору безпеки і оборони, що забезпечує практичну реалізацію заходів кіберзахисту та технічного захисту інформації.

Щодо адміністративно-правового статусу інших органів публічної адміністрації у сфері захисту інформації, на нашу думку, варто вказати наступне.

1. Рада національної безпеки і оборони України (РНБО). В мовах збройної агресії проти України і посягання на її територіальну цілісність з боку режиму рашизму особливого значення набуває обговорення питань, пов'язаних із національною безпекою і обороною України. РНБО, яка діє як координаційний орган з питань національної безпеки і оборони при Президентові України (ст. 107 Конституції України), в умовах війни стає дуже важливим органом публічної влади. За Конституцією вона координує і контролює діяльність органів виконавчої влади у сфері національної безпеки і оборони. Рішення Ради національної безпеки і оборони України вводяться в дію указами Президента України. Компетенція та функції Ради національної безпеки і оборони України визначаються законом [103].

Примітно, що первісно вона створювалася за американським взірцем, а її статус отримав конституційне закріплення в Основному Законі 1996 року і деталізацію – в Законі «Про Раду національної безпеки і оборони» 1998 року. Рада є саме тим органом, де в результаті колегіального обговорення між вищими посадовими особами, відповідальними за стан обороноздатності та національної безпеки, формулюються відповідні політичні рішення, які потім

втілюються в укази глави Української держави. Згідно з Законом, основними функціями Ради національної безпеки і оборони України є: 1) внесення пропозицій Президентові України щодо реалізації принципів внутрішньої та зовнішньої політики у сфері національної безпеки і оборони; 2) координація і здійснення контролю за діяльністю органів виконавчої влади у сфері національної безпеки і оборони у мирний час; 3) координація і здійснення контролю за діяльністю органів виконавчої влади у сфері національної безпеки і оборони в умовах воєнного чи надзвичайного стану та у випадках виникнення кризових ситуацій, що загрожують національній безпеці України [23].

Отже, адміністративно-правовий статус РНБО у сфері захисту інформації є загальним, має стратегічний характер та проявляється координаційною діяльністю щодо усіх суб'єктів у цій сфері, зокрема з використанням спроможностей Центру протидії дезінформації [157], Національного координаційного центру кібербезпеки.

Зауважимо, що Центр протидії дезінформації є робочим органом Ради національної безпеки і оборони України, утвореним відповідно до рішення Ради національної безпеки і оборони України від 11 березня 2021 року «Про створення Центру протидії дезінформації», уведеного в дію Указом Президента України від 19 березня 2021 року № 106. Центр забезпечує здійснення заходів щодо протидії поточним і прогнозованим загрозам національній безпеці та національним інтересам України в інформаційній сфері, забезпечення інформаційної безпеки України, виявлення та протидії дезінформації, ефективної протидії пропаганді, деструктивним інформаційним впливам і кампаніям, запобігання спробам маніпулювання громадською думкою [117].

Основними завданнями Центру є: 1) проведення аналізу та моніторингу подій і явищ в інформаційному просторі України, стану інформаційної безпеки та присутності України у світовому інформаційному просторі; 2) виявлення та вивчення поточних і прогнозованих загроз інформаційній

безпеці України, чинників, які впливають на їх формування, прогнозування та оцінка наслідків для безпеки національних інтересів України; 3) забезпечення Ради національної безпеки і оборони України, Голови Ради національної безпеки і оборони України інформаційно-аналітичними матеріалами з питань забезпечення інформаційної безпеки України, виявлення та протидії дезінформації, ефективної протидії пропаганді, деструктивним інформаційним впливам і кампаніям, запобігання спробам маніпулювання громадською думкою; 4) підготовка та внесення Раді національної безпеки і оборони України, Голові Ради національної безпеки і оборони України пропозицій щодо: визначення концептуальних підходів у сфері протидії дезінформації та деструктивним інформаційним впливам і кампаніям; координації діяльності та взаємодії органів виконавчої влади з питань національної безпеки в інформаційній сфері, забезпечення інформаційної безпеки, виявлення та протидії дезінформації, ефективної протидії пропаганді, деструктивним інформаційним впливам і кампаніям, запобігання спробам маніпулювання громадською думкою; здійснення системних заходів, спрямованих на посилення спроможностей суб'єктів сектору безпеки та оборони, інших державних органів задля забезпечення інформаційної безпеки, виявлення та протидії дезінформації, ефективної протидії пропаганді, деструктивним інформаційним впливам і кампаніям, запобігання спробам маніпулювання громадською думкою, розвитку національної інфраструктури у відповідній сфері; удосконалення системи правового та наукового забезпечення інформаційної безпеки, виявлення та протидії дезінформації, ефективної протидії пропаганді, деструктивним інформаційним впливам і кампаніям, запобігання спробам маніпулювання громадською думкою; 5) участь у розбудові системи стратегічних комунікацій, організації та координації заходів щодо її розвитку; 6) участь у розробленні та реалізації Стратегії інформаційної безпеки України, здійсненні аналізу стану її реалізації, зокрема з питань ефективності заходів щодо протидії дезінформації; 7) участь у створенні інтегрованої системи

оцінки інформаційних загроз та оперативного реагування на них; 8) розроблення методології виявлення загрозливих інформаційних матеріалів маніпулятивного та дезінформаційного характеру; 9) сприяння взаємодії держави та інституцій громадянського суспільства щодо протидії дезінформації та деструктивним інформаційним впливам і кампаніям, організація та участь в інформаційно-просвітницьких заходах з питань підвищення медіа-грамотності суспільства; 10) вивчення, узагальнення й аналіз досвіду інших держав і міжнародних організацій з протидії дезінформації та підготовка пропозицій щодо його використання в Україні; 11) бере участь у визначенні пріоритетів залучення міжнародної технічної допомоги з питань забезпечення інформаційної безпеки, виявлення та протидії дезінформації, ефективної протидії пропаганді, деструктивним інформаційним впливам і кампаніям, запобігання спробам маніпулювання громадською думкою [117].

Своєю чергою, Національний координаційний центр кібербезпеки є робочим органом Ради національної безпеки і оборони України, утвореним відповідно до рішення Ради національної безпеки і оборони України від 27 січня 2016 року «Про Стратегію кібербезпеки України», уведеного в дію Указом Президента України від 15 березня 2016 року № 96. Основними завданнями Центру, наприклад, є: 1) здійснення координації та контролю за діяльністю суб'єктів сектору безпеки і оборони, які забезпечують кібербезпеку; 2) здійснення аналізу: стану кібербезпеки; стану кіберзахисту критично важливих об'єктів інфраструктури; результатів проведення огляду національної системи кібербезпеки, огляду стану кіберзахисту державних інформаційних ресурсів та критичної інформаційної інфраструктури; стану готовності суб'єктів забезпечення кібербезпеки до виконання завдань з питань протидії кіберзагрозам, здійснення превентивних заходів у боротьбі з кіберзлочинністю; стану фінансового та організаційного забезпечення програм та заходів із реалізації державної політики у сфері забезпечення кібербезпеки України; стану виконання вимог законодавства щодо

кіберзахисту державних електронних інформаційних ресурсів, інформації, вимога щодо захисту якої встановлена законом, а також критичної інформаційної інфраструктури; даних про кіберінциденти стосовно державних електронних інформаційних ресурсів та критично важливих об’єктів інфраструктури; стану забезпечення кадрами національної системи кібербезпеки; 4) прогнозування та виявлення потенційних та реальних загроз у сфері кібербезпеки України; 5) участь у забезпеченні розроблення і впровадження суб'єктами забезпечення кібербезпеки механізмів обміну інформацією, необхідною для організації реагування на кібератаки і кіберінциденти, усунення їх чинників та негативних наслідків [153].

2. Кабінет Міністрів України. Згідно положень Закону України «Про Кабінет Міністрів України» від 27 лютого 2014 року № 794-VII означений суб’єкт публічного адміністрування є вищим органом у системі органів виконавчої влади, здійснюючи її безпосередньо та через міністерства, інші центральні органи виконавчої влади, Раду міністрів Автономної Республіки Крим та місцеві державні адміністрації, спрямовує, координує та контролює діяльність цих органів [152]. В досліджуваному контексті через свої структури, зокрема Управління стратегії розвитку інформаційних ресурсів та технологій, він втілює в життя державну політику в галузі інформаційної безпеки, забезпечуючи координацію та взаємодію між різними відомствами та організаціями [193, с. 10]. Тобто, Кабінет Міністрів України має універсально-управлінський адміністративно-правовий статус у сфері захисту інформації, який проявляється у здійсненні ним нормотворчої, організаційно-розпорядчої, координаційної та контрольної функцій щодо діяльності інших органів публічної адміністрації у цій сфері.

Основним з таких в досліджуваному контексті є Міністерство цифрової трансформації. Згідно положень чинного законодавства Мінцифри є головним органом у системі центральних органів виконавчої влади, що забезпечує формування та реалізацію державної політики: у сферах цифровізації, цифрового розвитку, цифрової економіки, цифрових інновацій

та технологій, робототехніки та роботизації, розвитку штучного інтелекту, розвитку напівпровідникових технологій, електронного урядування та електронної демократії, розвитку інформаційного суспільства, інформатизації; у сфері впровадження електронного документообігу; у сфері розвитку цифрових навичок та цифрових прав громадян; у сферах відкритих даних, публічних електронних реєстрів, розвитку національних електронних інформаційних ресурсів та інтероперабельності, електронних комунікацій та радіочастотного спектра, розвитку інфраструктури широкосмугового доступу до Інтернету, електронної комерції та бізнесу; у сфері надання електронних та адміністративних послуг; у сферах електронної ідентифікації та електронних довірчих послуг; у сфері розвитку ІТ-індустрії; у сфері розвитку та функціонування правового режиму Дія Сіті; у сфері хмарних послуг; у сфері організації та проведення азартних ігор та лотерейній сфері [116].

3. Служба безпеки України. Мова йде про державний орган спеціального призначення з правоохоронними функціями, який забезпечує державну безпеку України. Загалом на Службу безпеки України покладається у межах визначеної законодавством компетенції захист державного суверенітету, конституційного ладу, територіальної цілісності, науково-технічного і оборонного потенціалу України, законних інтересів держави та прав громадян від розвідувально-підривної діяльності іноземних спеціальних служб, посягань з боку окремих організацій, груп та осіб, а також забезпечення охорони державної таємниці [158].

Відповідно до положень Закону України «Про основні засади забезпечення кібербезпеки України» Служба безпеки України здійснює запобігання, виявлення, припинення та розкриття злочинів проти миру і безпеки людства, які вчиняються у кіберпросторі; здійснює контррозвідувальні та оперативно-розшукові заходи, спрямовані на боротьбу з кібертероризмом та кібершпигунством, негласно перевіряє готовність об’єктів критичної інфраструктури до можливих кібератак та кіберінцидентів; протидіє кіберзлочинності, наслідки якої можуть створити

загрозу життєво важливим інтересам держави; розслідує кіберінциденти та кібератаки щодо державних електронних інформаційних ресурсів, інформації, вимога щодо захисту якої встановлена законом, критичної інформаційної інфраструктури; забезпечує реагування на кіберінциденти у сфері державної безпеки [157; 193, с. 10].

З боку наукової доктрини визначається, що специфіка адміністративно-правового статусу органів Служби безпеки України полягає в тому, що вони є спеціальними правоохоронними органами, що передбачено на законодавчому рівні та підтверджується наявністю у них науково обґрунтованих ознак, притаманних правоохоронним органам, що дозволяє їм брати участь у правоохоронних адміністративно-правових відносинах [63, с. 140]. Тому логічно адміністративно-правовий статус Служби безпеки України у сфері захисту інформації визначити як спеціальний, що об’єктивує поєднанням адміністративно-правових, оперативно-розшукових та контррозвідувальних інструментів впливу, спрямованих на запобігання, виявлення, припинення та нейтралізацію загроз інформаційній безпеці держави, а також на забезпечення охорони інформації з обмеженим доступом.

Отже, з наведеного матеріалу прослідковується наша основна позиція стосовно того, що адміністративно-правовий статус органів публічної адміністрації у сфері захисту інформації більшою мірою характеризується через функціональний компонент, представлений сукупністю цільових орієнтирів їх діяльності, що відображають основне призначення відповідних органів у механізмі забезпечення інформаційної безпеки держави. Йдеться не стільки про формально визначені елементи статусу, скільки про ті напрями публічно-владного впливу, які вони реалізують у процесі виконання покладених на них завдань.

2.2. Повноваження органів публічної адміністрації у сфері захисту інформації

З урахуванням викладених теоретико-методологічних підходів до розуміння адміністративно-правового статусу органів публічної адміністрації у сфері захисту інформації, а також обґрунтованої його функціональної спрямованості, на нашу думку, логічним є перехід до аналізу конкретного інструментарію реалізації такого статусу. Адже саме через практичну реалізацію визначених цілей і завдань відповідних суб'єктів відбувається їх включення у систему адміністративно-правових відносин у досліджуваній сфері.

Тому вбачаємо доречним звернути увагу на категорію повноважень як базового елементу адміністративно-правового статусу досліджуваних суб'єктів, який найбільш явно корелює із функціональним призначенням органів публічної адміністрації.

Однак варто вказати, що звертаючись до чинного законодавства України, в ньому простежується довільне застосування категорій «повноваження» та «компетенція», а також не міститься загального визначення поняття «компетенція органів державної влади», яким можна було б керуватися у законотворчій практиці. Серед 14551 постанов і законів, прийнятих Верховною Радою України у всіх скликаннях, в 111 актах вжито термін «компетенція» в сенсі повноважень, наданих законом [104, с. 100; 187, с. 19]. Тому не викликає подиву факт того, що вчені неодноразово у своїх дослідженнях звертались до проблеми визначення компетенції державних органів. При цьому й досі серед науковців відсутня єдина точка зору щодо змісту означених понять [91, с. 86; 94].

Так, наприклад, Н. О. Армаш, компетенцію визначає як елемент правового статусу, який встановлює сукупність юридично встановлених прав та обов'язків органу виконавчої влади або його керівника, реалізація яких забезпечує виконання їх основних функцій [7, с. 97]. Тобто на думку авторки

«компетенція» пов’язана із посадою особи [70]. Схожу позицію дотримувався і законодавець при формулюванні терміну «компетенція». Наприклад, у Державному стандарті початкової загальної освіти, який був затверджений Постановою Кабінету Міністрів України від 20 квітня 2011 року № 462, термін «компетенція» тлумачився як: «суспільно визнаний рівень знань, умінь, навичок, ставлень у певній сфері діяльності людини» [135]. Аналогічний підхід до роз’яснення аналізованого терміну можна зустріти у ратифікованій Директиві Європейського Союзу 2017/2397 від 12 грудня 2017 року «Про визнання професійних кваліфікацій у внутрішньому судноплавстві та про скасування директив Ради 91/672/ЄЕС та 96/50/ЄС». У цьому документі «компетенція» визначена як: «доведена здатність використовувати знання та навички» [44]. Але, варто погодитись з позицією Ю. Кондрацького, що в зазначених трактуваннях розкривається термін «компетентність», а не «компетенція» [70].

Своєю чергою, в енциклопедичній літературі компетенція визначається як сукупність предметів відання, функцій, повноважень, прав і обов’язків органу державної влади, органу місцевого самоврядування або їх посадової особи чи службової особи, що визначаються Конституцією [30, с. 210; 187, с. 19]. З точки зору наукової доктрини варто виділити такі інтерпретації цього терміну: 1) сукупність визначених Конституцією та законами предметів відання і повноважень, де повноваження – це конкретні права та обов’язки (В. Кравченко) [82, с. 295]; 2) сфера діяльності певного органу (що саме повинен робити даний орган) та необхідні для цього повноваження (А. Солонар) [174, с. 253]; 3) дає цілком однозначну відповідь на питання, що має право і що повинен робити публічний орган за кожним із доручених йому напрямів суспільного управління з метою цілеспрямованого впорядкування громадського життя, згідно з його стратегічними цілями й завданнями. Державно-владним установленням компетенції чітко фіксуються обсяг і зміст діяльності того чи іншого суб’єкта. Одночасно проводиться розмежування його функцій із функціями інших суб’єктів, які співвідносяться з ним як «за

вертикаллю», так і «за горизонталлю». Інакше кажучи, закріплюється певний порядок розподілу всієї сукупності державних функцій (С. Серьогіна) [37, с. 45–46; 91]; 4) сукупність основних (повноваження та предмет ведення) та організаційних (призначення органу, мети та завдання, професіоналізм посадових осіб) елементів, які у своєму взаємозв'язку дають можливість якісного виконання покладених на органи державної виконавчої влади та місцевого самоврядування функцій (М. Потіп) [91; 123, с. 35]; 5) це самостійне юридичне поняття, відмінне від понять «предмети відання», «правоздатність» тощо. Компетенція органу завжди дає уявлення про те, в якій галузі державного управління він діє, якою галуззю керує, які підприємства і установи, що йому підпорядковані і навіть який зміст виконуваних ним функцій. Але досягається це не перерахуванням предметів, питань, сфер, а вказівкою на права й обов'язки органу у відносинах, що стосуються цих предметів, питань і сфер. Ці права та обов'язки можуть бути деталізовані або ж сформульовані в загальному вигляді, на кшталт «реалізує державну політику». Однак і в першому, і в другому випадку йдеться про характеристику відносин органу до певних сфер, предметів і питань, а не про них самих. Отже, під компетенцією слід розуміти сукупність прав і обов'язків органу стосовно галузей, сфер, об'єктів управління («предметів відання»), а не права та обов'язки плюс згадані предмети відання (О. Дніпров) [47, с. 260]; 7) сукупність предметів відання і владних повноважень, передбачених законодавством або іншими нормативно-правовими актами, шляхом реалізації яких орган виконавчої влади здійснює свою діяльність (О. Сікорський) [94; 171, с. 54].

Що ж стосується розкриття змісту поняття «повноваження», то вчені не мають єдиної точки зору. Деякі вважають, що повноваження – це сукупність прав і обов'язків державних органів і громадських організацій, а також посадових та інших осіб, закріплених за ними у встановленому законодавством порядку для здійснення покладених на них функцій [24, с. 639]. Інші – що повноваження слід розглядати як право, надане кому-

небудь для здійснення чогось, компетенція, доручення, повновласть [97, с. 469]. На думку А. Солонар, перше визначення є більш повним і конкретизованим, адже відображає всі структурні елементи повноваження. Однак з огляду на друге визначення не можна погодитися з тим, що під повноваженням можна розуміти певне право чи доручення. Право – це можливість певної поведінки окремого суб'єкта правовідносин, яка забезпечена відповідним обов'язком, що у своїй сукупності і становлять певне повноваження. Що стосується доручення, то дане поняття стосується сфери представницьких відносин між одним суб'єктом та іншим, у результаті яких одному з них доручається вчинення конкретних процесуальних дій [174]. Вчений також зауважує, що поняття повноваження вчені розглядають таким чином: повноваження як сукупність прав та обов'язків; повноваження як складовий елемент компетенції; повноваження як функції. Проте найбільш поширеною точкою зору, у якій сходяться більшість авторів, є включення у зміст поняття повноваження певних прав та обов'язків. Із даним твердженням неможливо не погодитися [174].

Отже, якщо коротко, то повноваження органів публічної адміністрації у сфері захисту інформації відображають міру та спосіб публічно-владного впливу органів публічної адміністрації на суспільні відносини у сфері захисту інформації. Вони виступають тією юридичною формою, через яку функціональна диференціація цих органів набуває свого практичного вияву – від нормотворчої та координаційної діяльності до реалізації контрольно-наглядових, правоохоронних та спеціальних заходів інформаційної безпеки.

Зауважимо, що положення статті 10 Закону України «Про захист інформації в інформаційно-комунікаційних системах» визначають наступне:

«Мінімальні вимоги щодо заходів захисту як базовий профіль безпеки щодо систем, власниками або розпорядниками яких є органи державної влади, державні органи, державні підприємства, установи та організації, органи місцевого самоврядування, в яких обробляються державні інформаційні ресурси або інформація з обмеженим доступом, вимога щодо

захисту якої встановлена законом (крім вимог щодо забезпечення захисту інформації, встановлених законом у сфері надання платіжних, банківських та інших фінансових послуг), встановлюються Кабінетом Міністрів України.».

«Спеціально уповноважений центральний орган виконавчої влади з питань організації спеціального зв'язку та захисту інформації:

розробляє пропозиції щодо державної політики у сфері захисту інформації та забезпечує її реалізацію в межах своєї компетенції;

визначає вимоги та порядок створення комплексної системи захисту державних інформаційних ресурсів або інформації з обмеженим доступом, вимога щодо захисту якої встановлена законом;

організовує проведення державної експертизи комплексних систем захисту інформації, експертизи та підтвердження відповідності засобів технічного і криптографічного захисту інформації;

здійснює контроль за забезпеченням захисту державних інформаційних ресурсів або інформації з обмеженим доступом, вимога щодо захисту якої встановлена законом;

здійснює заходи щодо виявлення загроз державним інформаційним ресурсам від несанкціонованих дій та витоку інформації технічними каналами в інформаційних, електронних комунікаційних, інформаційно-комунікаційних та технологічних системах, надає рекомендації щодо запобігання таким загрозам;

забезпечує реалізацію та здійснює методичне керівництво щодо підтвердження відповідності комплексної системи захисту інформації, авторизації з безпеки, порядок проведення яких затверджується Кабінетом Міністрів України;

затверджує порядок ведення переліку авторизованих систем з безпеки;

здійснює включення авторизованих систем з безпеки до переліку авторизованих систем з безпеки та виключення з такого переліку;

у порядку, встановленому Кабінетом Міністрів України, розробляє та затверджує базовий профіль безпеки як мінімальний набір заходів захисту,

встановлених для відповідної категорії інформаційних, електронних комунікаційних та інформаційно-комунікаційних систем, в яких обробляються державні інформаційні ресурси.»

«Органи державної влади, державні органи, органи місцевого самоврядування з урахуванням набору мінімальних вимог щодо заходів захисту (базового профілю безпеки), відповідних стандартів, політик безпеки, призначення системи, її структурно-функціональних характеристик, результатів аналізу ризиків безпеки та особливостей функціонування системи розробляють та затверджують цільові профілі безпеки для інформаційних, електронних комунікаційних, інформаційно-комунікаційних та технологічних систем, власником або розпорядником яких вони є.»

«Органи державної влади, державні органи в межах своїх повноважень у відповідній сфері або галузі розробляють та за погодженням із Державною службою спеціального зв'язку та захисту інформації України затверджують галузеві профілі безпеки для відповідної сфери або галузі з урахуванням мінімальних вимог щодо заходів захисту (базового профілю безпеки), а також відповідних стандартів, політик безпеки та особливостей функціонування системи у відповідній сфері або галузі.»

«Порядок затвердження цільових та галузевих профілів безпеки затверджується Кабінетом Міністрів України.»

«Національний банк України встановлює вимоги щодо забезпечення захисту інформації, вимоги щодо захисту якої встановлені законом у сфері надання платіжних, банківських та інших фінансових послуг (крім професійної діяльності на ринках капіталу та діяльності в системі накопичувального пенсійного забезпечення), державне регулювання та нагляд за діяльністю яких здійснює Національний банк України, валютного регулювання та валютного нагляду, а також у системі депозитарного обліку Національного банку України.»

«Міністерство оборони України та Служба безпеки України в порядку, встановленому Кабінетом Міністрів України, розробляють і затверджують

галузеві та/або цільові профілі безпеки для інформаційних, електронних комунікаційних та інформаційно-комунікаційних систем, власником (розпорядником) яких є відповідно Міністерство оборони України та/або Збройні Сили України і Служба безпеки України» [149].

Аналіз зазначеного спонукає до формулювання таких висновків:

– по-перше, повноваження органів публічної адміністрації у сфері захисту інформації мають чітко виражену ієрархічну структуру, в межах якої Кабінет Міністрів України виконує нормотворчу та системоутворюючу функцію, визначаючи мінімальні вимоги до захисту інформації (базовий профіль безпеки), тоді як інші суб’єкти конкретизують ці вимоги на галузевому та інституційному рівнях;

– по-друге, простежується функціональна диференціація повноважень між органами: Державна служба спеціального зв'язку та захисту інформації України наділена спеціалізованими повноваженнями у сфері формування та реалізації політики, нормативного регулювання, контролю, експертизи та методичного забезпечення, що підтверджує її ключову роль як центрального органу технічного та криптографічного захисту інформації;

– по-третє, уповноважені органи вправі не тільки встановлювати вимоги, а й забезпечувати їх реалізацію через процедури експертизи, авторизації, моніторингу та надання рекомендацій;

– по-четверте, повноваження органів публічної адміністрації у досліджуваній сфері реалізуються через механізм профілювання безпеки (базові, галузеві та цільові профілі), що дозволяє адаптувати загальні вимоги до конкретних умов функціонування інформаційних систем, рівня ризиків та специфіки відповідної сфери;

– по-п’яте, закріплено секторальний підхід до регулювання, відповідно до якого окремі органи, зокрема Національний банк України, Міністерство оборони України та Служба безпеки України, наділяються спеціальними повноваженнями щодо визначення вимог до захисту інформації з урахуванням специфіки відповідних сфер (фінансової, оборонної,

правоохоронної);

– по-шосте, характерною є декомпозиція відповідальності між суб’єктами, за якої органи державної влади та місцевого самоврядування не лише виконують встановлені вимоги, а й самостійно розробляють цільові профілі безпеки для підпорядкованих систем, що свідчить про їх залучення до безпосередньої реалізації заходів захисту інформації.

Водночас, в контексті повноважень «спеціально уповноваженого центрального органу виконавчої влади з питань організації спеціального зв'язку та захисту інформації» варто уточнити, що профільне законодавство також містить вказівку про те, що: «Положення про центральний орган виконавчої влади, що забезпечує формування та реалізацію державної політики у сферах організації спеціального зв’язку, захисту інформації, затверджує Кабінет Міністрів України» [129].

Так постановою Кабінету Міністрів України від 3 вересня 2014 року № 411 затверджено Положення про Адміністрацію Державної служби спеціального зв’язку та захисту інформації України. Її положення визначають таке:

1) Адміністрація Державної служби спеціального зв’язку та захисту інформації України (Адміністрація Держспецзв’язку) є спеціально уповноваженим центральним органом виконавчої влади з питань організації спеціального зв’язку та захисту інформації;

2) Адміністрація Держспецзв’язку відповідно до покладених на неї завдань: забезпечує нормативно-правове регулювання у сферах криптографічного і технічного захисту інформації, організації спеціального зв’язку, урядового фельд’єгерського зв’язку, захисту державних інформаційних ресурсів та інформації, вимога щодо захисту якої встановлена законом, у кіберпросторі, в інформаційно-комунікаційних системах і на об’єктах інформаційної діяльності, протидії технічним розвідкам, кіберзахисту об’єктів критичної інформаційної інфраструктури; здійснює технічне регулювання у сферах криптографічного і технічного захисту

інформації, кіберзахисту об’єктів критичної інфраструктури, протидії технічним розвідкам, захисту державних інформаційних ресурсів та інформації, вимога щодо захисту якої встановлена законом, в інформаційно-комунікаційних системах і на об’єктах інформаційної діяльності, організацію, координацію та проведення робіт з підтвердження відповідності, розроблення в установленому порядку технічних регламентів; здійснює методичне керівництво та координацію діяльності державних органів, органів місцевого самоврядування, військових формувань, утворених відповідно до законів України, підприємств, установ і організацій незалежно від форми власності у сферах криптографічного і технічного захисту інформації, протидії технічним розвідкам, а також з питань, пов’язаних із запобіганням вчиненню порушень безпеки інформації в інформаційно-комунікаційних системах, виявленням та усуненням наслідків інших несанкціонованих дій щодо державних інформаційних ресурсів та інформації, вимога щодо захисту якої встановлена законом, в інформаційно-комунікаційних системах; контролює виконання вимог законодавства у сфері захисту інформації в приміщеннях абонентів урядового зв’язку; установлює порядок розроблення, виготовлення та постачання ключових документів та державних шифрів до засобів криптографічного захисту інформації, що містить державну таємницю, службову інформацію та публічну інформацію з обмеженим доступом; установлює порядок організації та проведення державної експертизи у сфері криптографічного та технічного захисту інформації, забезпечує організацію проведення державної експертизи щодо відсутності у програмному забезпеченні недокументованих функцій, проводить експертні та тематичні дослідження у сфері криптографічного захисту інформації, визначає криптографічні алгоритми як рекомендовані, надає допуск до експлуатації засобів криптографічного захисту інформації, видає експертні висновки за результатами державної експертизи у сфері криптографічного захисту інформації, свідоцтва про допуск до експлуатації засобів криптографічного захисту інформації, реєструє експертні висновки за результатами державної

експертизи у сфері технічного захисту інформації, декларації та атестати відповідності комплексних систем захисту інформації; установлює порядок створення та допуску до експлуатації, допускає до експлуатації засоби криптографічного захисту службової інформації та інформації, що становить державну таємницю, засоби, комплекси та системи спеціального зв'язку, визначає криптографічні алгоритми для застосування у засобах криптографічного захисту інформації; установлює порядок надання висновків та погоджень міжнародних передач криптосистем, засобів криптографічного і технічного захисту інформації, у тому числі тих, що є складовими частинами озброєння, військової та спеціальної техніки, надає такі висновки і погодження; установлює порядок здійснення державного контролю і здійснює державний контроль за станом криптографічного і технічного захисту державних інформаційних ресурсів та інформації, вимога щодо захисту якої встановлена законом, у державних органах, органах місцевого самоврядування, військових формуваннях, утворених відповідно до законів України, на підприємствах, в установах і організаціях незалежно від форми власності, зокрема в закордонних дипломатичних установах України, національних контингентах за кордоном, місцях постійного і тимчасового перебування Президента України, Голови Верховної Ради України та Прем'єр-міністра України, а також під час діяльності на території України іноземних інспекційних груп відповідно до міжнародних договорів України, згода на обов'язковість яких надана Верховною Радою України; установлює порядок здійснення державного контролю і здійснює державний контроль за додержанням вимог безпеки під час розроблення, виробництва, використання, експлуатації, сертифікаційних випробувань, проведення тематичних досліджень, експертизи, вивезення та знищення криптографічних систем і засобів криптографічного захисту інформації та обладнання спеціального зв'язку, що мають гриф обмеження доступу; організовує впровадження комплексних систем захисту інформації на об'єктах інформаційної діяльності та в інформаційно-комунікаційних системах

закордонних дипломатичних установ України за рахунок коштів, передбачених у законі про Державний бюджет України на функціонування та утримання таких установ [141] та багато інших.

Зазначене дає нам розуміння того, що повноваження органів публічної адміністрації у сфері захисту інформації не мають виключно відокремленого характеру, а значною мірою перетинаються та взаємодоповнюють одне одного. Зокрема, окремі функції, пов'язані з формуванням вимог до захисту інформації, їх конкретизацією, впровадженням та контролем за дотриманням, реалізуються різними суб'єктами паралельно або у взаємодії, що зумовлює наявність спільних зон компетенції.

Показовим з точки зору реалізації повноважень суб'єктів у сфері захисту інформації, оскільки дозволяє чітко окреслити їх функціональне розмежування та юридичну природу діяльності є рішення № 125202700 від 17 лютого 2025 року Київського окружного адміністративного суду [165]. Коротко проаналізуємо його у контексті розмежування повноважень органів публічної адміністрації у сфері захисту інформації.

1. Повноваження спеціально уповноваженого суб'єкта – Держспецзв'язку. Суд підтвердив, що Адміністрація Держспецзв'язку є спеціально уповноваженим суб'єктом у сфері захисту інформації, який: а) формує та реалізує державну політику у сфері технічного та криптографічного захисту інформації; 2) здійснює державний контроль за станом технічного захисту інформації; 3) має право проводити перевірки незалежно від форми власності суб'єкта; 4) виявляє загрози інформаційним ресурсам та надає рекомендації щодо їх усунення.

Важливим є висновок суду про те, що такі перевірки: здійснюються на підставі спеціального законодавства (а не загального законодавства про держнагляд у сфері господарської діяльності); мають контрольно-аналітичний, а не каральний характер. Таким чином, суд фактично розмежував: державний контроль у сфері інформаційної безпеки та державний нагляд (контроль) у сфері господарської діяльності.

2. Повноваження СБУ як співсуб'єкта. У справі також встановлено участь Служби безпеки України у перевірці. Це свідчить про: міжвідомчий характер системи захисту інформації; наявність у СБУ повноважень щодо участі у заходах, пов'язаних із захистом державних інформаційних ресурсів.

Водночас суд підкреслив, що така перевірка не є слідчою (розшуковою) дією, навіть якщо інформація надійшла в межах кримінального провадження.

3. Повноваження власника та адміністратора інформаційних систем (тут йдеться про ДП «НАІС»). Суд чітко окреслив і обов'язки суб'єкта, що експлуатує інформаційні системи: ДП «НАІС» є адміністратором державних реєстрів; відповідає за: технічне та технологічне функціонування систем; збереження та захист даних; управління доступом до реєстрів.

На підставі законодавства суд підтвердив, що відповідальність за захист інформації покладається на власника (адміністратора) системи; такий суб'єкт зобов'язаний бути об'єктом державного контролю.

4. Суттєвим є висновок суду щодо акту перевірки: акт: складається у довільній формі (для цільових перевірок); має інформаційно-аналітичний характер; не породжує юридичних наслідків у вигляді санкцій. Відповідно, він не є рішенням у класичному розумінні адміністративного права та не порушує права суб'єкта господарювання сам по собі.

Це означає, що акт перевірки у сфері технічного захисту інформації – це інструмент «м'якого» впливу («soft law»), а не примусу.

5. Межі повноважень та законність перевірки. Суд встановив, що Держспецзв'язку діяв в межах повноважень та на підставі закону, а також у спосіб, передбачений нормативними актами (Наказ №87). Зокрема: перевірка була позаплановою, але обґрунтованою (наявність інформації про порушення), оформлена належним приписом, строки не порушені (оскільки вони не регламентовані жорстко).

Отже, аналізоване рішення суду демонструє таку модель розподілу повноважень основних суб'єктів у сфері захисту інформації:
а) Держспецзв'язку – ключовий суб'єкт, який формує відповідну політику,

здійснює контрольні функції, а також загалом координує систему технічного захисту інформації; б) СБУ – допоміжний (спеціальний) суб'єкт, адже залучається до перевірок та забезпечує безпековий компонент; в) власники/адміністратори систем (як ДП «НАІС») – несуть основну відповідальність за захист інформації, є об'єктами контролю.

Тобто з аналізу цього судового рішення випливає, що публічне адміністрування у сфері захисту інформації реалізується через: контрольні повноваження держави, які мають превентивний характер; обов'язок підконтрольних суб'єктів забезпечувати належний рівень захисту; координацію між різними органами публічної адміністрації.

Отже, дана справа підтверджує, що система захисту інформації в Україні побудована за моделлю, де держава не лише встановлює правила, але й здійснює постійний моніторинг їх дотримання без прямого втручання у господарську діяльність, що відповідає сучасним підходам до публічного адміністрування.

Поряд із розглянутими ключовими суб'єктами, які безпосередньо здійснюють формування та реалізацію державної політики, а також контроль у сфері захисту інформації, важливе місце у відповідному механізмі посідають й інші органи публічної адміністрації, повноваження яких мають переважно координаційний, аналітичний та стратегічний характер. Як зауважено попередньо, їхня діяльність не спрямована на безпосереднє впровадження заходів технічного чи криптографічного захисту інформації, однак вони забезпечують узгодженість дій різних органів, формування єдиних підходів та реагування на сучасні загрози.

У цьому контексті можна вести мову, наприклад, про Національний координаційний центр кібербезпеки. Згідно нормативних положень Центр для виконання покладених на нього завдань має право в установленому порядку: 1) запитувати та одержувати від органів виконавчої влади, органів місцевого самоврядування, підприємств, установ і організацій статистичні дані, інформацію, довідкові та інші матеріали, необхідні для вирішення

питань, що належать до його компетенції; 2) користуватися інформаційними базами даних державних органів, державними, в тому числі урядовими, системами зв'язку і комунікацій, мережами спеціального зв'язку та іншими технічними засобами; 3) утворювати в разі потреби експертні та робочі групи, залучати до виконання окремих робіт і завдань, вивчення окремих питань працівників центральних та місцевих органів виконавчої влади, органів місцевого самоврядування, підприємств, установ та організацій, провідних вчених і фахівців; 4) ініціювати проведення аудиту інформаційної безпеки державних інформаційних ресурсів та критично важливих об’єктів інфраструктури; 5) організовувати проведення науково-дослідних, дослідно-конструкторських та інших робіт у галузі кібербезпеки та захисту критично важливих об’єктів інфраструктури; 6) ініціювати проведення конференцій, семінарів, нарад з питань, вирішення яких віднесено до повноважень Центру, із залученням державних органів, інших організацій та установ; 7) використовувати можливості Головного ситуаційного центру Ради національної безпеки і оборони України, а також за згодою Голови Державної служби спеціального зв’язку та захисту інформації України - Державного центру кіберзахисту Державної служби спеціального зв’язку та захисту інформації України, за згодою керівників державних органів - центрів забезпечення кібербезпеки державних органів, за згодою керівників підприємств, установ та організацій незалежно від форми власності, які віднесені до критично важливих об’єктів інфраструктури, - центрів забезпечення кібербезпеки таких об’єктів; 8) порушувати питання про проведення перевірок діяльності суб'єктів забезпечення кібербезпеки, зокрема операторів телекомунікаційних послуг, щодо виконання вимог технічного захисту інформації та ліцензійних умов; 9) взаємодіяти відповідно до покладених завдань з державними органами, органами місцевого самоврядування, підприємствами, установами та організаціями [153].

Або ж наведено приклад повноважень Центру протидії дезінформації, який для виконання покладених на нього завдань: 1) одержує в

установленому порядку від органів виконавчої влади, правоохоронних та розвідувальних органів, органів прокуратури, органів місцевого самоврядування, підприємств, установ і організацій незалежно від форм власності та підпорядкування статистичні дані, інформацію, довідкові та інші матеріали; 2) користується в установленому законодавством порядку інформаційними базами даних державних органів, державними, зокрема урядовими, системами зв'язку і комунікацій, мережами спеціального зв'язку та іншими технічними засобами; 3) створює в разі потреби експертні та робочі групи, залучає в установленому порядку до вивчення окремих питань представників державних органів, органів місцевого самоврядування, підприємств, установ і організацій; 4) виступає замовником науково-дослідних робіт з питань протидії дезінформації, деструктивним інформаційним впливам і кампаніям та забезпечення інформаційної безпеки; 5) організовує проведення конференцій, семінарів, нарад, інших заходів; 6) взаємодіє з органами державної влади, правоохоронними та розвідувальними органами, органами місцевого самоврядування, а також підприємствами, установами і організаціями, в тому числі іноземними; 7) встановлює партнерські відносини з центрами стратегічних комунікацій і протидії дезінформації іноземних держав та міжнародних організацій, що займаються питаннями забезпечення інформаційної безпеки, виявлення та протидії дезінформації, ефективної протидії пропаганді, деструктивним інформаційним впливам і кампаніям, запобігання спробам маніпулювання громадською думкою, здійснює обмін з ними в установленому порядку інформацією з цих питань; 8) бере участь у структурованих діалогах з питань стратегічних комунікацій і протидії дезінформації між Україною та міжнародними організаціями й іноземними державами; 9) здійснює інші дії, передбачені законодавством України [117].

Аналіз зазначеного свідчить, що їх компетенція концентрується навколо таких функціональних напрямів, як збір та узагальнення інформації, аналітичне опрацювання даних, ініціювання контрольних та дослідницьких

заходів, формування експертного середовища, а також налагодження міжвідомчої та міжнародної співпраці, що свідчить про значну обмеженість кола їхніх повноважень у досліджуваній сфері.

Таким чином, як підсумок розкриття порушених питань варто узагальнити, що повноваження органів публічної адміністрації у сфері захисту інформації зводяться до нормотворчих, контрольних, координаційних, аналітичних та спеціальних. Зрозуміло, що ключовими з таких є саме останні, адже забезпечують формування та реалізацію державної політики, нормативне регулювання і державний контроль у сфері технічного та криптографічного захисту інформації. Водночас інші суб'єкти, зокрема СБУ, галузеві та інші органи, виконують спеціалізовані або допоміжні функції, що забезпечують практичну реалізацію вимог інформаційної безпеки.

2.3. Взаємодія органів публічної адміністрації з іншими суб'єктами у сфері захисту інформації

Варто зауважити, що нині актуальною є наукова думка, що сучасні виклики у сфері інформаційної безпеки – зокрема гібридна агресія, кіберзлочинність та масове поширення дезінформації – обумовлюють необхідність скоординованої взаємодії органів публічної влади у формуванні та реалізації політики інформаційної безпеки. Автори зазначають, що у цьому контексті надзвичайно багато питань, що потребують наукового супроводу. Водночас у роботах, присвячених адміністративно-правовому забезпеченню інформаційної безпеки, широко розглядається роль обміну даними як ключового елементу взаємодії, що є основою для формування своєчасних рішень, оцінки загроз та координування дій суб'єктів. Проте конкретизація питання вивчення особливостей взаємодії органів публічної адміністрації з

іншими суб’єктами у сфері захисту інформації не знайшла свого наукового висвітлення [201].

Для нас означене є вихідною методологічною позицією, яка дозволяє розглядати взаємодію органів публічної адміністрації не як допоміжний елемент їх діяльності, а як самостійний адміністративно-правовий інститут, що забезпечує цілісність функціонування системи захисту інформації.

Розпочнемо з того, що у контексті філософського підходу категорія взаємодії є фундаментальною, ключовою для глибокого та конструктивного розуміння інших категорій, таких як «рух», «детермінація», «причина», «зв’язок», «вплив», «дія» та ін. Категорії «причина» і «дія» логічно відтворюють один з моментів руху і взаємодії речей на сутнісному рівні. Причина, переходячи в дію, відроджується у ній і навпаки. У цьому взаємному обумовленні причина і дія зливаються у взаємодію; однонаправлена детермінація переходить в симетричну, взаємну детермінацію. Відповідно, речі виступають одночасно як активні та пасивні, діють зовні і як такі, що відчувають дію на собі, як рушійні та приведені в рух (але в різних взаємозв’язках). Причинність виступає як взаємна причинність, взаємодія, як виявлення саморуху матерії [64, с. 34].

З цього маємо, що досліджуване явище передбачає не просто вплив одного об’єкта на іншого, а це взаємний процес, де обидві сторони одночасно впливають одна на одну та змінюються під впливом одна одної. Тому цілком логічним є словникове визначення терміну «взаємодія» як «взаємний зв’язок між предметами у дії, а також погоджена дія між ким-, чим-небудь, взаємний вплив тіл чи частинок, який зумовлює зміну стану їхнього руху» [25].

Варто зауважити, що в юридичній літературі теоретичні питання взаємодії державно-правових явищ досить широко освітлені, і є досить велика кількість тлумачень цього терміну, але не дивлячись на це, відсутня однозначна характеристика сутності даної категорії і це обумовлюється багатогранністю семантики самого слова «взаємодія» та акцентуванням уваги у визначенні цієї категорії на детальних аспектах. «Взаємодія» є як

міжгалузевою категорією, так і адміністративно-правовою. Найчастіше, взаємодія визначається як погоджена діяльність, або кооперація праці. Сама ж діяльність – категорія настільки різнопланова, що дати їй однозначну інтерпретацію неможливо. Саме тому багато вчених для формулювання дефініції «взаємодія» пропонують брати за основу принципово різні функціональні аспекти взаємодії [118, с. 338].

Разом з тим слід уточнити, що згідно з термінологією законодавства, взаємодією є [54, с. 40]: а) в загальному аспекті – 1) спосіб забезпечення певної дії, який полягає у спільній діяльності конкретних суб'єктів, спрямованій на здійснення їх компетенції (аналіз положень Наказу Адміністрації Державної прикордонної служби України «Про затвердження Порядку дій посадових осіб органів охорони державного кордону Державної прикордонної служби України щодо установлення режиму в пунктах пропуску через державний кордон, здійснення контролю за його додержанням, а також організації і забезпечення взаємодії та координації контрольних органів і служб, що здійснюють різні види контролю або беруть участь у забезпеченні режиму в пунктах пропуску через державний кордон» від 29 серпня 2011 року № 627); 2) узгоджені за метою, завданням, місцем, часом та способом виконання завдань дії конкретних суб'єктів для досягнення мети (аналіз Наказів Міністерства внутрішніх справ України «Про затвердження Положення про організацію та несення служби з охорони дипломатичних представництв, консульських установ іноземних держав, представництв міжнародних організацій в Україні військовими частинами і підрозділами Національної гвардії України» від 2 лютого 2016 року № 74 та «Про затвердження Положення про організацію та несення служби з охорони органів державної влади військовими частинами і підрозділами Національної гвардії України» від 20 липня 2016 року № 692); б) в інформаційному аспекті – обмін інформацією (аналіз Рішення Національної комісії з цінних паперів та фондових ринків «Про затвердження Положення про функціонування фондових бірж» від 22 листопада 2012 року № 1688); в) в між секторальному

аспекті – існування та рівноправна комунікація різних об’єктів та суб’єктів на основі діалогу і взаємної поваги (аналіз Конвенції про охорону та заохочення розмаїття форм культурного самовираження від 20 жовтня 2005 року); г) в секторальному аспекті – функціонування всіх складових об’єкта/суб’єкта як єдиної системи, очолюваної командуванням (аналіз Наказу Міністерства інфраструктури України «Про затвердження Правил сертифікації авіаційних навчальних закладів цивільної авіації з підготовки льотного складу в Україні» від 29 березня 2002 року № 215); д) в управлінському аспекті – передача результатів виконання етапу технологічного процесу іншому суб’єкту, який несе відповідальність за результати виконання цього етапу технологічного процесу (аналіз Постанови Кабінету Міністрів України «Про затвердження Ліцензійних умов провадження господарської діяльності банків пуповинної крові, інших тканин і клітин людини згідно з переліком, затвердженим Міністерством охорони здоров’я» від 2 березня 2016 року № 286) [53, с. 68–69].

Додамо, що як управлінська категорія, взаємодія проявляється у внутрішній діяльності системи та в зовнішніх її функціях [93, с. 72]. Це означає, що варто вести мову як про внутрішньоорганізаційні процеси, пов’язані з координацією діяльності владних структур, розподілом повноважень і узгодженням управлінських рішень, так і про зовнішні зв’язки, що виникають у процесі співпраці з іншими суб’єктами публічного та приватного секторів.

Таким чином, можна узагальнити, що юридична природа категорії «взаємодія» репрезентується через процес узгодженої діяльності суб’єктів, спрямованої на досягнення спільної мети.

Примітно, що ні Закон України «Про інформацію», ні Закон України «Про захист інформації в інформаційно-комунікаційних системах» не містять вказівки на те, що суб’єкти захисту інформації мають взаємодіяти між собою. Водночас профільне законодавство у сфері діяльності Державної служби спеціального зв’язку та захисту інформації України чітко визначає, що:

«Державна служба спеціального зв'язку та захисту інформації України виконує покладені на неї завдання у взаємодії з центральними органами виконавчої влади, іншими державними органами, органами місцевого самоврядування, військовими формуваннями, утвореними відповідно до законів України, правоохоронними органами, підприємствами, установами та організаціями. Державні органи та органи місцевого самоврядування, їх посадові та службові особи в межах своїх повноважень сприяють діяльності Державної служби спеціального зв'язку та захисту інформації України у виконанні покладених на неї завдань» [129].

Відповідно, взаємодія за цього контексту постає як обов'язкова умова належного виконання покладених на суб'єктів владних повноважень функцій у сфері захисту інформації, що знаходить своє закріплення у спеціальному законодавстві, передбачаючи як партнерський тип її здійснення, так і ієрархічний (субординаційний) характер взаємовідносин між відповідними суб'єктами, а також сприяння як особливу форму взаємодії, що має допоміжний, забезпечувальний характер і спрямована на створення належних умов для реалізації повноважень.

Однак можна виокремлювати й інші форми взаємодії, які пов'язані з рівнями її реалізації. Зокрема у науковій доктрині міститься думка, що першим рівнем взаємодії є співіснування, яке відбувається коли принаймні два актори присутні в спільному середовищі. Взаємодія, що відбувається на цьому рівні, здійснюється з метою сприяння взаєморозумінню між сторонами. Другий рівень взаємодії – комунікації. На цьому рівні актори використовують активні чи пасивні заходи для передачі інформації іншим у спільному середовищі [226]. Тобто, на рівні співіснування сторони лише знаходять спільну мову і припускають, що в майбутньому вони можуть взаємодіяти, а вже на другому етапі вони створюють різні види інформативного матеріалу про себе, свої цілі та плани, щоб знайти точки дотику в можливості досягнення спільних цілей. Після комунікації йде рівень координації, яка відбувається коли учасники спільного середовища

взаємодіють, намагаючись організувати свою діяльність на основі певних критеріїв (наприклад, часу, розміру або вартості). Цей рівень переходить у наступний – кооперацію. А власне кооперація має місце, коли робота чи дія виконуються спільно з іншими учасниками. Найвищою метою взаємодії на цьому рівні є підвищення спроможності учасників досягати своїх індивідуальних цілей шляхом використання навичок, ресурсів або знань інших учасників [226]. Після означеного відбувається активна співпраця, де учасники взаємодії спільно працюють над досягненням визначених цілей, інтегруючи свої ресурси, знання та навички для забезпечення найбільш ефективного результату [9].

Тому не дивно, що деякі науковці вважають більш доцільним використовувати категорію «співробітництво» як таку, що забезпечує внутрішній (особистісний), когнітивний, мотиваційний, рефлексивний та професійний вияв (самовираження) сторін, що спільно діють [93, с. 73]. Проте, на нашу думку, у контексті порушених питань категорія «співробітництво» не повною мірою відображає специфіку порушених питань через наявність сприяння як допоміжної форми взаємодії, де одним суб'єктом виконуються ключові функції, тоді як інші забезпечують їх належне функціонування шляхом організаційної, інформаційної чи технічної підтримки.

Наочно вид взаємодії демонструє суб'єкт прийняття акту врегулювання порядку її здійснення (за умови відсутності відповідної норми законодавства). Приміром, у контексті партнерської взаємодії Державної служби спеціального зв'язку та захисту інформації України з іншим суб'єктом публічного права видається спільний нормативно-правовий акт. Щодо цього актуальним є приклад необхідності забезпечення оперативного проходження інформації між Державною службою спеціального зв'язку та захисту інформації України та Державною службою України з надзвичайних ситуацій України про загрозу або факт виникнення надзвичайної ситуації державного рівня. Відповідна інструкція передбачає, що така взаємодія

передбачає: 1) інформування про загрозу або факт виникнення надзвичайних ситуацій державного рівня; 2) уточнення стану довкілля на території, що зазнала впливу надзвичайних ситуацій, з метою вжиття заходів з безпеки особового складу Держспецзв'язку, що виконуватиме завдання з організації урядового зв'язку; 3) з'ясування інформації щодо утворення Урядової комісії, місця та початку її роботи, стану під'їзних шляхів та місця можливого розгортання рухомих засобів урядового зв'язку [137].

Водночас у випадках ієрархічної (субординаційної) взаємодії ініціатором врегулювання порядку її здійснення виступає уповноважений суб'єкт публічного права. Наприклад, положеннями постанови Кабінету Міністрів України від 29 березня 2006 року № 373, якою затверджено мінімальні вимоги до захисту інформаційних, електронних комунікаційних, інформаційно-комунікаційних та технологічних систем визначено, що органи державної влади, підприємства, установи та організації зобов'язані забезпечувати захист інформації у своїх системах. При цьому вони діють під методичним керівництвом та контролем Державної служби спеціального зв'язку та захисту інформації України [140].

Приміром, відповідний наказ Адміністрації Державної служби спеціального зв'язку та захисту інформації України щодо реагування суб'єктами забезпечення кібербезпеки на різні види подій у кіберспросторі містить такі рекомендації: необхідний перелік заходів із кіберзахисту, яких можуть вживати суб'єкти забезпечення кібербезпеки послідовно за етапами реагування на кіберінциденти / кібератаки; мету та цілі виконання заходів; механізм застосування критеріїв, за якими визначається категорія (рівень) критичності кіберінциденту / кібератаки; принципи пріоритезації кіберінцидентів / кібератак; типовий перелік заходів із реагування на кіберінциденти / кібератаки для одночасного відстеження заходів до їх завершення тощо. Окрім того, Рекомендаціями затверджені Загальні правила обміну інформацією про кіберінциденти (Протокол TLP) версії 2.0, схвалені

Національним координаційним центром кібербезпеки при РНБО, а також – Перелік категорій і типів кіберінцидентів [39].

Своєю чергою в контексті необхідності залучення організаційної, інформаційної чи технічної підтримки підписуються меморандуми або імперативно залучаються відповідальні суб'єкти. Наприклад, 12 вересня 2019 року було підписано Меморандум про взаємодію та співробітництво у сфері кібербезпеки та кіберзахисту між Міжнародною фундацією виборчих систем (IFES)/IFES Україна та Державним центром кіберзахисту Державної служби спеціального зв'язку та захисту інформації України. Угода передбачає тісну співпрацю у сферах електронних комунікацій, IT-технологій, безпеки інформації, кібербезпеки, кіберзахисту та організаційно-технічну підтримку рішень для кібербезпеки, кіберзахисту та управління інформаційною безпекою IT-систем, задіяних у виборчих процесах в Україні та інших країнах світу, що сприятиме підвищенню загального рівня кіберзахисту державних інформаційних ресурсів та критичної інфраструктури. Крім того, Сторони Меморандуму домовились про обмін інформацією та проведення консультацій найближчим часом з метою формування плану спільних заходів [140].

У продовження питання про співробітництво, на нашу думку, варто уточнити, що у сфері захисту інформації воно не може розглядатися виключно як добровільна форма взаємодії суб'єктів, адже для його характерним є й імперативний компонент. У цій сфері воно набуває ознак функціонально обумовленого інструменту публічного адміністрування, який спрямований не лише на підвищення ефективності діяльності окремих суб'єктів, а й на мінімізацію ризиків, пов'язаних із фрагментарністю системи захисту інформації.

Це надзвичайно важливо, адже як демонструє практика, виникають ризики зловживань, пов'язаних із використанням інформаційних систем, що, своєю чергою, може нівелювати позитивний ефект від налагодженої взаємодії та створювати додаткові загрози інформаційній безпеці держави.

Зокрема подекуди відсутність належного і ефективного державного контролю за станом упровадження та функціонування державних електронних інформаційних ресурсів призводить до створення корупційних механізмів використання електронних інформаційних систем та програмного забезпечення. Такі системи і програмне забезпечення належать їх розробникам (комерційним структурам) на правах об'єктів інтелектуальної власності, за їх використання органи державної влади сплачують за рахунок бюджетних коштів. У тих випадках, коли майнові права на програмне забезпечення не передаються у державну власність з вихідним кодом, створюються передумови й для несанкціонованого втручання в роботу відповідних інформаційних систем та порушення цілісності інформації, наприклад для здійснення успішних кібератак. Зокрема, органи СБУ виявили протиправну діяльність службових осіб Державного центру кіберзахисту Державної служби спеціального зв'язку та захисту інформації України та посадових осіб суб'єктів підприємницької діяльності, причетних до розтрати бюджетних коштів під час здійснення публічних закупівель [115, с. 120].

Власне службовими особами Державного центру кіберзахисту Держспецзв'язку та іншими посадовими особами суб'єктів підприємницької діяльності за підтримки представників Cisco в Україні та керівництва Ради національної безпеки і оборони України організовано протиправну схему по розтраті бюджетних коштів в особливо великих розмірах. Протягом 2017–2019 років службовими особами Державного центру кіберзахисту Держспецзв'язку проведено низку конкурсних закупівель за результатами, яких підписано договори з ДП «Державний центр інформаційної безпеки», ТОВ «Спеціальні телекомунікаційні рішення», ТОВ «Інформаційні технології та інформаційна безпека», ТОВ «Айті-Со- 121 люшнс», ТОВ «Есай Біс», ТОВ Фірма «ВалТек», ТОВ «Ньютест Україна», ТОВ «Грін Нетворкс», ТОВ «Ай Ай Ті Трейдінг». 30.10.2017 року ДЦКЗ Держспецзв'язку укладено договір з Державним підприємством «Державний центр інформаційної безпеки» на закупівлю «спеціального програмного забезпечення терміналу мобільного

зв’язку для шифрованого обміну даними, що циркулюють в межах мобільного зв’язку та має бути реалізовано у вигляді додатку…» в кількості 1 шт. загальною вартістю 1,1 млн. грн. Посадові особи ДП «ДЦІБ» того ж дня, 30.10.2017 року за результатами проведення конкурсної закупівлі № UA-2017-11-07-000231-c уклали Договір № ДП30/10 з підприємством ПП «Альфа Ком» на закупівлю спеціального програмного забезпечення терміналу мобільного зв’язку вартістю 1 142 729,59 грн. В ході досудового розслідування, з’ясовано, що директор вищевказаного СПД не має відношення до фінансово-господарської діяльності підприємства, а фактично керують діяльністю ПП «Альфа Ком» службові особи Державного центру кіберзахисту Держспецзв’язку. Зобов’язань ПП «Альфа Ком» перед ДП «ДЦІБ» не виконало, спеціальне програмне забезпечення не поставлено, при цьому акти виконаних робіт між Державного центру кіберзахисту Держспецзв’язку та ДП «ДЦІБ» підписано. За результатом виконання зазначеного договору, посадові особи Державного центру кіберзахисту Держспецзв’язку у змові з посадовими особами ДП «ДЦІБ» безпідставно перерахували, а у подальшому привласнили 1,1 млн. грн. бюджетних коштів [185].

Наведений приклад наочно демонструє, що відсутність належно вибудуваної системи взаємодії між суб’єктами публічної адміністрації, а також недостатня прозорість і контрольованість процесів співробітництва з приватним сектором можуть призводити не лише до неефективного використання бюджетних коштів, але й до формування системних загроз інформаційній безпеці держави.

Окремо зауважимо, що Кабінет Міністрів України ухвалив постанову від 13 листопада 2025 року № 1471, якою затвердив Порядок, що регламентує механізм взаємодії суб’єктів національної системи реагування на кіберінциденти, кібератаки, кіберзагрози із суб’єктами забезпечення кібербезпеки, правоохоронними, контррозвідувальними, розвідувальними органами та суб’єктами оперативно-розшукової діяльності (силові

структури). Документ, ухвалений відповідно до Закону України «Про основні засади забезпечення кібербезпеки України», встановлює чіткі правила співпраці для ефективного реагування на кіберінциденти, кібератаки, кіберзагрози. Зокрема, Порядок визначає механізми взаємодії: Національної команди реагування на кіберінциденти, кібератаки, кіберзагрози (CERT-UA) із силовими структурами; галузевих та регіональних команд реагування на кіберінциденти, кібератаки, кіберзагрози (CSIRT) із силовими структурами та іншими суб'єктами національної системи реагування; Національної поліції та СБУ з іншими суб'єктами національної системи реагування. Затвердження цього Порядку створює єдині «правила гри», що дозволить значно прискорити обмін інформацією, підвищити рівень скоординованості дій та ефективності реагування на кіберінциденти, кібератаки та кіберзагрози та підвищити стійкість інформаційно-комунікаційних систем держави. Для громадян це означатиме посилений захист персональних даних та державних сервісів, зменшення ризиків від кібератак і загальне підвищення рівня кібербезпеки в Україні [184].

З усім тим маємо вказати, що співробітництво у сфері захисту інформації не зводиться лиш до внутрішньодержавного контексту, адже багато проблем, пов'язаних із забезпеченням інформаційної безпеки, можуть бути успішно розв'язані лише в тісній скоординованій співпраці з міжнародними партнерами, зокрема такою потужною і впливовою міжнародною організацією як НАТО [28].

Співробітництво між НАТО та країнами-партнерами в рамках Ради євроатлантичного партнерства (РЄАП) та Програми «Партнерство заради миру» (ПЗМ) передбачає певні зобов'язання сторін щодо обміну та захисту інформації. Участь країн в оборонному плануванні і військових навчаннях НАТО в рамках програми ПЗМ надає доступ до деяких технічних даних НАТО щодо сумісності. Приєднання країни до програми ПЗМ передбачало ратифікацію «Угоди про безпеку між НАТО та країнами, які беруть участь у РЄАП та/або програмі ПЗМ». Згідно цієї Угоди, сторони погоджувалися

консультуватися щодо політичних питань і питань безпеки, розширювати й інтенсифікувати політичне і військове співробітництво в Європі, усвідомлюючи, що ефективність співробітництва в цих сферах має на увазі обмін «таємною» інформацією і/або інформацією обмеженого доступу серед учасників. Відповідальним органом при захисті таємної інформації став Державний комітет зв'язку та інформатизації України. У 2010 р. цей орган було перетворено на Державний комітет України з питань науки, інновацій та інформатизації, який у 2014 році було реорганізовано та на його базі створено Державне агентство з питань науки, інновацій та інформації України [28].

Сьогодні основоположними документами, що визначають відносини між Україною та НАТО є Хартія про особливе партнерство між Україною та Організацією Північноатлантичного договору та Декларація про доповнення Хартії про особливе партнерство [28].

Зокрема враховуючи важливість інформаційної діяльності для покращення обопільної обізнаності та розуміння, НАТО заснувала Центр інформації та документації в Україні. Українська сторона має забезпечувати повну підтримку діяльності Центру у відповідності з Меморандумом про взаєморозуміння між урядом України та НАТО, підписаним у Києві 7 травня 1997 році [188].

Також, між НАТО та країною-партнером укладається окрема адміністративна угода по стандартах взаємного забезпечення безпеки інформації, якою обмінюються сторони і призначається офіцер зв'язку між Управлінням безпеки НАТО і національним уповноваженим органом по безпеці інформації [28], тобто Державною службою спеціального зв'язку та захисту інформації України.

У межах Комплексного пакету допомоги також існує Платформа Україна – НАТО з протидії гібридній війні, яка є одним з ключових механізмів протидії гібридним загрозам, зокрема інформаційним і кібернетичним атакам. Платформа була заснована в 2016 році з метою виявлення та аналізу гібридних загроз, посилення національної стійкості, а

також впровадження заходів щодо їхньої нейтралізації [233]. Ця ініціатива передбачає обмін досвідом між Україною та країнами-членами Альянсу, дослідження нових методів інформаційної боротьби та координацію заходів у сфері кіберзахисту, стратегічних комунікацій і безпеки критичної інфраструктури. В межах Платформи реалізовано низку ініціатив, серед яких особливу увагу приділено впровадженню стратегічних комунікацій, розбудові системи раннього виявлення інформаційних загроз та зміцненню національних можливостей у сфері кібербезпеки. Також Платформа відіграє важливу роль у розробці протоколів швидкого реагування на інформаційні атаки, які можуть впливати на політичну та соціальну стабільність країни. Крім того, значні зусилля спрямовані на аналіз російських дезінформаційних кампаній, які поширюються через соціальні мережі та проросійські медіа, що дозволяє краще прогнозувати та нейтралізувати загрози інформаційного характеру [190]. В умовах повномасштабної агресії Росії діяльність Платформи активізувалася, зокрема через регулярні консультації, навчання та спільні ініціативи. Так, у листопаді 2023 року в Кишиневі відбулася зустріч представників України, НАТО та ЄС, присвячена аналізу новітніх гібридних загроз та розширенню міжвідомчої співпраці. Особливу увагу приділили стратегічним комунікаціям, протидії дезінформації, енергетичній безпеці та захисту критичної інфраструктури. Співпраця в межах Платформи сприяє розбудові стійких механізмів запобігання та реагування на інформаційні атаки, що є важливим елементом євроатлантичної інтеграції України та зміцнення її безпекової системи [164; 186].

Таким чином, узагальнюючи, можна стверджувати, що міжнародне співробітництво у сфері захисту інформації: є об’єктивно необхідним елементом сучасної системи інформаційної безпеки; реалізується через інституціоналізовані механізми та міжнародні програми; базується на обміні чутливою інформацією, що потребує високих стандартів її захисту.

Разом з тим сьогодні активно обговорюється думка, що особливо актуальними досі залишаються питання організації ефективної взаємодії між

підрозділами Служби безпеки України і Державної служби спеціального зв'язку та захисту інформації України. Нормативним підґрунтям для налагодження такої взаємодії має стати стаття 6 Положення про Адміністрацію, відповідно до якої, нагадаємо, Адміністрація Держспецзв'язку під час виконання покладених на неї завдань взаємодіє з іншими центральними та місцевими органами виконавчої влади, органами місцевого самоврядування, військовими формуваннями, підприємствами, установами і організаціями незалежно від форми власності, а також з відповідними органами іноземних держав [35].

Як відзначають науковці, взаємодія Держспецзв'язку та Служби безпеки України у сфері охорони державної таємниці та технічного захисту інформації зумовлюється низкою обставин: 1) спільністю завдань, які постають перед зазначеними органами у сфері протидії загрозам інформації обмеженого доступу (зокрема, державної таємниці); 2) різним обсягом їх повноважень щодо забезпечення безпеки інформації; 3) особливістю призначення сил і засобів, що застосовуються для вирішення відповідних завдань; 4) різними методами діяльності; 5) взаємозалежністю кінцевих результатів спільної діяльності [35].

Така спільна діяльність може бути короткочасною або тривалою. Короткочасна пов'язана з виконанням конкретного поточного завдання захисту інформації, тривала – із систематичним, спільно запланованим, узгодженим використанням сил і засобів досліджуваних державних органів [35].

Як підсумок дослідження варто вказати, що відсутність прямої вказівки на необхідність організації та здійснення взаємодії органів публічної адміністрації з іншими суб'єктами у сфері захисту інформації у загальному законодавстві не виключає її фактичного існування та практичної реалізації, оскільки така взаємодія випливає із системного тлумачення норм права, що регламентують повноваження різних суб'єктів у сфері інформаційної безпеки.

При цьому провідною особливістю взаємодії органів публічної адміністрації з іншими суб’єктами у сфері захисту інформації є її характер сприяння, який має подвійний юридичний зміст. Йдеться про те, що з одного боку, Державна служба спеціального зв’язку та захисту інформації України як провідний суб’єкт досліджуваної системи, сприяє іншим публічним суб’єктам у реалізації їхніх функцій. З іншого боку, інші суб’єкти публічного права надають сприяння Державній службі спеціального зв’язку та захисту інформації України, забезпечуючи належне виконання покладених на неї завдань через організаційну, інформаційну або технічну підтримку.

Означене свідчить про те, що сприяння у даному контексті не є пасивною дією, а виступає активним процесом, який включає узгодження процедур, надання необхідних ресурсів, координацію дій та обмін інформацією між усіма уповноваженими, залученими та зацікавленими суб’єктами.

Висновки до Розділу 2

1. Зауважено, що узагальнення наукових підходів до розуміння категорії «правовий статус» створює теоретико-методологічну основу для з’ясування специфіки його галузевої модифікації – адміністративно-правового статусу. Визначено, що категорія «правовий статус»: а) у контексті фізичних осіб окреслює їх законодавчо встановлені права та обов’язки; б) у контексті юридичних осіб публічного права характеризує їх роль і призначення в механізмі реалізації функцій держави як сукупність нормативних, інформаційно-аналітичних, реалізаційних, оптимізаційних, експертних, погоджувальних, організаційних, контрольно-наглядових, адміністративних та інших активних управлінських дій. Тобто кожен такий суб’єкт, діючи від імені та в інтересах держави, є носієм владних повноважень, виконує

визначені завдання та має власні функції, належне виконання яких забезпечується обов'язком нести юридичну відповідальність.

2. З'ясовано, що категорійно-понятєва визначеність правового концепту «адміністративно-правовий статус органів публічної адміністрації» у вітчизняній науковій думці сформована через подвійний інтерпретаційний підхід: а) через зміст як репрезентації елементів внутрішньої структури його складу, що ідентифікує суб'єкта у межах потенційно та фактично існуючих адміністративних правовідносин; б) через сутність, яка окреслює місце і роль органів публічної адміністрації в механізмі виконання адміністративних функцій держави.

3. Запропоновано під адміністративно-правовим статусом органів публічної адміністрації у сфері захисту інформації розуміти сукупність нормативно визначених універсальних характеристик, які детермінують правове положення цих органів як суб'єктів публічної адміністрації в колі адміністративно-правових взаємозв'язків, пов'язаних із реалізацією ними повноважень під час забезпечення інформаційної безпеки та здійснення адміністративно-правового захисту прав громадян, юридичних осіб і держави в інформаційній сфері.

4. Схарактеризовано зміст та сутність адміністративно-правового статусу окремих органів публічної адміністрації у сфері захисту інформації за функціональним критерієм. Зокрема стверджується, що :

– адміністративно-правовий статус Держспецзв'язку характеризується чітко визначеною законодавством правосуб'єктністю, спеціальною компетенцією та функціональною спрямованістю діяльності. При цьому специфіка адміністративно-правового статусу цього суб'єкта полягає у його подвійному інституційному призначенні: з одного боку, як центрального органу виконавчої влади зі спеціальним статусом, що формує та реалізує державну політику у сфері захисту інформації, а з іншого – як суб'єкта сектору безпеки і оборони, що забезпечує практичну реалізацію заходів кіберзахисту та технічного захисту інформації. Відповідно, він має

спеціалізований, техніко-безпековий характер, що проявляється безпосереднім забезпеченням захисту інформації, зокрема державних інформаційних ресурсів, а також реалізацією заходів кіберзахисту, криптографічного і технічного захисту інформації та функціонуванням захищених урядових комунікацій;

– адміністративно-правовий статус РНБО у досліджуваній сфері є загальним, має стратегічний характер та проявляється координаційною діяльністю щодо усіх суб'єктів у цій сфері Основною метою її діяльності є забезпечення узгодженості дій усіх суб'єктів сектору безпеки і оборони, а також вироблення стратегічних рішень щодо протидії інформаційним загрозам, зокрема дезінформації та кіберзагрозам;

– адміністративно-правовий статус Кабінету Міністрів України у сфері захисту інформації характеризується як універсально-управлінський, який проявляється у здійсненні ним нормотворчої, організаційно-розпорядчої, координаційної та контрольної функцій щодо діяльності інших органів публічної адміністрації у цій сфері;

– адміністративно-правовий статус Міністерства цифрової трансформації України у сфері захисту інформації має політико-формувальний та інноваційно-орієнтований характер, що обумовлено його роллю як головного органу у формуванні та реалізації державної політики у сферах цифровізації та розвитку інформаційного суспільства. Основною метою його діяльності є створення умов для безпечного функціонування цифрового середовища, розвитку електронних послуг та забезпечення захисту інформаційних ресурсів у процесі цифрової трансформації держави;

– адміністративно-правовий статус СБУ у сфері захисту інформації є спеціальним правоохоронно-безпековим, що поєднує адміністративно-правові, оперативно-розшукові та контррозвідувальні інструменти. Основною метою її діяльності є виявлення, запобігання та нейтралізація загроз інформаційній безпеці держави, у тому числі у кіберпросторі, а також захист державної таємниці.

5. Узагальнено, що адміністративно-правовий статус органів публічної адміністрації у сфері захисту інформації характеризується функціональною диференціацією, що проявляється у розмежуванні їх основних цілей діяльності: від стратегічного планування та координації до безпосередньої реалізації заходів захисту та протидії загрозам, тобто кожен суб’єкт виконує специфічну роль, спрямовану на досягнення спільної мети – гарантування інформаційної безпеки держави, суспільства та особи.

6. Визначено, що повноваження органів публічної адміністрації у сфері захисту інформації відображають міру та спосіб публічно-владного впливу органів публічної адміністрації на суспільні відносини у сфері захисту інформації. Вони виступають тією юридичною формою, через яку функціональна диференціація цих органів набуває свого практичного вияву – від нормотворчої та координаційної діяльності до реалізації контрольно-наглядових, правоохоронних та спеціальних заходів інформаційної безпеки.

7. Результати аналізу положень статті 10 Закону України «Про захист інформації в інформаційно-комунікаційних системах» є такими:

– по-перше, повноваження органів публічної адміністрації у сфері захисту інформації мають чітко виражену ієрархічну структуру, в межах якої Кабінет Міністрів України виконує нормотворчу та системоутворюючу функцію, визначаючи мінімальні вимоги до захисту інформації (базовий профіль безпеки), тоді як інші суб’єкти конкретизують ці вимоги на галузевому та інституційному рівнях;

– по-друге, простежується функціональна диференціація повноважень між органами: Державна служба спеціального зв'язку та захисту інформації України наділена спеціалізованими повноваженнями у сфері формування та реалізації політики, нормативного регулювання, контролю, експертизи та методичного забезпечення, що підтверджує її ключову роль як центрального органу технічного та криптографічного захисту інформації;

– по-третє, уповноважені органи вправі не тільки встановлювати вимоги, а й забезпечувати їх реалізацію через процедури експертизи,

авторизації, моніторингу та надання рекомендацій;

– по-четверте, повноваження органів публічної адміністрації у досліджуваній сфері реалізуються через механізм профілювання безпеки (базові, галузеві та цільові профілі), що дозволяє адаптувати загальні вимоги до конкретних умов функціонування інформаційних систем, рівня ризиків та специфіки відповідної сфери;

– по-п’яте, закріплено секторальний підхід до регулювання, відповідно до якого окремі органи, зокрема Національний банк України, Міністерство оборони України та Служба безпеки України, наділяються спеціальними повноваженнями щодо визначення вимог до захисту інформації з урахуванням специфіки відповідних сфер (фінансової, оборонної, правоохоронної);

– по-шосте, характерною є декомпозиція відповідальності між суб’єктами, за якої органи державної влади та місцевого самоврядування не лише виконують встановлені вимоги, а й самостійно розробляють цільові профілі безпеки для підпорядкованих систем, що свідчить про їх залучення до безпосередньої реалізації заходів захисту інформації.

8. Зауважено, що повноваження органів публічної адміністрації у сфері захисту інформації не мають виключно відокремленого характеру, а значною мірою перетинаються та взаємодоповнюють одне одного. Зокрема, окремі функції, пов’язані з формуванням вимог до захисту інформації, їх конкретизацією, впровадженням та контролем за дотриманням, реалізуються різними суб’єктами паралельно або у взаємодії, що зумовлює наявність спільних зон компетенції.

9. Проаналізовано судове рішення № 125202700 від 17 лютого 2025 року Київського окружного адміністративного суду з точки зору реалізації повноважень суб’єктів у сфері захисту інформації. Виявлено, що аналізоване рішення суду демонструє таку модель розподілу повноважень основних суб’єктів у сфері захисту інформації: а) Держспецзв’язку – ключовий суб’єкт, який формує відповідну політику, здійснює контрольні функції, а також

загалом координує систему технічного захисту інформації; б) СБУ – допоміжний (спеціальний) суб'єкт, адже залучається до перевірок та забезпечує безпековий компонент; в) власники/адміністратори систем (як ДП «НАІС») – несуть основну відповідальність за захист інформації, є об'єктами контролю.

10. Обґрунтовано, що публічне адміністрування у сфері захисту інформації реалізується через: контрольні повноваження держави, які мають превентивний характер; обов'язок підконтрольних суб'єктів забезпечувати належний рівень захисту; координацію між різними органами публічної адміністрації.

11. Окремо проаналізовано повноваження органів стратегічного управління, які мають переважно координаційний, аналітичний та стратегічний характер. Визначено, що їх компетенція концентрується навколо таких функціональних напрямів, як збір та узагальнення інформації, аналітичне опрацювання даних, ініціювання контрольних та дослідницьких заходів, формування експертного середовища, а також налагодження міжвідомчої та міжнародної співпраці, що свідчить про значну обмеженість кола їхніх повноважень у досліджуваній сфері.

12. Доведено, що повноваження органів публічної адміністрації у сфері захисту інформації зводяться до нормотворчих, контрольних, координаційних, аналітичних та спеціальних. Зауважено, що ключовими з таких є саме останні, адже забезпечують формування та реалізацію державної політики, нормативне регулювання і державний контроль у сфері технічного та криптографічного захисту інформації. Водночас інші суб'єкти, зокрема СБУ, галузеві та інші органи, виконують спеціалізовані або допоміжні функції, що забезпечують практичну реалізацію вимог інформаційної безпеки.

13. З'ясовано, що юридична природа категорії «взаємодія» репрезентується через процес узгодженої діяльності суб'єктів, спрямованої на досягнення спільної мети.

14. Доведено, що у сфері захисту інформації взаємодія постає як обов'язкова умова належного виконання покладених на суб'єктів владних повноважень функцій у цій сфері, що знаходить своє закріплення у спеціальному законодавстві, передбачаючи як партнерський тип її здійснення, так і ієрархічний (субординаційний) характер взаємовідносин між відповідними суб'єктами, а також сприяння як особливу форму взаємодії, що має допоміжний, забезпечувальний характер і спрямована на створення належних умов для реалізації повноважень. Однак уточнено, що можна виокремлювати й інші форми взаємодії, які пов'язані з рівнями її реалізації.

15. Визначено, що відсутність прямої вказівки на необхідність організації та здійснення взаємодії органів публічної адміністрації з іншими суб'єктами у сфері захисту інформації у загальному законодавстві не виключає її фактичного існування та практичної реалізації, оскільки така взаємодія випливає із системного тлумачення норм права, що регламентують повноваження різних суб'єктів у сфері інформаційної безпеки.

16. Стверджується, що наочно вид взаємодії демонструє суб'єкт прийняття акту врегулювання порядку її здійснення (за умови відсутності відповідної норми законодавства). Приміром, у контексті партнерської взаємодії Державної служби спеціального зв'язку та захисту інформації України з іншим суб'єктом публічного права видається спільний нормативно-правовий акт. Водночас у випадках ієрархічної (субординаційної) взаємодії ініціатором врегулювання порядку її здійснення виступає уповноважений суб'єкт публічного права. А в контексті необхідності залучення організаційної, інформаційної чи технічної підтримки підписуються меморандуми або імперативно залучаються відповідальні суб'єкти.

17. Окремо визначається, що у сфері захисту інформації співробітництво не може розглядатися виключно як добровільна форма взаємодії суб'єктів, адже для його характерним є й імперативний компонент. У цій сфері воно набуває ознак функціонально обумовленого інструменту публічного адміністрування, який спрямований не лише на підвищення

ефективності діяльності окремих суб’єктів, а й на мінімізацію ризиків, пов’язаних із фрагментарністю системи захисту інформації. Це надзвичайно важливо, адже як демонструє практика, виникають ризики зловживань, пов’язаних із використанням інформаційних систем, що, своєю чергою, може нівелювати позитивний ефект від налагодженої взаємодії та створювати додаткові загрози інформаційній безпеці держави.

18. З’ясовано, що міжнародне співробітництво у сфері захисту інформації: є об’єктивно необхідним елементом сучасної системи інформаційної безпеки; реалізується через інституціоналізовані механізми та міжнародні програми; базується на обміні чутливою інформацією, що потребує високих стандартів її захисту.

19. Констатується, що провідною особливістю взаємодії органів публічної адміністрації з іншими суб’єктами у сфері захисту інформації є її характер сприяння, який має подвійний юридичний зміст. Йдеться про те, що з одного боку, Державна служба спеціального зв’язку та захисту інформації України як провідний суб’єкт досліджуваної системи, сприяє іншим публічним суб’єктам у реалізації їхніх функцій. З іншого боку, інші суб’єкти публічного права надають сприяння Державній службі спеціального зв’язку та захисту інформації України, забезпечуючи належне виконання покладених на неї завдань через організаційну, інформаційну або технічну підтримку. Означене свідчить про те, що сприяння у даному контексті не є пасивною дією, а виступає активним процесом, який включає узгодження процедур, надання необхідних ресурсів, координацію дій та обмін інформацією між усіма уповноваженими, залученими та зацікавленими суб’єктами.

РОЗДІЛ 3
ШЛЯХИ УДОСКОНАЛЕННЯ ДІЯЛЬНОСТІ ОРГАНІВ ПУБЛІЧНОЇ АДМІНІСТРАЦІЇ У СФЕРІ ЗАХИСТУ ІНФОРМАЦІЇ

3.1. Зарубіжний досвід адміністративно-правового захисту інформації

Основне завдання сучасного міжнародного права полягає у розробці та погодженні універсальних модальностей державної політики, які стосуються захисту прав і свобод людини, а також забезпечення міжнародного миру, безпеки та правопорядку. Для збереження фундаментальних загальнолюдських цінностей на глобальному рівні, включаючи діяльність Організації Об'єднаних Націй (ООН), і в рамках регіонального співробітництва, міжнародне співтовариство постійно координує зусилля держав для вирішення як глобальних, так і регіональних проблем, а також для запобігання можливим загрозам, що виникають на національному та міжнародному рівнях. Нагадаємо, однією з таких проблем є загроза інформаційній безпеці суверенних держав, коли їхній національний інформаційний простір стає об'єктом ворожих дій з боку інших країн чи суб'єктів, які ті контролюють. У таких випадках держави на національному рівні здійснюють заходи з публічного управління у сфері забезпечення інформаційної безпеки. З огляду на те, що міжнародне право намагається адаптуватися до стрімкого розвитку суспільства та інформаційних технологій, на рівні актів ООН поступово сформувалися універсальні принципи розробки, планування та реалізації державної політики у сфері інформаційної безпеки [162].

Разом з тим, світовий досвід свідчить про різноманітність підходів до формування системи адміністративно-правового захисту інформації, що зумовлено особливостями правових систем, рівнем технологічного розвитку

та пріоритетами державної політики конкретної країни. Однак є певна спільність, – у провідних країнах світу сформовано комплексні моделі, які поєднують нормативне регулювання, інституційну спроможність уповноважених органів та сучасні інструменти кібербезпеки.

Вбачаємо, що аналіз таких моделей дозволяє виявити ефективні практики, що можуть бути актуальними для впровадження в Україні.

У цьому контексті особливої уваги заслуговує досвід Сполучених Штатів Америки як одного з провідних світових центрів розвитку інформаційних технологій і кібербезпеки. Адміністративно-правова система захисту інформації в цій державі вирізняється високим рівнем інституційного розвитку, чітким розподілом повноважень між органами публічної влади, а також активною участю приватного сектору у забезпеченні інформаційної безпеки. Водночас нормативно-правове регулювання охоплює широкий спектр питань – від захисту персональних даних до протидії кіберзлочинності та забезпечення критичної інфраструктури.

З огляду на це, доцільним є детальний аналіз адміністративно-правових засад захисту інформації у США з метою виявлення ключових принципів, механізмів та інструментів, що можуть бути використані для вдосконалення національної системи інформаційної безпеки України.

Зауважимо, що протягом останнього десятиліття федеральний уряд США, штати та місцеві муніципалітети видали десятки законів, постанов, статутів та інших інструкцій щодо захисту даних та конфіденційності.

Ключове значення має Закон про управління федеральною інформаційною безпекою (FISMA) [219], який встановлює вимоги до захисту інформаційних систем федеральних органів, включаючи обов’язковість оцінки ризиків, впровадження заходів безпеки та регулярного аудиту. Закон став частиною реформи управління IT-інфраструктурою уряду США. Його головна мета – підвищити рівень безпеки інформаційних систем, які обробляють, зберігають або передають федеральну інформацію. FISMA

вимагає створення інтегрованої програми управління ризиками та звітування перед Конгресом.

Крім зазначеного, Закон про модернізацію федеральної інформаційної безпеки 2014 року (FISMA 2014) оновлює практику кібербезпеки федерального уряду шляхом: 1) кодифікації повноважень Міністерства внутрішньої безпеки (DHS) щодо управління впровадженням політик інформаційної безпеки для федеральних систем виконавчої гілки влади, що не стосуються національної безпеки, включаючи надання технічної допомоги та розгортання технологій у таких системах; 2) внесення змін та уточнення повноважень Адміністративно-бюджетного управління щодо нагляду за практикою інформаційної безпеки федеральних агентств; а також шляхом 3) вимоги «усунення неефективної та марнотратної звітності» [219].

Важливим є також Закон про конфіденційність (1974) [244], який регламентує обробку персональних даних федеральними органами, визначає права громадян щодо доступу до інформації про себе та обмежує її розповсюдження. Прийнятий після скандалів Вотергейт та Програма контррозвідки (COINTELPRO), пов'язаних із незаконним стеженням за опозиційними політичними партіями та особами, яких вважали «підривними», Закон про конфіденційність мав на меті відновити довіру до уряду та вирішити проблему, яка на той час вважалася екзистенційною загрозою американській демократії. За словами головного автора законопроекту, голови Судової ради, сенатора Сема Ервіна, «[якщо] ми чогось і навчилися за цей останній рік Вотергейту, то це того, що повинні бути обмеження щодо того, що уряд може знати про кожного зі своїх громадян» [234].

Закон про конфіденційність 1974 року з поправками, 5 USC § 552a, встановлює кодекс добросовісної інформаційної практики, який регулює збір, зберігання, використання та поширення інформації про осіб, що зберігається в системах записів федеральними агентствами. Система записів – це група записів, що знаходяться під контролем агентства, з яких інформація

отримується за іменем особи або за певним ідентифікатором, призначеним цій особі. Закон про конфіденційність вимагає, щоб установи публікували інформацію про свої системи обліку шляхом публікації у Федеральному реєстрі. Закон про конфіденційність забороняє розкриття запису про особу із системи обліку без письмової згоди особи, окрім випадків, коли розкриття здійснюється відповідно до одного з дванадцяти встановлених законом винятків. Закон також надає особам засоби для отримання доступу до своїх записів та внесення змін до них й встановлює різні вимоги до ведення обліку установ [236].

Окрему роль відіграє Закон про обмін інформацією у сфері кібербезпеки (CISA) [237], федеральний закон США, ухвалений у 2015 році з метою посилення обміну інформацією про кіберзагрози між урядом і приватним сектором. Закон покликаний покращити кіберзахист країни, не порушуючи конфіденційність громадян.

Загалом CISA 2015 встановлює законодавчу базу для добровільного обміну індикаторами кіберзагроз та захисними заходами між приватними організаціями та федеральними урядовими установами. Закон передбачає певний захист відповідальності та інші правові гарантії для організацій, які обмінюються кваліфікованою інформацією про кібербезпеку відповідно до вимог закону, включаючи захист, пов'язаний з розкриттям інформації, привілеями та використанням у регуляторних цілях. Закон також надає певні дозволи та захист для участі в моніторингу кібербезпеки і впровадженні захисних заходів [235].

Хоча в США немає повноцінного регулятора захисту даних, повноваження Федеральної торгової комісії (FTC) дуже широкі та часто задають тон у питаннях федеральної конфіденційності та безпеки даних. Крім того, низка інших установ регулює захист даних за допомогою галузевих законів, включаючи Міністерство охорони здоров'я та соціальних служб (HHS), Федеральну комісію зі зв'язку (FCC), Комісію з цінних паперів та бірж (SEC), Бюро фінансового захисту споживачів (CFPB) тощо. На рівні

штатів CPRA створило першого спеціалізованого регулятора конфіденційності в США – Каліфорнійське агентство захисту конфіденційності (CPPA). Обов'язки CPPA включають забезпечення виконання CPRA разом з Генеральним прокурором Каліфорнії, нормотворчу діяльність відповідно до CPRA та підвищення обізнаності громадськості щодо питань конфіденційності. Інші штати продовжують уповноважити своїх Генеральних прокурорів проводити нормотворчу діяльність або вживати заходів щодо забезпечення виконання, пов'язаних з порушеннями їхнього відповідного законодавства про конфіденційність даних [206].

Координаційну роль у сфері кібербезпеки виконує Міністерство внутрішньої безпеки США [207], у структурі якого функціонує Агентство з кібербезпеки та безпеки інфраструктури (CISA) [202]. Це агентство відповідає за захист критичної інфраструктури, реагування на кіберінциденти та взаємодію з приватним сектором.

Важливі повноваження у сфері розслідування кіберзлочинів має Федеральне бюро розслідувань (FBI) [217], який здійснює оперативно-розшукову діяльність і кримінальні розслідування.

Регуляторні функції у сфері захисту персональних даних та споживачів виконує Федеральна торгова комісія (FTC) [224], яка має право застосовувати санкції до компаній за порушення конфіденційності даних.

Також важливу роль відіграє Національний інститут стандартів і технологій (NIST) [232], який розробляє стандарти та рекомендації у сфері інформаційної безпеки, зокрема широко відомий «NIST Cybersecurity Framework».

Окремо зауважимо, що ефективність американської моделі адміністративно-правового захисту інформації підтверджується низкою резонансних кейсів. Одним із найвідоміших є справа проти компанії Фейсбук у зв’язку зі Кембридж Аналітика скандалом [241]. Федеральна торгова комісія наклала штраф у розмірі 5 млрд доларів США за порушення зобов’язань щодо захисту персональних даних користувачів.

Кембридж Аналітика використала зовнішній додаток Фейсбук, щоб отримати інформацію від понад 87 мільйонів користувачів. Дані являли собою тест на особистість, у якому взяли участь приблизно 270 000 осіб, яким платили за проходження тесту. Тест під назвою «this is your digital life» також зібрав дані з профілів друзів користувачів, що дало компанії колосальний запас даних. Ці дані допомогли компанії створити психологічні профілі, оскільки вони змогли отримати знання, що включали персональні дані про те, де проживає людина, які сторінки їй подобаються тощо. Ці дані пізніше використовувалися в політичних кампаніях [241].

Іншим прикладом є кіберінцидент у компанії «Equifax» (2017 рік) [218], унаслідок якого було скомпрометовано персональні дані понад 140 млн осіб. У результаті компанія погодилася на багатомільйонні компенсації та посилення заходів безпеки.

Також варто відзначити атаку на компанію «Colonial Pipeline» у 2021 році [240], що призвела до перебоїв у постачанні пального. Цей випадок став поштовхом до посилення державної політики у сфері захисту критичної інфраструктури та розширення повноважень Агентства з кібербезпеки та безпеки інфраструктури.

Таким чином, досвід США демонструє ефективність комплексного підходу до адміністративно-правового захисту інформації, що включає: 1) спеціалізоване законодавство; 2) потужну інституційну систему з чітким розподілом повноважень; 3) активну взаємодію держави та бізнесу; 4) орієнтацію на ризик-менеджмент і превентивні заходи.

Для України важливим є запозичення таких елементів, як розбудова інституційної спроможності органів кібербезпеки, впровадження стандартів на кшталт «NIST», а також розвиток механізмів публічно-приватного партнерства у сфері захисту інформації.

Необхідно відмітити, що у США відсутній єдиний універсальний закон про захист персональних даних (на відміну від «GDPR» у ЄС), натомість діє

галузевий підхід із численними законами на федеральному та штатному рівнях (зокрема, Закон Каліфорнії про захист конфіденційності споживачів).

Уточнимо, що протягом останніх п'яти років майже половина штатів прийняли аналогічні комплексні закони про конфіденційність даних споживачів. Зокрема у 2020 році Каліфорнія внесла зміни до CCPA, прийнявши Закон Каліфорнії про права на конфіденційність (CPRA), який розширив права, надані споживачам, та посилив зобов'язання щодо дотримання вимог для бізнесу. У 2021 році Вірджинія прийняла Закон про захист даних споживачів (Virginia CDPA), ставши другим штатом із комплексним законом про конфіденційність даних, невдовзі після цього за нею пішов Колорадо, який прийняв Закон про конфіденційність Колорадо. Продовжуючи цю тенденцію, у 2022 році Юта прийняла Закон Юти про конфіденційність споживачів, а Коннектикут – Закон про конфіденційність персональних даних та онлайн-моніторинг (Закон про конфіденційність Коннектикуту). У 2023 році Делавер, Флорида, Індіана, Айова, Монтана, Орегон, Теннессі та Техас прийняли комплексні закони про конфіденційність даних споживачів на рівні штатів, а у 2024 році – Кентуккі, Меріленд, Міннесота, Небраска, Нью-Гемпшир, Нью-Джерсі та Род-Айленд. Тобто, за відсутності системи конфіденційності даних на федеральному рівні штати продовжують розробляти законодавство [206].

Отже, узагальнений досвід США свідчить, що сучасна модель адміністративно-правового захисту інформації має будуватися не лише на імперативному регулюванні, а й на гнучких інструментах взаємодії та локальному регулюванні у питаннях реалізації превентивних заходів та управління ризиками. Водночас важливим є врахування балансу між посиленням кібербезпеки та забезпеченням належного рівня захисту персональних даних громадян.

З урахуванням викладеного, логічним є звернення до досвіду Європейського Союзу, який сформував іншу модель регулювання у сфері інформаційної безпеки та захисту даних, що ґрунтується на принципах

уніфікації правових стандартів, централізованої гармонізації законодавства держав-членів та пріоритеті захисту прав і свобод людини в цифровому середовищі.

Ключовим актом у сфері захисту інформації є Загальний регламент про захист даних (GDPR) 2016/679 [225], який встановлює єдині правила обробки персональних даних на всій території ЄС. Регламент визначає принципи законності, добросовісності, прозорості, мінімізації даних та обмеження цілей їх обробки. Він також передбачає широкі права суб’єктів даних, зокрема право на доступ, виправлення, стирання («право на забуття») та обмеження обробки.

Важливим елементом є Директива про безпеку мережевих та інформаційних систем (NIS Directive) [210], яка спрямована на підвищення рівня кібербезпеки та захисту критичної інформаційної інфраструктури. У 2022 році її було оновлено у вигляді NIS2, що розширює сферу застосування та посилює вимоги до суб’єктів господарювання. Директива запровадила культуру управління ризиками та звітності про інциденти серед ключових економічних суб'єктів – операторів, що надають основні послуги (OES), та постачальників цифрових послуг (DSP). Директива також визначила механізми співпраці, такі як Група співробітництва NIS та мережа національних груп реагування на інциденти комп’ютерної безпеки (CSIRT) [211].

Також значення має Директива про приватність та електронні комунікації [209], яка регулює конфіденційність електронних комунікацій, включаючи використання «cookies» та обробку трафікових даних. Як і інші директиви ЄС, вона сама по собі не є обов’язковим законом, а радше інструкцією для держав-членів ЄС щодо створення власних законів, що відповідають цій директиві. Директива про електронну конфіденційність була прийнята у 2002 році, а потім змінена у 2009 році [246].

Окремо варто відзначити Акт про цифрові послуги та Акт про цифрові ринки від 19 вересня 2022 року, які встановили нові правила для цифрових

платформ і спрямовані на підвищення прозорості, безпеки та підзвітності у цифровому середовищі.

Ці документи вимагають від постачальників посередницьких послуг внести зміни до правил користування платформами, створити єдині канали для комунікації з контролюючими органами та споживачами послуг, відкрити представництва у ЄС, публікувати інформацію про систему модерації контенту тощо. Їх норми розповсюджуються на всіх постачальників посередницьких послуг, що зареєстровані в ЄС або надають послуги на території ЄС. Зауважимо, що посередницькі послуги є послугами зі зберігання та передачі будь-якої інформації, а саме соціальні мережі, маркетплейси, відеохостинги, месенджери тощо. До надавачів посередницьких послуг відносяться, наприклад, Google, YouTube, Facebook, Airbnb, Amazon тощо [216].

Щодо інституційного контексту адміністративно-правового захисту інформації в ЄС, то він включає як наднаціональні, так і національні органи.

Координаційну роль відіграє Європейська рада із захисту даних (EDPB) [213], який забезпечує узгоджене застосування GDPR, розробляє рекомендації та сприяє співпраці між національними органами.

EDPB – це незалежний європейський орган із правосуб'єктністю. Він забезпечує послідовне застосування Загального регламенту про захист даних та Директиви про правоохоронну діяльність і співпрацю, зокрема у сфері забезпечення дотримання законодавства. Європейська рада з захисту даних складається з керівників національних органів захисту даних (наглядових органів) країн Європейської економічної зони, а також Європейського інспектора із захисту даних. Органи захисту даних відповідають за забезпечення дотримання законодавства про захист даних на національному та транскордонному рівнях шляхом співпраці через механізм єдиного вікна [243].

Контроль за дотриманням правил у кожній державі-члені здійснюють незалежні національні органи із захисту даних (Data Protection Authorities).

Вони мають повноваження проводити перевірки, розглядати скарги та накладати адміністративні санкції.

Кожен орган захисту даних (DPA) відповідає за моніторинг та забезпечення дотримання GDPR, а також за підвищення обізнаності та розуміння громадськістю ризиків, правил, гарантій та прав, пов'язаних з обробкою персональних даних. DPA також мають завдання консультувати національний парламент, уряд та інші установи й органи, а також надавати інформацію будь-якій особі щодо здійснення їхніх прав. DPA також сприяють обізнаності контролерів даних та обробників даних про їхні зобов'язання згідно з GDPR. DPA розглядають скарги від фізичних осіб, проводять розслідування щодо належного застосування GDPR та співпрацюють з іншими DPA щодо застосування GDPR. Органи влади також несуть відповідальність за: 1) прийняття та затвердження стандартних договірних положень; 2) затвердження обов'язкових корпоративних правил; 3) затвердження кодексів поведінки; 4) заохочення до створення механізмів сертифікації захисту даних; 5) сприяння діяльності Європейської ради з захисту даних (ЄДПБ); 6) виконання будь-яких інших завдань, пов'язаних із захистом персональних даних [205].

У сфері кібербезпеки важливу роль виконує Агентство Європейського Союзу з кібербезпеки (ENISA) [215], яке розробляє рекомендації, проводить оцінку ризиків та сприяє підвищенню кіберстійкості держав-членів.

Разом з тим європейська модель характеризується активним застосуванням адміністративних санкцій за порушення законодавства у сфері захисту інформації. Одним із найбільш відомих прикладів є накладення штрафів на компанію «Google» за порушення вимог GDPR щодо прозорості обробки даних та отримання згоди користувачів (рішення французького регулятора CNIL, 2019 р.) [242]. Іншим прикладом є штрафи щодо «Meta Platforms» (Фейсбук) [212], пов’язані з незаконною передачею персональних даних за межі ЄС, що підкреслює суворість вимог до трансграничної передачі інформації. Також показовим є рішення Суду ЄС у справі «Schrems

II» (2020 р.) [98], яким було визнано недійсним механізм «Privacy Shield»/«Щит конфіденційності» між ЄС і США через недостатній рівень захисту персональних даних.

Отже, адміністративно-правовий захист інформації в Європейському Союзі базується на: 1) уніфікованому та комплексному правовому регулюванні; 2) високому рівні захисту прав суб'єктів даних; 3) ефективній системі нагляду та контролю; 4) значних адміністративних санкціях як механізмі забезпечення дотримання законодавства.

При цьому додамо, що загалом європейський підхід орієнтований насамперед на захист прав людини та забезпечення балансу між розвитком цифрової економіки і приватністю, що робить його одним із найбільш прогресивних у світі та релевантним для імплементації в національне законодавство України.

Тож, якщо порівняти дві вище проаналізовані системи адміністративно-правового захисту інформації, можна прийти до наступних висновків:

– на концептуальному рівні обидві моделі визнають людину та її фундаментальне право на приватність і захист персональних даних;

– щодо нормативно-правової структури, – європейська модель характеризується високим рівнем уніфікації та системності. Основним актом є Загальний регламент про захист даних, який має пряму дію в усіх державах-членах. Додатково функціонують галузеві акти, такі як Директива про безпеку мережевих та інформаційних систем (NIS/NIS2) та Директива про конфіденційність та електронні комунікації. Американська система є фрагментованою: відсутній єдиний універсальний закон, натомість діє сукупність спеціалізованих актів, серед яких Закон про конфіденційність 1974 року, Закон про переносимість та підзвітність медичного страхування та Закон про управління федеральною інформаційною безпекою. Значну роль відіграє також законодавство штатів;

– щодо інституційної моделі то у ЄС функціонує скоординована система незалежних наглядових органів, діяльність яких узгоджується

Європейською радою із захисту даних. Контроль здійснюється на національному рівні через органи із захисту даних, які мають широкі повноваження щодо застосування санкцій. У США інституційна система є більш децентралізованою. Повноваження розподілені між різними органами, зокрема Федеральною торговою комісією, Міністерством внутрішньої безпеки та Агентством з кібербезпеки та безпеки інфраструктури. Такий підхід забезпечує гнучкість, але може призводити до фрагментації регулювання;

– щодо механізмів забезпечення та відповідальності за правопорушення у сфері захисту інформації то європейський підхід передбачає суворі адміністративні санкції. Відповідно до Загального регламенту про захист даних штрафи можуть досягати 20 млн євро або 4% глобального обороту компанії. Така модель стимулює високий рівень дотримання законодавства. У США відповідальність реалізується через поєднання адміністративних санкцій, судових позовів і механізмів колективних позовів (class actions). Значну роль відіграє правозастосовна практика Федеральної торгової комісії;

– щодо підходів до кібербезпеки то у ЄС кібербезпека інтегрована в загальну систему регулювання через Директиву про безпеку мережевих та інформаційних систем та діяльність Агентства Європейського Союзу з кібербезпеки. У США кібербезпека розглядається як складова національної безпеки. Значну роль відіграють Агентство з кібербезпеки та безпеки інфраструктури та стандарти Національного інституту стандартів і технологій, що широко застосовуються у публічному та приватному секторах.

Порівняльний аналіз свідчить, що обидві моделі мають свої переваги та недоліки. Європейський підхід забезпечує високий рівень захисту прав людини та правову визначеність, тоді як американський – гнучкість, інноваційність і ефективну взаємодію з приватним сектором. Для України доцільним є поєднання елементів обох систем, зокрема: 1) імплементація європейських стандартів захисту персональних даних; 2) запозичення американського досвіду публічно-приватного партнерства; 3) впровадження

ризик-орієнтованого підходу до кібербезпеки; 4) посилення інституційної спроможності органів державної влади.

3.2. Удосконалення адміністративного законодавства щодо діяльності органів публічної адміністрації у сфері захисту інформації

Сьогодні вкрай нагально постає питання забезпечення інформаційної безпеки держави, суспільства та особи [4, с. 177]. Тому логічно, що органи публічної адміністрації у сфері захисту інформації стикаються з низкою складних викликів та проблем, які вимагають комплексного підходу та постійного оновлення стратегій захисту. Одними з основних викликів є кіберзагрози та витоки інформації, що можуть мати різноманітні форми та масштаби [193, с. 11].

У зв'язку з цим був прийнятий Національний план реагування на кіберінциденти, кібератаки та кіберзагрози і затверджений постановою Кабінету Міністрів України від 26 листопада 2025 року № 1533.

Цей Національний план визначає загальні процедури реагування на кіберінциденти, кібератаки, кіберзагрози, а також механізм координації та взаємодії між суб'єктами національної системи реагування на кіберінциденти, кібератаки, кіберзагрози та суб'єктами забезпечення кібербезпеки, їх роль в рамках функціонування національної системи реагування на кіберінциденти, кібератаки, кіберзагрози та національної системи обміну інформацією про кіберінциденти, кібератаки, кіберзагрози [42].

Якщо оцінювати його саме крізь призму діяльності органів публічної адміністрації у сфері захисту інформації, то можна виділити низку системних недоліків.

– нормативна декларативність та розмитість повноважень. Йдеться про відсутність чіткої ієрархії між суб'єктами в контексті забезпечення необхідної

взаємодії та імперативності формулювань («можуть», «за потреби»). Основна проблема в зазначеному, це розмивання відповідальності, а точніше її відсутність;

– відсутність механізмів юридичної відповідальності. Логічне продовження попереднього тезису. Проте тут мається на увазі більш загальний контекст, адже нормативним матеріалом не визначено наслідків невиконання обов'язків щодо реагування та інформування;

– фрагментарна імплементація ризик-орієнтованого підходу. Хоча на рівні законодавства та підзаконних актів задекларовано необхідність урахування кіберризиків, відповідний підхід не набув ознак системності, оскільки відсутні уніфіковані та обов'язкові для застосування методики оцінки ризиків, а також їх інтеграція у процеси прийняття управлінських рішень органами публічної адміністрації;

– надмірна децентралізація функцій реагування без належного ресурсного забезпечення. Передбачена можливість створення галузевих і регіональних команд реагування (CSIRT) не супроводжується встановленням мінімальних стандартів їх кадрового, технічного та фінансового забезпечення, що призводить до нерівномірності спроможностей різних суб'єктів та потенційного перевантаження національного рівня;

– неврегульованість участі приватного сектору у механізмах реагування. Нормативний матеріал допускає залучення приватних суб'єктів, однак не визначає їх чіткого правового статусу, порядку акредитації, меж відповідальності та гарантій захисту інформації, що ускладнює ефективну реалізацію публічно-приватного партнерства у сфері кібербезпеки;

– дисбаланс між відкритістю інформації та її обмеженням. З одного боку, встановлюється принцип відкритості інформації про кіберінциденти, з іншого –передбачено широкі підстави для віднесення відомостей до інформації з обмеженим доступом. Відсутність чітких критеріїв їх співвідношення створює ризики як надмірного засекречування, так і потенційного розголошення чутливої інформації;

– недостатня деталізація адміністративних процедур прийняття рішень. План переважно орієнтований на технічні аспекти реагування, водночас залишаючи поза належною увагою управлінський компонент, зокрема форми актів реагування, строки їх прийняття та порядок документування відповідних рішень органами публічної адміністрації;

– відсутність ефективних механізмів оцінки результативності реагування. Хоча передбачено етап аналізу ефективності, він має здебільшого формальний характер, оскільки не супроводжується встановленням чітких показників оцінки (KPI), процедур незалежного аудиту та обов'язкових наслідків за результатами такого аналізу.

Нагадаємо, що міжнародний досвід демонструє ефективні правові моделі, які можуть бути адаптовані до українських реалій. Директива ЄС NIS2 встановлює стандарти захисту критичної інфраструктури, передбачаючи адміністративну відповідальність за невідповідність вимогам кібераудиту [208]. Наприклад, у Польщі імплементація NIS2 дозволила скоротити кіберінциденти на 30% за 2022–2023 роки завдяки обов'язковому кібераудиту приватних компаній [229]. Стратегія НАТО акцентує на правових аспектах кібернавчань, що сприяють координації країн-членів. У 2023 році НАТО провела навчання Cyber Coalition, які включали юридичний компонент для відпрацювання транскордонних санкцій [230]. У США Агентство з кібербезпеки та безпеки інфраструктури (CISA) діє як юридична особа з правом накладати санкції за кіберправопорушення, що забезпечує швидке реагування [229]. Ці моделі потребують модифікації для України через специфіку воєнного стану. Тому долучаємось до пропозиції створення міжнародного хабу кіберзахисту як юридичної особи під егідою Міністерства цифрової трансформації, який мав би повноваження укладати угоди з НАТО, ЄС і приватними компаніями, такими як Microsoft чи Google. Аналіз співпраці України з Microsoft у 2022 році показує, що обмін технологіями скоротив час реагування на кібератаки на 20% [57]. Такий хаб міг би координувати правові стандарти, розробляти протоколи реагування та

забезпечувати юридичну підтримку для транскордонного переслідування кіберзлочинців [32].

Узагальнюючи, варто зазначити, що цей документ за своєю природою має переважно описовий та рамковий характер. Він формує загальну модель реагування на кіберінциденти, визначає основні етапи, суб'єктний склад та напрями взаємодії, однак не забезпечує належного рівня нормативної деталізації відповідних процедур і повноважень.

З одного боку, окремі його положення вже конкретизуються в інших нормативно-правових актах (зокрема, у сфері захисту інформації, кібербезпеки, критичної інфраструктури, діяльності спеціально уповноважених органів), що частково компенсує його декларативність. З іншого боку, значна частина передбачених механізмів фактично залишається незавершеною, оскільки потребує подальшої регламентації на рівні підзаконних актів, відомчих інструкцій, стандартів та процедур.

Таким чином, Національний план не виступає самодостатнім регуляторним інструментом, а радше виконує функцію концептуально-організаційної основи, яка має бути наповнена конкретним юридичним змістом через систему спеціалізованих нормативних актів. Без такого нормативного «доопрацювання» його практична ефективність у сфері діяльності органів публічної адміністрації щодо захисту інформації залишається обмеженою.

Приміром, необхідний акт, який би деталізував: 1) алгоритми взаємодії між Державною службою спеціального зв'язку та захисту інформації України, Службою безпеки України, іншими органами виконавчої влади та органами місцевого самоврядування; 2) процедури обміну інформацією (з урахуванням рівнів доступу); 3) порядок спільного прийняття рішень у кризових ситуаціях.

Варто вказати й що чинна нормативно-правова база України, зокрема Закони «Про основи національної безпеки», «Про кібербезпеку» і «Про інформацію», закладають базові принципи захисту інформаційного простору,

мають системні недоліки. Закон «Про основи національної безпеки» визначає інформаційну безпеку як складову національного суверенітету, але не містить конкретних норм прямої дії для умов воєнного стану. Наприклад, стаття 7 цього закону декларує захист інформаційного простору, але не уточнює механізмів координації між державними органами в умовах кібератак. Це призводить до правової невизначеності, як було у випадку з атакою на «Укренерго», де повноваження РНБО та Міненерго дублювалися [6]. Закон «Про кібербезпеку» регулює захист критичної інфраструктури, але не враховує сучасних технологій, таких як ШІ чи блокчейн, які активно використовуються в кібератаках. Наприклад, у 2023 році зафіксовано випадки використання ШІ для автоматизації фішингових атак, які не підпадають під чинні норми закону через відсутність їхнього правового визначення [58]. Порівняно з Директивою ЄС NIS2, яка встановлює стандарти кібераудиту та відповідальність за використання новітніх технологій [208], українське законодавство виглядає фрагментарним. Крім того, закон не адаптований до умов воєнного стану, що вимагає швидшого реагування на загрози, ніж передбачено стандартними процедурами. Закон «Про інформацію» гарантує право на достовірну інформацію, але не містить механізмів протидії дезінформації в цифровому середовищі. Колізії між цими законами ускладнюють правозастосування. Наприклад, у 2023 році судовий розгляд справи про поширення фейків у Telegram виявив дублювання повноважень між Міністерством культури та інформаційної політики РНБО, що призвело до затримки в ухваленні рішення [51]. Аналіз судової практики підтверджує, що правові прогалини перешкоджають ефективному захисту інформаційного простору. У порівнянні з міжнародними стандартами, такими як Стратегія кібербезпеки НАТО [230], яка передбачає чітку координацію між органами влади, Україна потребує системного оновлення законодавства [79].

Відповідно, з практичного боку є доцільним: 1) впровадження ризикоорієнтованого підходу, який сприятиме більш гнучкому і ефективному управлінню кіберзагрозами, зменшуючи залежність від формальних

процедур; 2) закріплення законодавчих рамок для застосування штучного інтелекту у кіберзахисті, що включатиме як етичні, так і технічні аспекти; 3) розширення повноважень Держспецзв'язку, які посилить координацію національної системи реагування на кіберінциденти; 4) імплементація вимог директиви NIS2, яка закріпить інтеграцію України у європейське кібербезпекове середовище [79].

Також з метою підвищення спроможності публічної адміністрації варто: запровадити обов'язкові вимоги до кваліфікації керівників з кіберзахисту; визначити систему сертифікації та регулярного підвищення кваліфікації; закріпити стандарти професійної підготовки.

Ну і звісно посилення юридичної відповідальності. При цьому зазначене є актуальним як за кіберправопорушення, адже це критично важливо для стримування агресорів (нинні норми Кримінального кодексу України не відповідають масштабам сучасних кіберзагроз через що доцільним є внесення зміни до КК України, запровадивши нову статтю, яка б визначала «кібердиверсію» як злочин, спрямований на порушення національної безпеки через кіберпростір, із санкціями до 10 років позбавлення волі [79]), так і в контексті функціонування інституту юридичної відповідальності юридичних осіб публічного права.

Уточнимо, що жоден закон не спроможний упорядкувати певну галузь або сферу суспільного життя, якщо він не виконується [36, с. 79]. Особливо небезпечно, коли законодавства не дотримаються представники органів державної влади чи місцевого самоврядування, тобто особами, які в силу своїх повноважень повинні забезпечувати законність та правопорядок у суспільстві. Відповідно, високий рівень виконавської дисципліни в органах державної влади і місцевого самоврядування є важливим індикатором для суспільства чи діє принцип верховенства права. Тому особливістю норм, які регламентують відповідальність органів влади, повинна бути їхня невідворотність для посадовців усіх рівнів. Лише персональна відповідальність посадових осіб органів влади і перспектива бути

дискваліфікованим на деякий час (неможливість займати відповідні посади) сприятиме прозорому і зрозумілому для суспільства результату та меті, для чого існують органи влади і їхня цінність у забезпеченні принципу верховенства права. Така модель сприйматиметься суб'єктами цивільних правовідносин як закріплення реальних можливостей, що забезпечує держава. А невідворотність відповідальності за скоєні правопорушення стимулюватиме представників органів державної влади і місцевого самоврядування до правомірних дій. У цьому і проглядається тісний взаємозв'язок між категоріями «законність» та «юридична відповідальність» [96, с. 187].

Ми погоджуємося з позицією Т. Гуржій та Н. Нікітченко про те, що майнова відповідальність органів публічної влади набуває декларативного характеру за відсутності реального фінансового забезпечення її виконання, зокрема коштів, за рахунок яких може бути здійснене відшкодування шкоди потерпілій особі. На сьогодні механізм відшкодування шкоди, завданої державою, має комплексний характер і визначається положеннями Цивільний кодекс України, бюджетного законодавства, а також щорічного закону про державний бюджет. Виконання відповідних судових рішень здійснюється за участю Державна казначейська служба України, яка забезпечує списання коштів у межах бюджетних асигнувань та відповідно до встановлених процедур. Водночас, попри наявність нормативного регулювання, на практиці зберігається низка суттєвих проблем. Зокрема, дискусійним залишається питання визначення належного боржника у справах про відшкодування шкоди: з одного боку, покладення такого статусу на казначейські органи є юридично некоректним, оскільки вони не є суб'єктами правопорушення; з іншого – окремі органи публічної влади, дії чи бездіяльність яких спричинили шкоду, не завжди мають статус юридичної особи або відповідні бюджетні повноваження для самостійного виконання таких зобов'язань [36; 96, с. 189].

У результаті зазначені обставини зумовлюють неоднорідність судової практики, ускладнюють виконання судових рішень та знижують ефективність механізму реалізації права на відшкодування шкоди, завданої державою. Це, у свою чергу, свідчить про необхідність подальшого вдосконалення адміністративно-правових та фінансово-правових засад відповідальності держави, зокрема в частині чіткого визначення суб'єкта відповідальності та забезпечення належного бюджетного покриття відповідних виплат.

Також створенню дієвого механізму притягнення до відповідальності органів державного контролю перешкоджає і той факт, що відсутність бюджетних коштів автоматично призводить до ігноруванням з боку держави обов'язку відшкодування завданих витрат, оскільки бюджетний процес не передбачає обов'язковості фінансування всіх зобов'язань органів державної влади. Так, за відсутності в розписі видатків бюджету статті, за рахунок якої повинно здійснюватися відшкодування шкоди, завдані збитки можуть бути не відшкодовані взагалі, навіть на підставі рішення суду. Зокрема, чинне законодавство передбачає відшкодування шкоди за рахунок бюджетних коштів, що виділяються на фінансування органу, який завдав шкоду, а це кошти, що виділяються із сум, передбачених на забезпечення діяльності цього органу. Відповідно, орган влади не поспішає приймати рішення про відшкодування шкоди, а потерпіла особа роками не може захистити свої законні права [96, с. 189].

Окремо зазначимо щодо витоку інформації, адже варто уточнити, що несанкціонований доступ до конфіденційної інформації та її подальше поширення може призвести до значних фінансових збитків, втрати репутації та інших негативних наслідків для організацій та індивідів. Витоки можуть статися через слабкі місця в захисті даних, людські помилки або навмисні дії інсайдерів [193]. Тому вкрай важливо забезпечити функціонування належного механізму оцінки ефективності систем протидії витоку інформації, зокрема володільцями чи розпорядником якої є держава.

Щодо цього актуально буде також зазначити, що зараз активно поширюється інформація про можливий «злив» даних з системи «Дія». Йдеться про те, що у відкритому доступі знайшли архів даних із назвою diia_users_db_2025.zip. Файл потенційно може містити паспортні, податкові та контактні дані мільйонів громадян [191].

У Міністерстві цифрової трансформації заперечили «злив» даних з «Дії», адже після перевірки було встановлено, що ці файли – суміш старих витоків із комерційних джерел, які вручну доповнили вигаданими записами, щоб видати їх за нову базу. Це типова практика чорного ринку. У міністерстві підкреслили, що «Дія» не зберігає даних користувачів. Система працює за моделлю data-in-transit. Це означає, що інформація підтягується з державних реєстрів у момент запиту і не накопичується на серверах застосунку чи порталу. Тобто навіть у разі злому самої «Дії» витягнути з неї «повну базу» неможливо. Додатковим аргументом проти звинувачень стало й те, що ще в березні 2024 року вихідний код застосунку був оприлюднений у відкритому доступі. Це дало змогу всім охочим переконатися, які саме дані обробляє система, а яких у ній немає [191].

Водночас сама поява подібних інформаційних приводів, незалежно від їх достовірності, свідчить про наявність системної проблеми у сфері захисту інформації – недостатній рівень довіри до державних інформаційних систем та відсутність ефективних механізмів превентивної комунікації і верифікації таких повідомлень.

У цьому контексті важливо підкреслити, що навіть якщо конкретний випадок не є реальним витоком, він демонструє вразливість інформаційного середовища до маніпуляцій, що можуть мати не менш серйозні наслідки, ніж фактичні кіберінциденти. Зокрема, поширення недостовірної інформації про витоки даних може спричинити паніку серед населення, підірвати довіру до цифрових сервісів держави та дискредитувати діяльність органів публічної адміністрації.

Це, у свою чергу, актуалізує необхідність розширення підходів до забезпечення інформаційної безпеки. Власне, додамо, що кампанії з поширення фейкової інформації, як-от у Telegram у березні 2023 року, продемонстрували вразливість цифрових платформ до маніпулятивного контенту. Аналіз цього кейсу дозволяє стверджувати, що оперативне виявлення шкідливого контенту могло б скоротити його вплив на 90%, як це спостерігалося в аналогічних випадках у країнах ЄС після впровадження алгоритмічного аналізу. У зв'язку з актуальною є розробка окремого Закону України «Про алгоритмічний моніторинг інформаційного простору», який би встановлював юридичну відповідальність платформ за поширення дезінформації. Закон має передбачати запровадження нової правової категорії «кіберпсихологічна агресія», що охоплюватиме маніпулятивний контент, спрямований на дестабілізацію суспільства. Порівняно з німецьким Законом про мережеву безпеку (NetzDG), який встановлює штрафи до 50 млн євро за ігнорування дезінформації, українська модель має бути адаптованою до економічних умов, передбачаючи штрафи до 1 млн грн за порушення. Це дозволить не лише посилити контроль над цифровим середовищем, а й стимулювати платформи до співпраці з державними органами [79].

Однак важливими є не лише технічні та організаційні заходи протидії витокам, але й запровадження ефективних механізмів стратегічних комунікацій, оперативного інформування та спростування недостовірних відомостей. Відповідні функції мають бути чітко інституціоналізовані та нормативно закріплені за визначеними суб'єктами публічної адміністрації або делеговані приватному сектору.

Щодо цього зауважимо, що аналітичні дослідження національних та зарубіжних авторів підтверджують: ефективна система державно-приватного партнерства у кібербезпеці не обмежується залученням технічних спроможностей бізнесу, а охоплює нормативно-правові механізми взаємодії, моделі обміну інформацією, інституційні формати спільного реагування на інциденти та стандарти організації кіберзахисту на рівні критичної

інфраструктури [33; 38; 56; 114]. В умовах повномасштабної війни Україні особливо значущими є сталі канали обміну оперативною інформацією, участь приватних компаній у виявленні та нейтралізації загроз, а також розбудова партнерських механізмів, що довели свою ефективність у країнах ЄС, США та НАТО [45; 76, с. 175; 203; 214; 231].

Нам також слушною видається думка, що доцільно запровадити механізм «цифрових санкцій», який передбачав би відключення серверів, що сприяють поширенню дезінформації. Практика ЄС, зокрема у Франції, де відключення серверів російських бот-мереж у 2022 році скоротило дезінформаційні кампанії на 60%, підтверджує ефективність такого інструменту. На відміну від традиційних штрафів, цифрові санкції мають перевагу швидкого реагування, що є критично важливим у воєнний період. Ці зміни дозволять не лише підвищити ефективність правозастосування, а й забезпечити превентивний ефект, стримуючи потенційних правопорушників [79].

Разом з тим, окремої уваги, на нашу думку, заслуговує питання корупційних проявів. На сьогодні існує великий масив доказів, що електронні системи закупівель підвищують конкуренцію і зменшують можливості корупції, але ефект більш помітний там, де є сильні інститути та відкритість даних [175].

Зокрема службовими особами Державного центру кіберзахисту (ДЦКЗ) Держспецзв’язку та іншими посадовими особами суб’єктів підприємницької діяльності за підтримки представників Cisco в Україні та керівництва Ради національної безпеки і оборони України організовано протиправну схему по розтраті бюджетних коштів в особливо великих розмірах. Протягом 2017–2019 років службовими особами ДЦКЗ Держспецзв’язку проведено низку конкурсних закупівель за результатами, яких підписано договори з ДП «Державний центр інформаційної безпеки», ТОВ «Спеціальні телекомунікаційні рішення», ТОВ «Інформаційні технології та інформаційна безпека», ТОВ «Айті-Со- 121 люшнс», ТОВ «Есай Біс», ТОВ Фірма

«ВалТек», ТОВ «Ньютест Україна», ТОВ «Грін Нетворкс», ТОВ «Ай Ай Ті Трейдінг». 30.10.2017 року ДЦКЗ Держспецзв'язку укладено договір з Державним підприємством «Державний центр інформаційної безпеки» на закупівлю «спеціального програмного забезпечення терміналу мобільного зв'язку для шифрованого обміну даними, що циркулюють в межах мобільного зв'язку та має бути реалізовано у вигляді додатку…» в кількості 1 шт. загальною вартістю 1,1 млн. грн. Посадові особи ДП «ДЦІБ» того ж дня, 30.10.2017 року за результатами проведення конкурсної закупівлі № UA-2017-11-07-000231-c уклали Договір № ДП30/10 з підприємством ПП «Альфа Ком» на закупівлю спеціального програмного забезпечення терміналу мобільного зв'язку вартістю 1 142 729,59 грн. В ході досудового розслідування, з'ясовано, що директор вищевказаного СПД не має відношення до фінансово-господарської діяльності підприємства, а фактично керують діяльністю ПП «Альфа Ком» службові особи ДЦКЗ Держспецзв'язку. Зобов'язань ПП «Альфа Ком» перед ДП «ДЦІБ» не виконало, спеціальне програмне забезпечення не поставлено, при цьому акти виконаних робіт між ДЦКЗ Держспецзв'язку та ДП «ДЦІБ» підписано. За результатом виконання зазначеного договору, посадові особи ДЦК Держспецзв'язку у змові з посадовими особами ДП «ДЦІБ» безпідставно перерахували, а у подальшому привласнили 1,1 млн. грн. бюджетних коштів [185]. Зазначимо, що теоретично можна допускати недостатнє матеріальне забезпечення співробітників Держспецзв'язку України як передумову до подібних протиправних дій. Однак у сучасний період, коли держава перебуває у фактичному стані війни з РФ, жодних виправдань для подібних протиправних дій не може бути [115, с. 120–121].

Однак варто враховувати й те, що з розвитком інформаційно-комунікаційних технологій і їх інтенсивним впровадженням у діяльність органів державної влади трансформуються і самі форми корупційної діяльності, набуваючи більш прихованого, технологічно опосередкованого характеру.

Тому вбачаємо також актуальним запровадити: а) у сфері протидії політичній корупції – посилення діяльності НАЗК: 1) забезпечення ефективної його діяльності шляхом зміни моделі цього органу й посилення його інституційної спроможності; 2) забезпечення дієвості заходів, спрямованих на отримання повних, об'єктивних і достовірних даних щодо стану корупції в Україні; 3) забезпечення ефективного функціонування уповноважених осіб (уповноважених підрозділів) з питань запобігання та виявлення корупції; 4) удосконалення законодавства про запобігання та врегулювання конфлікту інтересів у діяльності осіб, уповноважених на виконання функцій держави або місцевого самоврядування, та прирівняних до них осіб; 5) підвищення рівня оперативності й ефективності виявлення фактів порушення вимог законодавства про запобігання та врегулювання конфлікту інтересів; 6) однакове тлумачення й застосування законодавства правозастосовними органами; 7) підвищення рівня знань вимог законодавства про запобігання та врегулювання конфлікту інтересів, формування навичок правильної поведінки в різних життєвих ситуаціях; 8) забезпечення належного правового регулювання захисту викривачів відповідно до міжнародних стандартів; 9) забезпечення спроможності НАЗК та інших спеціально уповноважених суб'єктів у сфері протидії корупції гарантувати державний захист викривачів [198]; б) у бізнес-середовищі: 1) на державному рівні: залучення бізнесу до політик подолання корупції, підтримка цих політик вищим керівництвом держави, пошук нової еліти, яка може ці політики реалізувати на практиці; 2) на рівні бізнес-середовища: прийняття внутрішньої корпоративної політики на рівні окремої компанії, програми комплаєнс, запровадження системи внутрішнього контролю, спеціальної посади в компанії з протидії корупції, формування культури неприйняття корупції всередині компанії на рівні топменеджерів й інших співробітників; 3) на рівні асоціацій: спільне просування антикорупційних принципів ведення бізнесу та відстоювання своїх інтересів [5, с. 7; 125, с. 375].

Разом із тим наведений приклад свідчить не лише про наявність окремих правопорушень, а й про існування системних прогалин у механізмах контролю, підзвітності та прозорості діяльності органів публічної адміністрації у сфері кібербезпеки та захисту інформації. Йдеться, зокрема, про недостатню ефективність процедур публічних закупівель, формальний характер перевірки виконання договірних зобов'язань, а також відсутність належного внутрішнього та зовнішнього аудиту реалізації відповідних проєктів.

Існує думка, що вирішити цю проблему зможе цифрове врядування як чинник інституційної модернізації, який забезпечує перехід від бюрократичної моделі управління до проактивної, прозорої та орієнтованої на громадянина системи, у межах якої корупційні можливості системно обмежуються технологічними засобами. Вважається, що у контексті протидії корупційним проявам, перевагами застосування цифрових інструментів у публічно-владній площині є такі: 1) автоматизація адміністративних процесів, що забезпечує безособову взаємодію держави з громадянами та мінімізує дискреційний вплив посадових осіб; 2) відкритість даних і підзвітність, які формують належне правове середовище для ефективної реалізації громадського контролю та проведення журналістських розслідувань; 3) оперативність та ефективність, що передбачають скорочення часових, фінансових та інших витрат під час здійснення адміністративних процедур; 4) підвищення рівня довіри до публічної влади, оскільки ефективне і прозоре надання адміністративних послуг за допомогою цифрових сервісів сприяє зміцненню легітимності державних інститутів в очах громадян [175].

У цьому контексті важливо наголосити, що цифровізація сама по собі не усуває корупційні ризики, а лише змінює форми їх прояву. Якщо традиційні корупційні практики були пов'язані переважно з адміністративними рішеннями та розподілом ресурсів, то в умовах інформатизації вони дедалі частіше пов'язані з маніпулюванням цифровими

процесами, технічними специфікаціями, алгоритмами закупівель, а також із використанням складних ланцюгів підрядників для приховування протиправної діяльності.

Саме тому запропоновані заходи протидії корупції мають розглядатися не ізольовано, а як складова комплексного адміністративно-правового механізму забезпечення інформаційної безпеки. Їх реалізація повинна супроводжуватися:

– посиленням цифрової прозорості процедур (зокрема, через повну відстежуваність життєвого циклу проєктів у сфері ІКТ);

– запровадженням обов'язкового технічного та фінансового аудиту ІТ-рішень, що закуповуються за бюджетні кошти;

– уніфікацією вимог до підрядників у сфері кібербезпеки та встановленням чітких критеріїв їх доброчесності;

– інтеграцією антикорупційних інструментів безпосередньо в інформаційні системи (журналювання дій, автоматичні тригери ризиків, контроль доступу тощо).

Крім того, важливо забезпечити належну координацію між антикорупційними органами, суб'єктами забезпечення кібербезпеки та органами фінансового контролю, що дозволить своєчасно виявляти як класичні, так і новітні форми корупційних правопорушень.

Таким чином, боротьба з корупційними проявами у сфері захисту інформації повинна здійснюватися з урахуванням технологічної специфіки сучасних управлінських процесів і передбачати поєднання правових, організаційних та технічних інструментів.

Варто звернути увагу на зауваження П. Яковлєва, що «однією із найбільш важливих функцій державного регулювання у сфері забезпечення інформаційної безпеки слід вважати, на нашу думку, функцію створення умов для формування безпечного інформаційного простору в Україні. Значення цієї функції є вирішальним, оскільки в умовах протидії інформаційній агресії з боку РФ ззовні та її прихильників всередині держави, необхідно

запропонувати адекватне заміщення інформації на таку, що давала б можливість громадянам України адекватно оцінювати ситуацію в країні та не піддаватися на інформаційні провокації, позбавитись негативного впливу ворожої пропаганди, не допустити використання інформаційного простору держави в деструктивних цілях або для дій, що спрямовані на дискредитацію України на міжнародному рівні» [199]. До таких функцій, зокрема, можна віднести: 1) «стимулювання розвитку національного виробництва текстового і аудіовізуального контенту; 2) забезпечення функціонування Суспільного телебачення і радіомовлення України, у тому числі його належного фінансування; 3) створення системи мовлення територіальних громад, яка сприятиме розширенню комунікативних можливостей та зниженню конфліктності всередині громад; 4) підтримка вітчизняної книговидавничої справи, зокрема перекладів іноземних творів, забезпечення ними навчальних закладів і бібліотек; 5) комплексна підтримка розвитку механізмів саморегуляції засобів масової інформації на засадах соціальної відповідальності; 6) підвищення медіа-грамотності суспільства, сприяння підготовці професійних кадрів для медіа-сфери з високим рівнем компетентності; 7) формування системи державної підтримки виробництва вітчизняного аудіовізуального продукту; 8) пропагування, у тому числі через аудіовізуальні засоби, зокрема соціальну рекламу, основних етапів і досвіду державотворення, цінностей свободи, демократії, патріотизму, національної єдності, захисту України від зовнішніх і внутрішніх загроз тощо» [163, с. 186–187; 199].

Нам імпонує думка того, що значущий елемент функції формування передумов для створення безпечного інформаційного простору в Україні – функція забезпечення відкритості й прозорості держави перед громадянами, що передбачає: зростання механізмів електронного урядування; підтримку розвитку доступу й застосування публічної інформації у форматі відкритих даних; надання громадянам України інформації про роботу органів державної влади, налагодження дієвого співробітництва згаданих органів зі ЗМІ й

журналістами; реалізація реформи урядових комунікацій; розвиток сервісів, орієнтованих на значно масштабніше і більш результативне залучення громадян до ухвалення рішень органами державної влади й органами місцевого самоврядування; підтримка утворення культури суспільної дискусії та ін. [163, с. 187].

Разом з тим, логічним продовженням викладеного є акцент на тому, що виявлені проблеми та запропоновані напрями їх вирішення потребують не лише концептуального обґрунтування, але й належного нормативного закріплення, інституційного забезпечення та практичної імплементації.

У цьому контексті доцільно зазначити, що подальше удосконалення адміністративного законодавства у сфері діяльності органів публічної адміністрації щодо захисту інформації має здійснюватися за кількома взаємопов’язаними напрямами:

– йдеться про систематизацію та кодифікацію відповідного нормативного матеріалу. Наявна фрагментарність правового регулювання, яка проявляється у розпорошеності норм між різними законами та підзаконними актами, ускладнює їх застосування та знижує ефективність управлінських рішень. У зв’язку з цим перспективним видається розроблення єдиного комплексного нормативного акта (або пакету взаємоузгоджених актів), який би визначав адміністративно-правові засади функціонування системи захисту інформації, чітко окреслював повноваження суб’єктів та встановлював узгоджені процедури їх взаємодії;

– особливого значення набуває деталізація адміністративних процедур у сфері реагування на кіберзагрози та інциденти. Як було встановлено, чинні акти мають переважно рамковий характер і не містять достатньо чітких алгоритмів дій. Тому необхідним є нормативне закріплення стандартів управлінських рішень, строків їх прийняття, порядку документування та механізмів контролю за їх виконанням. Це дозволить не лише підвищити оперативність реагування, але й забезпечити належний рівень підзвітності органів публічної адміністрації;

– потребує подальшого розвитку інститут юридичної відповідальності у сфері інформаційної безпеки. Відсутність чітко визначених санкцій за порушення вимог щодо захисту інформації, неналежне реагування на кіберінциденти або недотримання процедур обміну інформацією фактично нівелює імперативність відповідних норм. У цьому аспекті доцільним є як удосконалення норм адміністративної та кримінальної відповідальності, так і запровадження спеціальних видів відповідальності для суб'єктів, які забезпечують функціонування критичної інформаційної інфраструктури;

– важливим напрямом є інституційне посилення суб'єктів публічної адміністрації. Йдеться не лише про розширення їх повноважень, але й про забезпечення належного кадрового, технічного та фінансового ресурсу. Без цього навіть найбільш досконалі нормативні моделі залишатимуться декларативними. Особливу увагу слід приділити розвитку спеціалізованих підрозділів (зокрема CSIRT), підвищенню кваліфікації персоналу та впровадженню сучасних технологій аналізу кіберзагроз;

– подальшого розвитку потребує механізм публічно-приватного партнерства у сфері кібербезпеки. З огляду на те, що значна частина критичної інфраструктури перебуває у приватній власності або експлуатується приватними суб'єктами, ефективна взаємодія між державою та бізнесом є необхідною умовою забезпечення інформаційної безпеки. Відповідно, законодавство має чітко визначати правовий статус таких суб'єктів, їх права, обов'язки та відповідальність, а також гарантії захисту інформації, що передається у межах такої взаємодії;

– актуальним є впровадження сучасних технологічних рішень у правове поле. Зокрема, використання штучного інтелекту, автоматизованих систем моніторингу та аналізу даних має супроводжуватися належним нормативним регулюванням, яке забезпечуватиме баланс між ефективністю кіберзахисту та дотриманням прав і свобод людини.

Отже, не можна не погодитись з тим, що динамічний розвиток цифрових технологій зумовлює трансформацію традиційних підходів до

управління та правового регулювання суспільних відносин [86, с. 5]. Усі сучасні технології (штучний інтелект, блокчейн, великі дані тощо) створюють одночасно нові можливості та вразливості, тому держава повинна формувати цифрове середовище, у якому розвиток інновацій поєднується з високим рівнем захисту [102, с. 415]. В інформаційні сфері це проявляється у необхідності переосмислення ролі публічної адміністрації як не лише регулятора, але й активного суб'єкта формування безпечного, стійкого та керованого інформаційного простору.

Узагальнюючи, слід підкреслити, що вдосконалення адміністративного законодавства у сфері захисту інформації не може обмежуватися точковими змінами. Воно має носити системний характер і передбачати узгоджене реформування нормативної, інституційної та процедурної складових – через узгодження норм різних галузей права, усунення колізій, деталізацію процедур та запровадження нових правових інститутів, адаптованих до умов цифрової трансформації та воєнного стану.

Висновки до Розділу 3

1. Виявлена різноманітність підходів до формування системи адміністративно-правового захисту інформації на світовому рівні, що зумовлено особливостями правових систем, рівнем технологічного розвитку та пріоритетами державної політики конкретної країни. Однак зауважено, є певна спільність, – у провідних країнах світу сформовано комплексні моделі, які поєднують нормативне регулювання, інституційну спроможність уповноважених органів та сучасні інструменти кібербезпеки.

2. У ході аналізу ефективних практик, що можуть бути актуальними для впровадження в Україні з'ясовано таке:

– у США система адміністративно-правового захисту інформації характеризується високим рівнем інституціоналізації, чітким розмежуванням

повноважень між органами державної влади, а також активним залученням приватного сектору до забезпечення інформаційної безпеки. Загалом досвід США демонструє ефективність комплексного підходу до адміністративно-правового захисту інформації, що включає: 1) спеціалізоване законодавство; 2) потужну інституційну систему з чітким розподілом повноважень; 3) активну взаємодію держави та бізнесу; 4) орієнтацію на ризик-менеджмент і превентивні заходи. Для України важливим є запозичення таких елементів, як розбудова інституційної спроможності органів кібербезпеки, впровадження стандартів на кшталт «NIST», а також розвиток механізмів публічно-приватного партнерства у сфері захисту інформації;

– у ЄС функціонує інша модель регулювання у сфері інформаційної безпеки та захисту даних, що ґрунтується на принципах уніфікації правових стандартів, централізованої гармонізації законодавства держав-членів та пріоритеті захисту прав і свобод людини в цифровому середовищі;

– адміністративно-правовий захист інформації в Європейському Союзі базується на: 1) уніфікованому та комплексному правовому регулюванні; 2) високому рівні захисту прав суб’єктів даних; 3) ефективній системі нагляду та контролю; 4) значних адміністративних санкціях як механізмі забезпечення дотримання законодавства;

– європейський підхід орієнтований насамперед на захист прав людини та забезпечення балансу між розвитком цифрової економіки і приватністю, що робить його одним із найбільш прогресивних у світі та релевантним для імплементації в національне законодавство України.

3. Порівняльний аналіз засвідчив, що: а) на концептуальному рівні обидві моделі визнають людину та її фундаментальне право на приватність і захист персональних даних; б) щодо нормативно-правової структури, – європейська модель характеризується високим рівнем уніфікації та системності. Основним актом є Загальний регламент про захист даних, який має пряму дію в усіх державах-членах. Додатково функціонують галузеві акти, такі як Директива про безпеку мережевих та інформаційних систем

(NIS/NIS2) та Директива про конфіденційність та електронні комунікації. Американська система є фрагментованою: відсутній єдиний універсальний закон, натомість діє сукупність спеціалізованих актів, серед яких Закон про конфіденційність 1974 року, Закон про переносимість та підзвітність медичного страхування та Закон про управління федеральною інформаційною безпекою. Значну роль відіграє також законодавство штатів; в) щодо інституційної моделі то у ЄС функціонує скоординована система незалежних наглядових органів, діяльність яких узгоджується Європейською радою із захисту даних. Контроль здійснюється на національному рівні через органи із захисту даних, які мають широкі повноваження щодо застосування санкцій. У США інституційна система є більш децентралізованою. Повноваження розподілені між різними органами, зокрема Федеральною торговою комісією, Міністерством внутрішньої безпеки та Агентством з кібербезпеки та безпеки інфраструктури. Такий підхід забезпечує гнучкість, але може призводити до фрагментації регулювання; г) щодо механізмів забезпечення та відповідальності за правопорушення у сфері захисту інформації то європейський підхід передбачає суворі адміністративні санкції. Відповідно до Загального регламенту про захист даних штрафи можуть досягати 20 млн євро або 4% глобального обороту компанії. Така модель стимулює високий рівень дотримання законодавства. У США відповідальність реалізується через поєднання адміністративних санкцій, судових позовів і механізмів колективних позовів (class actions). Значну роль відіграє правозастосовна практика Федеральної торгової комісії; д) щодо підходів до кібербезпеки то у ЄС кібербезпека інтегрована в загальну систему регулювання через Директиву про безпеку мережевих та інформаційних систем та діяльність Агентства Європейського Союзу з кібербезпеки. У США кібербезпека розглядається як складова національної безпеки. Значну роль відіграють Агентство з кібербезпеки та безпеки інфраструктури та стандарти Національного інституту стандартів і технологій, що широко застосовуються у публічному та приватному секторах.

4. Констатується, що обидві моделі мають свої переваги та недоліки. Європейський підхід забезпечує високий рівень захисту прав людини та правову визначеність, тоді як американський – гнучкість, інноваційність і ефективну взаємодію з приватним сектором. Для України доцільним є поєднання елементів обох систем, зокрема: 1) імплементація європейських стандартів захисту персональних даних; 2) запозичення американського досвіду публічно-приватного партнерства; 3) впровадження ризик-орієнтованого підходу до кібербезпеки; 4) посилення інституційної спроможності органів державної влади.

5. Встановлено, що чинне адміністративне законодавство України у сфері захисту інформації характеризується фрагментарністю, декларативністю окремих норм та недостатньою процедурною визначеністю, що ускладнює ефективну діяльність органів публічної адміністрації.

6. Проаналізовано положення Національного плану реагування на кіберінциденти, кібератаки та кіберзагрози, що затверджений постановою Кабінету Міністрів України від 26 листопада 2025 року № 1533 на предмет визначення засад діяльності органів публічної адміністрації у сфері захисту інформації. Виділено низку системних його недоліків. Зокрема:

– нормативна декларативність та розмитість повноважень. Йдеться про відсутність чіткої ієрархії між суб’єктами в контексті забезпечення необхідної взаємодії та імперативності формулювань («можуть», «за потреби»). Основна проблема в зазначеному, це розмивання відповідальності, а точніше її відсутність;

– відсутність механізмів юридичної відповідальності. Логічне продовження попереднього тезису. Проте тут мається на увазі більш загальний контекст, адже нормативним матеріалом не визначено наслідків невиконання обов’язків щодо реагування та інформування;

– фрагментарна імплементація ризик-орієнтованого підходу. Хоча на рівні законодавства та підзаконних актів задекларовано необхідність урахування кіберризиків, відповідний підхід не набув ознак системності,

оскільки відсутні уніфіковані та обов'язкові для застосування методики оцінки ризиків, а також їх інтеграція у процеси прийняття управлінських рішень органами публічної адміністрації;

– надмірна децентралізація функцій реагування без належного ресурсного забезпечення. Передбачена можливість створення галузевих і регіональних команд реагування (CSIRT) не супроводжується встановленням мінімальних стандартів їх кадрового, технічного та фінансового забезпечення, що призводить до нерівномірності спроможностей різних суб'єктів та потенційного перевантаження національного рівня;

– неврегульованість участі приватного сектору у механізмах реагування. Нормативний матеріал допускає залучення приватних суб'єктів, однак не визначає їх чіткого правового статусу, порядку акредитації, меж відповідальності та гарантій захисту інформації, що ускладнює ефективну реалізацію публічно-приватного партнерства у сфері кібербезпеки;

– дисбаланс між відкритістю інформації та її обмеженням. З одного боку, встановлюється принцип відкритості інформації про кіберінциденти, з іншого –передбачено широкі підстави для віднесення відомостей до інформації з обмеженим доступом. Відсутність чітких критеріїв їх співвідношення створює ризики як надмірного засекречування, так і потенційного розголошення чутливої інформації;

– недостатня деталізація адміністративних процедур прийняття рішень. План переважно орієнтований на технічні аспекти реагування, водночас залишаючи поза належною увагою управлінський компонент, зокрема форми актів реагування, строки їх прийняття та порядок документування відповідних рішень органами публічної адміністрації;

– відсутність ефективних механізмів оцінки результативності реагування. Хоча передбачено етап аналізу ефективності, він має здебільшого формальний характер, оскільки не супроводжується встановленням чітких показників оцінки (KPI), процедур незалежного аудиту та обов'язкових наслідків за результатами такого аналізу.

7. Узагальнено, що Національний план реагування на кіберінциденти, кібератаки та кіберзагрози не виступає самодостатнім регуляторним інструментом, а радше виконує функцію концептуально-організаційної основи, яка має бути наповнена конкретним юридичним змістом через систему спеціалізованих нормативних актів. Без такого нормативного «доопрацювання» його практична ефективність у сфері діяльності органів публічної адміністрації щодо захисту інформації залишається обмеженою. Тому пропонується, наприклад, прийняття нормативно-правового акту, який би деталізував: 1) алгоритми взаємодії між Державною службою спеціального зв'язку та захисту інформації України, Службою безпеки України, іншими органами виконавчої влади та органами місцевого самоврядування; 2) процедури обміну інформацією (з урахуванням рівнів доступу); 3) порядок спільного прийняття рішень у кризових ситуаціях.

8. З метою підвищення спроможності публічної адміністрації запропоновано запровадити обов'язкові вимоги до кваліфікації керівників з кіберзахисту; визначити систему сертифікації та регулярного підвищення кваліфікації; закріпити стандарти професійної підготовки.

9. Обґрунтовано, що загалом ключовими проблемами у досліджуваній сфері є: розмитість повноважень суб'єктів, відсутність чітких механізмів юридичної відповідальності, недостатній рівень імплементації ризик-орієнтованого підходу, неврегульованість участі приватного сектору, дисбаланс між відкритістю та обмеженням інформації, а також відсутність ефективних механізмів оцінки результативності діяльності публічної адміністрації.

10. Доведено, що сучасні виклики, зокрема кіберзагрози, витоки інформації, дезінформаційні кампанії та цифровізовані форми корупції, потребують комплексного адміністративно-правового реагування із застосуванням як традиційних, так і інноваційних інструментів.

11. Пропонується, щоб подальше удосконалення адміністративного законодавства у сфері діяльності органів публічної адміністрації щодо захисту інформації здійснювалось за кількома взаємопов'язаними напрямами:

– вирішення проблеми фрагментарності правового регулювання, яка проявляється у розпорошеності норм між різними законами та підзаконними актами, чим ускладнює їх застосування та знижує ефективність управлінських рішень. У зв'язку з цим перспективним видається розроблення єдиного комплексного нормативного акта (або пакету взаємоузгоджених актів), який би визначав адміністративно-правові засади функціонування системи захисту інформації, чітко окреслював повноваження суб'єктів та встановлював узгоджені процедури їх взаємодії;

– забезпечення деталізації адміністративних процедур у сфері реагування на кіберзагрози та інциденти, адже чинні акти мають переважно рамковий характер і не містять достатньо чітких алгоритмів дій. Тому необхідним є нормативне закріплення стандартів управлінських рішень, строків їх прийняття, порядку документування та механізмів контролю за їх виконанням. Це дозволить не лише підвищити оперативність реагування, але й забезпечити належний рівень підзвітності органів публічної адміністрації;

– потребує подальшого розвитку інститут юридичної відповідальності у сфері інформаційної безпеки. Відсутність чітко визначених санкцій за порушення вимог щодо захисту інформації, неналежне реагування на кіберінциденти або недотримання процедур обміну інформацією фактично нівелює імперативність відповідних норм. У цьому аспекті доцільним є як удосконалення норм адміністративної та кримінальної відповідальності, так і запровадження спеціальних видів відповідальності для суб'єктів, які забезпечують функціонування критичної інформаційної інфраструктури;

– важливим напрямом є інституційне посилення суб'єктів публічної адміністрації. Йдеться не лише про розширення їх повноважень, але й про забезпечення належного кадрового, технічного та фінансового ресурсу. Без цього навіть найбільш досконалі нормативні моделі залишатимуться

декларативними. Особливу увагу слід приділити розвитку спеціалізованих підрозділів (зокрема CSIRT), підвищенню кваліфікації персоналу та впровадженню сучасних технологій аналізу кіберзагроз;

– подальшого розвитку потребує механізм публічно-приватного партнерства у сфері кібербезпеки. З огляду на те, що значна частина критичної інфраструктури перебуває у приватній власності або експлуатується приватними суб'єктами, ефективна взаємодія між державою та бізнесом є необхідною умовою забезпечення інформаційної безпеки. Відповідно, законодавство має чітко визначати правовий статус таких суб'єктів, їх права, обов'язки та відповідальність, а також гарантії захисту інформації, що передається у межах такої взаємодії;

– актуальним є впровадження сучасних технологічних рішень у правове поле. Зокрема, використання штучного інтелекту, автоматизованих систем моніторингу та аналізу даних має супроводжуватися належним нормативним регулюванням, яке забезпечуватиме баланс між ефективністю кіберзахисту та дотриманням прав і свобод людини.

12. Узагальнено, що вдосконалення адміністративного законодавства у сфері захисту інформації не може обмежуватися точковими змінами. Воно має носити системний характер і передбачати узгоджене реформування нормативної, інституційної та процедурної складових – через узгодження норм різних галузей права, усунення колізій, деталізацію процедур та запровадження нових правових інститутів, адаптованих до умов цифрової трансформації та воєнного стану.

ВИСНОВКИ

У дисертаційному дослідженні здійснено наукове обґрунтування теоретико-методологічних основ та сформульовано практичні рекомендації, спрямовані на вирішення актуальних проблем реалізації адміністративно-правового захисту інформації в Україні. У результаті дисертаційного дослідження сформовано низку висновків і рекомендацій, основними з яких є такі:

1. З’ясовано, що сучасне розуміння інформації еволюціонує від вузького, антропоцентричного підходу до її трактування як фундаментальної характеристики реальності, що забезпечує функціонування та розвиток різних систем. В умовах становлення інформаційного суспільства вона трансформується із допоміжного елемента суспільних відносин у самостійний об’єкт правового захисту, який має комплексний характер. Це обумовлює подвійність її юридичної природи, – з одного боку, інформація виступає об’єктом приватноправових відносин, а з іншого – стратегічним ресурсом держави, що безпосередньо впливає на стан національної безпеки.

2. Визначено, що адміністративно-правовий захист інформації слід розглядати як самостійний різновид діяльності органів публічної адміністрації, спрямований на забезпечення стійкості інформаційного середовища різних рівнів. Його зміст охоплює комплекс нормативних, превентивних, оперативних та відновлювальних інструментів, реалізація яких забезпечує як гарантування інформаційних прав особи, так і захист національних інтересів в інформаційній сфері. Уточнюється, що об’єктами адміністративно-правового захисту виступають усі види інформації, правовий режим доступу до яких визначений чинним законодавством.

3. Обґрунтовано, що суб’єктний склад публічної адміністрації у сфері захисту інформації включає органи стратегічного управління, органи спеціальної та секторальної компетенції, регіональні та місцеві органи, а також інші інституції, наділені публічно-владними або делегованими

повноваженнями. Виявлено, що нормативне закріплення функціональних складових діяльності органів публічної адміністрації у сфері реалізації заходів захисту інформації об'єктивоване через конституційні положення, базові та спеціальні закони, акти стратегічного планування, інституційні, процедурні та контрольно-наглядові акти. Констатується, що у межах таких актів органічно знаходять свій вияв загальні та конкретні правила відповідної діяльності, покликані забезпечити як схоронне функціонування інформаційної сфери, так і сформувати ефективні спеціалізовані механізми реагування на сучасні загрози.

4. Узагальнено, що адміністративно-правовий статус органів публічної адміністрації у сфері захисту інформації більшою мірою характеризується через функціональний компонент, представлений сукупністю цільових орієнтирів їх діяльності, що відображають основне призначення відповідних органів у механізмі забезпечення інформаційної безпеки держави. Йдеться не стільки про формально визначені елементи статусу, скільки про ті напрями публічно-владного впливу, які вони реалізують у процесі виконання покладених на них завдань.

5. Доведено, що повноваження органів публічної адміністрації у сфері захисту інформації зводяться до нормотворчих, контрольних, координаційних, аналітичних та спеціальних. Зауважено, що ключовими з таких є саме останні, адже забезпечують формування та реалізацію державної політики, нормативне регулювання і державний контроль у сфері технічного та криптографічного захисту інформації. Водночас інші суб'єкти, зокрема СБУ, галузеві та інші органи, виконують спеціалізовані або допоміжні функції, що забезпечують практичну реалізацію вимог інформаційної безпеки.

6. Доведено, що відсутність прямої вказівки на необхідність організації та здійснення взаємодії органів публічної адміністрації з іншими суб'єктами у сфері захисту інформації у загальному законодавстві не виключає її фактичного існування та практичної реалізації, оскільки така взаємодія

випливає із системного тлумачення норм права, що регламентують повноваження різних суб'єктів у сфері інформаційної безпеки. Визначено, що провідною особливістю взаємодії органів публічної адміністрації з іншими суб'єктами у сфері захисту інформації є її характер сприяння, який має подвійний юридичний зміст. При цьому сприяння у даному контексті не є пасивною дією, а виступає активним процесом, який включає узгодження процедур, надання необхідних ресурсів, координацію дій та обмін інформацією між усіма уповноваженими, залученими та зацікавленими суб'єктами.

7. Узагальнений досвід США свідчить, що сучасна модель адміністративно-правового захисту інформації має будуватися не лише на імперативному регулюванні, а й на гнучких інструментах взаємодії та локальному регулюванні питань реалізації превентивних заходів та управління ризиками. Водночас важливим є врахування балансу між посиленням кібербезпеки та забезпеченням належного рівня захисту персональних даних громадян. Натомість ЄС має іншу модель регулювання у сфері інформаційної безпеки та захисту даних, що ґрунтується на принципах уніфікації правових стандартів, централізованої гармонізації законодавства держав-членів та пріоритеті захисту прав і свобод людини в цифровому середовищі.

Порівняльний аналіз засвідчив, що обидві моделі мають свої переваги та недоліки. Європейський підхід забезпечує високий рівень захисту прав людини та правову визначеність, тоді як американський – гнучкість, інноваційність і ефективну взаємодію з приватним сектором. Для України доцільним є поєднання елементів обох систем, зокрема: 1) імплементація європейських стандартів захисту персональних даних; 2) запозичення американського досвіду публічно-приватного партнерства; 3) впровадження ризик-орієнтованого підходу до кібербезпеки; 4) посилення інституційної спроможності органів державної влади.

8. Доведено, що сучасний стан адміністративно-правового регулювання діяльності органів публічної адміністрації у сфері захисту інформації характеризується наявністю як концептуально визначених засад, так і істотних структурних та функціональних прогалин. Зауважено, що удосконалення адміністративного законодавства має здійснюватися шляхом системної нормативної конкретизації повноважень і процедур діяльності суб'єктів публічної адміністрації, усунення колізій і дублювання компетенцій, впровадження ризикоорієнтованого підходу до управління кіберзагрозами, нормативного закріплення механізмів координації та взаємодії, а також встановлення чітких підстав і меж юридичної відповідальності за порушення вимог у сфері захисту інформації. Приміром, необхідний акт, який би деталізував: 1) алгоритми взаємодії між Державною службою спеціального зв'язку та захисту інформації України, Службою безпеки України, іншими органами виконавчої влади та органами місцевого самоврядування; 2) процедури обміну інформацією (з урахуванням рівнів доступу); 3) порядок спільного прийняття рішень у кризових ситуаціях.

СПИСОК ВИКОРИСТАНИХ ДЖЕРЕЛ

1. Авер’янов В. Б. Реформування українського адміністративного права: ґрунтовний привід для теоретичної дискусії. *Право України.* 2003. № 5. С. 117–120.

2. Авер’янов В.Б. Адміністративне право України: академічний курс. К.: Юридична думка, 2007. 592 с.

3. Адміністративне право України. Академічний курс: підручник: у 2 т. ред. кол.: В.Б. Авер’янов та ін. Київ: Юрид. думка, 2004. Т. 1: Загальна частина. 2004. 584 с.

4. Александрова М. В. Адміністративно-правове забезпечення інформаційної безпеки у сфері електронного урядування: дис. … доктора філософії 081 «Право». ПрАТ «Вищий навчальний заклад «Міжрегіональна Академія управління персоналом». Київ, 2024. 236 с.

5. Аналітична довідка «Боротьба з корупцією. Роль бізнесу в Україні». К.: ТОВ «Фарбований лист», 2011. 51 с.

6. Аналітичний звіт про кібератаку на «Укренерго» у грудні 2022 року. Київ: ДССЗЗІ, 2023. URL: https://cip.gov.ua/ua/news/analitichniy-zvit-pro-kiberataku-na-ukrenergo

7. Армаш Н. О. Керівник органу виконавчої влади: адміністративно-правовий статус. Запоріжжя: ГУ «ЗІДМУ», 2006. 248 с.

8. Бабенко К.А. Права людини як об’єкт конституційного захисту. URL: https://6aas.gov.ua/ua/proekty/articles/b/256-prava-lyudini-yak-ob-ekt-konstitutsijnogo-zakhistu.html

9. Базалук Е. О. Юридико-психологічний механізм допомоги та захисту жінок і дівчат, які постраждали від насильства під час збройних конфліктів: дис. … доктора філософії 081 «Право». НДІПП. Київ, 2024. 262 с.

10. Баран М. В. Адміністративно-правове забезпечення інформаційної безпеки в Україні: дис: … доктора філософії 081 «Право». Львівський державний університет внутрішніх справ. Львів, 2022. 244 с.

11. Батіщев С.О. Адміністративно-правовий захист інформації: теоретико-правовий аналіз. *Вісник Одеського національного університету. Правознавство*. 2025. Т. 27. №. 2(41). С. 12–16.

12. Батіщев С. О. Захист інформації через призму адміністративного законодавства України. *Актуальні проблеми імплементації наукових досягнень у практичну діяльність*: матеріали міжнародної науково-практичної конференції (м. Київ, 4–5 червня 2024 р.). Київ: Науково-дослідний інститут публічного права, 2024. С. 98–100.

13. Батіщев С. Інформація та публічна адміністрація: точки перетину. *Інноваційні підходи до реформування сучасного законодавства:* матеріали міжнародної науково-практичної конференції (м. Київ, 20–21 квітня 2023 р.). Київ: Науково-дослідний інститут публічного права, 2023. С. 44–46.

14. Батіщев С. Категорійно-поняттєва визначеність правового концепту «адміністративно-правовий статус органів публічної адміністрації» на прикладі сфери захисту інформації. *Актуальні питання розвитку правової системи в сучасній Україні:* Міжнародна науково-практична конференція. Науково-дослідний інститут публічного права (Львів–Торунь, 4 лютого 2025 р.). Львів–Торунь: Liha-Pres, 2025. С. 26–28.

15. Батіщев С.О. Інформація як об’єкт правового захисту. *Право і суспільство*. 2023. № 3. С. 638–642.

16. Бєлєвцева В.В. Адміністративно-правовий захист інформації з обмеженим доступом: визначення та удосконалення. *Інформація і право.* 2016. № 2 (17). С. 127–133.

17. Битяк Ю.П. Адміністративне право України. Харків: Право, 2012. 528 с.

18. Білоглазова Н., Галунько В, Короєд С. Адміністративно-правовий статус центральних банків країн-учасниць Європейського Союзу: монографія. Херсон: Грінь Д.С., 2015. 176 с.

19. Борисов В.І, Пащенко О.О. Щодо розуміння доктринальної концепції «безпека – стан захищеності». *Вісник Асоціації кримінального права України.* 2020. № 1(13). С. 126–144.

20. Бочкова І. І. Інформація як об'єкт правового регулювання. *Науковий вісник Ужгородського національного університету.* Серія: Право. 2022. Вип. 74(1). С. 88–92.

21. Бригінець О.О. Адміністративно-правовий статус Державної податкової служби України: дис. ... канд. юрид. наук: 12.00.07. Ірпінь, 2011. 220 с.

22. Вавринчук М.П., Когут О.В. Інформаційна безпека держави. *Правові засади організації та здійснення публічної влади:* зб. тез II Всеукр. наук.-практ. інтернет-конф. (м. Хмельницький, 2–8 травня 2019 р.). Хмельницький : ХУУП, 2019. С. 37–40.

23. Веклич Є. Рада національної безпеки і оборони України: загальна
характеристика. URL: https://elar.navs.edu.ua/server/api/core/bitstreams/e98bbb59-83bc-4d4f-80c3-093a3d0e6ecc/content

24. Великий енциклопедичний юридичний словник; за редакцією акад. НАН України Ю.С. Шемшученка. К.: ТОВ «Вид-во «Юридична думка», 2007. 992 с.

25. Великий тлумачний словник сучасної української мови (з дод. і допов.); уклад. і голов. ред. В. Т. Бусел. Київ ; Ірпінь : ВТФ «Перун», 2005. 1728 с.

26. Виконавча влада і адміністративне право; за заг. ред. В. Авер'янова. К.: Видавничий Дім «Ін-Юре», 2002. 668 с.

27. Вишнева А. В. Адміністративно-правовий статус органів суддівського врядування в Україні: дис. ... канд. юрид. наук: 12.00.07. Науково-дослідний інститут публічного права, 2021. 218 с.

28. Габро І., Цимбалюк І. Співробітництво України та НАТО в сфері інформаційної безпеки. Важливість євроатлантичної інтеграції у створенні в Україні системи колективної безпеки та оборони під час гібридної війни з Російською Федерацією: колективна монографія. Заг. ред. М. О. Багмета, С.Ф. Джерджа, В. М. Ємельянова. Миколаїв : Вид-во ЧНУ ім. Петра Могили, 2017. С. 28–34.

29. Гарбузюк К.Г. До проблеми співвідношення термінів «адміністративно-правова охорона» й «адміністративно-правовий захист». *Сучасні проблеми правового, економічного та соціального розвитку держави.* Харків, 2019. С. 38–40.

30. Гіжевський В., Головко В., Ковальський В., та ін. Популярна юридична енциклопедія. К. : Юрінком Інтер, 2003. 528 с.

31. Гончаров М. В. Теоретико-правові основи регулювання інформаційної безпеки в Україні: дис: … доктора філософії 081 «Право». Державний податковий університет, Міністерство фінансів України. Ірпінь, 2023. 214 с.

32. Горулько В. Основні напрями удосконалення законодавства України з інформаційної безпеки в умовах війни. *Науковий вісник Ужгородського Національного Університету*. 2025. Серія ПРАВО. Випуск 88. Ч. 2. С. 364–370.

33. Григоренко В. А. Найкращі зарубіжні практики розбудови механізмів державно-приватного партнерства у сфері кібербезпеки. *Державне управління: удосконалення та розвиток.* 2021. № 2 (37). С. 155–161.

34. Грубов В. Філософія інформації: у пошуках нової онтології. *Вісник Київського національного торговельно-економічного університету.* 2016. № 2. С. 16–29.

35. Гуз А.М., Шепета О.В. Діалектичні питання взаємодії суб’єктів охорони державної таємниці та технічного захисту інформації. *Державна політика України у сфері забезпечення інформаційної безпеки людини*, суспільства, держави. 2012. № 3(10). С. 29–33.

36. Гуржій Т. О. Актуальні проблеми державного контролю. *Адміністративне право та процес*. 2012. № 1. С. 78–88.

37. Державне будівництво і місцеве самоврядування в Україні: підручник для студентів вищих навчальних закладів; за ред. С.Г. Серьогіної. Харків : Право, 2005. 256 с.

38. Державно-приватне партнерство у сфері кібербезпеки: міжнародний досвід та можливості для України: аналітична доповідь; за заг. ред. Д. Дубова. Київ: НІСД, 2018. 84 с.

39. Держспецзв'язку затвердила Методичні рекомендації щодо реагування суб’єктами забезпечення кібербезпеки на різні види подій у кіберпросторі. URL: https://cybersec.net.ua/normatyvni-dokumenty/568-derzhspetszviazku-zatverdyla-metodychni-rekomendatsii-shchodo-reahuvannia-subiektamy-zabezpechennia-kiberbezpeky-na-rizni-vydy-podii-u-kiberprostori.html

40. Деякі питання електронної ідентифікації та електронних довірчих послуг: Постанова Кабінету Міністрів України від 28.06.2024 № 764. Верховна Рада України. Законодавство України. URL: https://zakon.rada.gov.ua/laws/show/764-2024-%D0%BF/ed20240628#n472

41. Деякі питання захисту інформаційних, електронних комунікаційних, інформаційно-комунікаційних, технологічних систем: Постанова Кабінету Міністрів України від 18.06.2025 № 712. Верховна Рада України. Законодавство України. URL: https://zakon.rada.gov.ua/laws/show/712-2025-%D0%BF#Text

42. Деякі питання реагування на кіберінциденти, кібератаки та кіберзагрози: Постанова Кабінету Міністрів України від 26.11.2025 № 1533.

Верховна Рада України. Законодавство України. URL: https://zakon.rada.gov.ua/laws/show/1533-2025-%D0%BF#Text

43. Дзьобань О. П. Інформаційна безпека у проблемному полі соціо-культурної реальності: монографія. Х.: Майдан, 2010. 260 с.

44. Директива (ЄС) 2017/2397 Європейського Парламенту і Ради від 12 грудня 2017 року про визнання професійних кваліфікацій у внутрішньому судноплавстві та про скасування директив Ради 91/672/ЄЕС та 96/50/ЄС: Міжнародний документ від 12.12.2017 № 2017/2397. Верховна Рада України. Законодавство України. URL: https://zakon.rada.gov.ua/laws/term/12906

45. Дідич О. Р., Наумко О. М. Державно-приватне партнерство у забезпеченні національної безпеки в умовах повномасштабного вторгнення. *Публічне адміністрування та національна безпека.* 2023. № 2. С. 118–123.

46. Дмитренко М. А. Проблемні питання інформаційної безпеки України. 2018. URL: journals.iir.kiev.ua/index.php/pol_n/article/ download/3318/2997

47. Дніпров О.С. Компетенція як елемент правового статусу органів виконавчої влади. В*існик Національного університету «Львівська політехніка».* Серія «Юридичні науки». 2017. № 861. С. 257–262.

48. Додіна Є.Є. Адміністративно-правовий статус громадських організацій в Україні: автореф. дис... канд. юрид. наук: 12.00.07; Одес. нац. юрид. акад. О., 2002. 21 с.

49. Дрозд О. Ю., Сорока Л. В., Миськів Л. І. Загальнотеоретичні основи концепту «адміністративно-правовий статус державної служби» з оглядом його особливостей на прикладі органів державної виконавчої служби. *Юридичний науковий електронний журнал.* 2023. № 5. С. 506–508.

50. Дубас О. П. Інформаційний розвиток сучасної України у світовому контексті: Монографія. Київ. 2004. 208 с.

51. Дубов Д.В. Державна інформаційна політика України в умовах гібридного миру та війни. *Стратегічні пріоритети.* 2016. № 3. С. 86–93.

52. Єщук О. М. Адміністративно-правова охорона і адміністративно-правовий захист: ціле і частка. *Закон і життя*. 2013. С. 49–53.

53. Жук Т. Адміністративно-правові засади забезпечення взаємодії контррозвідувальних органів з іншими суб'єктами сектору безпеки з метою охорони національних інтересів: дис. ... канд. юрид. наук: 12.00.07. НДІПП. Київ, 2021. 230 с.

54. Жук Т. Взаємодія контррозвідувальних органів з іншими суб'єктами сектору безпеки у сфері охорони національних інтересів: аналіз термінології законодавства. *Перспективні напрямки розвитку юридичної науки у XXI сторіччі:* матеріали міжнародної науково-практичної конференції (м. Київ, 17–18 лютого 2021 р.). Київ: Науково-дослідний інститут публічного права, 2021. С. 40–43

55. Замрига А. В. Адміністративно-правове забезпечення господарської діяльності в Україні. Теорія і практика: монографія. ОЛДІ+. 2020. 374 с.

56. Заскока Ю. В. Державно-приватне партнерство в сфері кібербезпеки України: стан та проблеми забезпечення. *Наукові перспективи.* 2021. № 9 (21). С. 85–98.

57. Звіт про співпрацю України з Microsoft у сфері кібербезпеки за 2022 рік. Київ: Мінцифри, 2023. URL: https://thedigital.gov.ua/news/zvit-pro-spivpratsyu-z-microsoft-2022

58. Звіт Центру стратегічних комунікацій та інформаційної безпеки за 2023 рік. Київ: ЦСКІБ, 2023. URL: https://spravdi.gov.ua/zvit-za-2023-rik.

59. Золотар О. О. Генеза суспільних відносин щодо інформаційної безпеки людини. *Інформація і право.* 2018. № 1 (24). С. 139–148.

60. Зубко А. Адміністративно-правовий статус Департаменту міжнародних спорів Міністерства юстиції України : дис. ... канд. юрид. наук : 12.00.07. Науково-дослідний інститут публічного права. Київ, 2019. 211 с.

61. Інші органи виконавчої влади. Державні сайти України. URL: https://www.kmu.gov.ua/catalog

62. Карпенко В. О. Інформаційна політика та безпека. К.: Нора-Друк, 2006. 320 с.

63. Карпенко М. М. Адміністративно-правовий статус органів Служби безпеки України. *Вісник Харківського національного університету внутрішніх справ.* 2014. № 4 (67). С. 137–148.

64. Кваша О.О. Зміст і значення понять «взаємодія» та «система» у філософських і правових досліджень. *Держава і право.* 2012. Вип. 56. С. 32–38.

65. Кодекс адміністративного судочинства України: Закон України від 06.07.2005 № 2747-IV. Верховна Рада України. Законодавство України. URL: https://zakon.rada.gov.ua/laws/show/2747-15#Text

66. Кожура Л.О. Адміністративно-правовий захист та охорона: поняття та співвідношення. *Науковий вісник Ужгородського національного університету.* 2015. Серія ПРАВО. Вип. 35. Ч. І. Т. 2. С. 119–122.

67. Козаченко Г.В. Економічні інтереси як об’єкт захисту. *Фінансова безпека в системі забезпечення національних економічних інтересів: проблеми і перспективи:* Матеріали IV Міжнародної науково-практичної конференції (м. Полтава, 26 – 28 травня 2016 р.) Полтава: ПолтНТУ, 2016. С. 12–13.

68. Колодій А., Копєйчиков В. Загальна теорія держави і права: навч. посібник. Національний педагогічний ун-т ім. М.П.Драгоманова. Київ: Юрінком Інтер. 1998. 317 с.

69. Коломоєць Т. О. Адміністративне право України. Академічний курс: підручник. Київ: Юрінком Інтер, 2011. 576 с.

70. Кондрацький Ю. М. Адміністративно-правовий статус керівника територіального органу Національної поліції як суб’єкта контролю: дис. канд.. юрид. наук: 12.00.07. Харківський національний університет внутрішніх справ. Харків. 239 с.

71. Комова М.В., Пелещишин А.М. Концепти філософії інформації Лучано Флоріді. *Вісник Харківської державної академії культури.* 2019. № 55. С. 16–25.

72. Конституція України: Закон України від 28.06.1996 № 254к/96-ВР. Верховна Рада України. Законодавство України. URL: https://zakon.rada.gov.ua/laws/show/254%D0%BA/96-%D0%B2%D1%80#Text

73. Корж І.Ф. Державна безпека: методологічні підходи до системи складових поняття. *Правова інформатика.* 2012. № 4 (36). С. 69–75.

74. Кормич Б.А. Інформаційне право. Підручник. Харків: БУРУН. К, 2011. 334 с.

75. Коротун О. М. Адміністративно-правовий статус суб'єктів публічної адміністрації, що забезпечують охорону прав інтелектуальної власності. *Вісник НТУУ «КПІ».* Політологія. Соціологія. Право. 2019. Вип. 4(44). С. 114–118.

76. Костенко І.В., Левченко Д.С., Оксінь В.Ю. Державно-приватне партнерство у сфері кібербезпеки як інструмент забезпечення національної безпеки: адміністративно-правовий аспект. *Наука і техніка сьогодні.* 2025. № 11(52). С. 175–188.

77. Кохановська О.В. Інформація як нематеріальне благо та захист інформаційних прав згідно з Цивільним кодексом України. URL: https://www.viaduk.net/clients/vsu/vsu.nsf/(documents)/6700A809B011484FC2257B7B004D77FF

78. Коцовська О. Л. Зміст та сутнісні ознаки адміністративно-правової охорони прав споживачів. *Держава і право.* 2011. Вип. 54. С. 270–277.

79. Кочман К., Форос Г. Шляхи удосконалення адміністративного законодавства у сфері адміністративно-правового регулювання забезпечення протидії кіберзагрозам. *Юридичний вісник.* 2025. № 5. С. 97–104.

80. Кочубей Л. Інформаційна безпека держави: напрями й інструменти захисту українського інформаційного поля. URL: https://ipiend.gov.ua/wp-content/uploads/2018/07/kochubei_informatsiina-1.pdf

81. Кошиков Д. Сутність правових засад реалізації державної політики у сфері забезпечення економічної безпеки держави. *Вісник Пенітенціарної асоціації України*. 2020. № 1(11). С. 164–175.

82. Кравченко В.В. Конституційне право України : навч. посіб. 2-е вид. Київ: Атіка, 2002. 480 с.

83. Кузнецова Н.С. Концептуальні засади інституту юридичної особи в новому цивільному законодавстві. *Проблеми державоутворення і захисту прав людини в Україні:* Матеріали VIII регіональної науково-практичної конференції. Львів, 2002. С. 215–216.

84. Кузьменко О.В. Адміністративне право України. К.: Алерта, 2019. 408 с.

85. Лебідь Н.В. Адміністративно-правовий статус державних інспекцій в Україні: автореф. дис... канд. юрид. наук: 12.00.07; Нац. ун-т внутр. справ. Х., 2004. 20 с.

86. Левченко Д. Парадигма ідеї глобального цифрового врядування як явища адміністративного права. *Адміністративне право і процес.* 2024. № 4. С. 5–13.

87. Логінова Н.І., Дробожур Р.Р. Правовий захист інформації: Навчальний посібник. Одеса: Фенікс, 2015. 264 с.

88. Лужецький В.А., Северин Л.І., Гульчак Ю.П., А.Д. Кожухівський Л. Основи організаційного захисту інформації. Навчальний посібник. Вінниця: ВНТУ, 2005. 148 с.

89. Лукашевич В. Г. До визначення поняття «інформація», що вживається в сучасному юридичному обігу. *Вісник ЗЮІ МВС України.* 1998. № 3. С. 263–268.

90. Лукашевич М., Туленков М. Соціологія. Загальний курс. Навчальний посібник. К.: Каравела, 2006. 408 с.

91. Майоров В. В. До питання співвідношення понять «компетенція» та «повноваження» Національної поліції України. *Право та державне управління.* 2020. № 1. Т. 1. С. 85–89.

92. Мелеганич Г. І. Суспільна безпека в Україні: теоретичний та практичний аспекти. *Політичне життя.* 2019. № 4. С. 39–44.

93. Михайловська О. В. Наукові підходи до розуміння сутності поняття «взаємодія» в системі «влада-громадськість». *Проблеми сучасних трансформацій.* 2021. № 2. С. 71–75.

94. Мозговий О.О. Повноваження суб'єктів формування та реалізації державної політики у сфері земельних відносин. *Європейські перспективи.* 2025. № 3. С. 438–445.

95. Мохова Ю. Л., Луцька А. І. Сутність та головні напрямки державної інформаційної політики України. *Державне управління: удосконалення та розвиток.* 2018. № 12. URL: http://nbuv.gov.ua/UJRN/Duur_2018_12_15

96. Никитченко Н. В. До питання відповідальності органів влади. *Міжнародний юридичний вісник: актуальні проблеми сучасності (теорія та практика).* 2017. Вип. 1. С. 186–190.

97. Новий тлумачний словник української мови: у 4 т. Т. 3: Обе - Роб; уклад.: В. Яременко, О. Сліпушко. К. : Аконіт, 1998. 928 с.

98. Нові умови передачі персональних даних в США та за межі ЄС в 2020 році. URL: https://bsoprivacygroup.com/ru/gdpr-transfer-data-shrems/

99. Обрусна С.Ю., Іванова І.В., Панімаш Ю.В., Пасинчук К.М. Адміністративно-правовий статус органів публічної адміністрації військово-цивільного характеру як суб'єктів публічного управління. *Науковий вісник Ужгородського Національного Університету*. 2023. Серія ПРАВО. Вип. 78. Ч. 2. С. 90–95.

100. Огурченко В.Г. Адміністративно-правовий статус Національної поліції України як провідного суб'єкта реалізації оперативно-розшукової функції: теоретико-правовий аналіз. *Юридичний науковий електронний журнал.* 2023. № 11. С. 398–401.

101. Огурченко В.Г. Дослідження структурних елементів адміністративно-правового статусу Національної поліції України як провідного суб'єкта реалізації оперативно-розшукової функції. *Вчені записки ТНУ імені В.І. Вернадського.* Серія: юридичні науки. 2023. № 5. Т. 34 (73). С. 46–52.

102. Оксінь В.Ю., Левченко Д.С., Костенко І.В. Кібербезпека держави як інструмент сталого розвитку цифрового середовища. *Електронне наукове видання «Аналітично-порівняльне правознавство».* 2025. Вип. 6. Ч. 2. С. 411–415.

103. Омелько І.І. Конституційно-правовий статус Ради національної безпеки і оборони України. *Електронне наукове видання «Аналітично-порівняльне правознавство».* 2023. № 5. С. 166–170.

104. Органи виконавчої влади: питання компетенції: монографія. Київ: КНЕУ, 2012. 255 с.

105. Організаційно-правові основи захисту інформації з обмеженим доступом: навч. посіб. А. Б. Тоцький, О. І. Тимошенко, А. М. Гуз та ін. Київ: Європейський університет, 2006. 232 с.

106. Орзіх М.П. Конституційне право України. Одеса: Юридична література, 2003. 512 с.

107. Орлов П. І. Інформація як об'єкт правового і технічного захисту. *Вісник Харківського національного університету внутрішніх справ.* 2000. № 12 (2). С. 146–151.

108. Особиста безпека та застосування сили: Частина 1. Фундаментальні питання теорії та практики особистої безпеки особового складу Державної прикордонної служби України: навч. посіб. Хмельницький: Видавництво НАДПСУ, 2012. 348 с.

109. Панфілов О., Калімбет А. Адміністративно-правовий статус Кабінету Міністрів України: характеристика поняття та змісту. *Прикарпатський юридичний вісник*. 2021. № 2 (37). С. 79–83.

110. Пашкова В. С. Інформаційна політика і бібліотека. *Бібліотека і влада*. Київ. 2000. С. 4–16.

111. Перун Т. С. Адміністративно-правовий механізм забезпечення інформаційної безпеки в Україні: дис... канд. юр. наук: 12.00.07. Національний університет «Львівська політехніка», Львів, 2019. 268 с.

112. Петрик В.М. Сутність інформаційної безпеки держави, суспільства та особи. *Юридичний журнал.* 2009. № 5. С. 12–17.

113. Петров Є. В. Інформація як об'єкт правовідносин. Вісник *Харківського національного університету внутрішніх справ.* 2001. № Спец. вип. С. 249–252.

114. Петров С. Г. Правові основи взаємодії державних органів та приватних суб'єктів із метою захисту електронних інформаційних ресурсів України. *Інформація і право.* 2019. № 4 (31). С. 107–113.

115. Петров С. Г. Корупційні правопорушення, пов'язані з розбудовою системи обігу державних електронних інформаційних ресурсів. *Запобігання корупції у приватному секторі:* матеріали наук.-практ. онлайн «круглого столу», присвяч. 25-річчю із дня створення НДІ вивчення проблем злочинності та 95-річчю із дня народж. акад. Володимира Сташиса (м. Харків, 1 лип. 2020 р.). М-во освіти і науки України, Нац. юрид. ун-т ім. Ярослава Мудрого, Нац. акад. прав. наук України, НДІ вивч. проблем злочинності ім. акад. В. В. Сташиса НАПрН України. Харків: Право, 2020. С. 119–121.

116. Питання Міністерства цифрової трансформації: Постанова Кабінету Міністрів України від 18.09.2019 № 856. Верховна Рада України. Законодавство України. URL: https://zakon.rada.gov.ua/laws/show/856-2019-%D0%BF#Text

117. Питання Центру протидії дезінформації: Указ Президента України від 07.05.2021 № 187/2021. Верховна Рада України. Законодавство України. URL: https://zakon.rada.gov.ua/laws/show/187/2021#Text

118. Подоляка А. М. Взаємодія державних органів в охороні громадського порядку. *Форум права. 2009*. № 2. С. 338–344.

119. Подоляка С. Адміністративно-правовий статус суб'єктів протидії корупції в органах прокуратури в Україні. *Форум права.* 2017. № 3. С. 160–165.

120. Популярна юридична енциклопедія; кол. авт.: В.Г. Гіжевський, В.В. Головченко, В.С. Ковальський (кер.) та ін. Київ: Юрінком Інтер, 2002. 528 с.

121. Порядок проведення огляду громадської безпеки та цивільного захисту Міністерством внутрішніх справ: Постанова Кабінету Міністрів України від 22.05.2019 № 507. Верховна Рада України. Законодавство України. URL: https://zakon.rada.gov.ua/laws/show/507-2019-%D0%BF

122. Порядок створення та припинення юридичних осіб згідно норм чинного законодавства України: Методичні рекомендації Старосинявського районного управління юстиції. URL: https://justice-km.gov.ua/uploads/files/stv%20i%20pryp%20yur%20os.doc

123. Потіп М.М. Щодо сутності компетенції органів державної виконавчої влади та місцевого самоврядування. *Право і суспільство.* 2012. № 6. С. 32–35.

124. Почепцов Г. Г., Чукут С. А. Інформаційна політика: навч. посіб. Київ. 2006. 663 с.

125. Приходько А.А. Адміністративно-правове забезпечення запобігання та протидія корупції в Україні за умов євроінтеграції: дис... д-ра юрид. наук. Дніпро, 2020. 485 с.

126. Приходько А.А. Адміністративно-правовий статус суб'єктів публічної адміністрації у сфері запобігання та протидії корупції: теоретична

та практична сутність. *Наукові праці Національного університету «Одеська юридична академія».* 2019. № 24. С. 88–96.

127. Про визнання таким, що втратив чинність, наказу Адміністрації Державної служби спеціального зв'язку та захисту інформації України від 16 травня 2007 року № 87: Наказ АдміністрацІЇ Держспецзв'язку від 08.04.2021 № 214. Верховна Рада України. Законодавство України. URL: https://zakon.rada.gov.ua/laws/show/z0555-21

128. Про Держспецзв'язку. URL: https://cip.gov.ua/ua/statics/pro-derszhpeczv-yazku

129. Про Державну службу спеціального зв'язку та захисту інформації України: Закон України від 23.02.2006 № 3475-IV. Верховна Рада України. Законодавство України. URL: https://zakon.rada.gov.ua/laws/show/3475-15/ed20221205#Text

130. Про державну таємницю: Закон України від 21.01.1994 № 3855-XII Верховна Рада України. Законодавство України. URL: https://zakon.rada.gov.ua/laws/show/3855-12#Text

131. Про додержання прав людини під час проведення оперативно-технічних заходів: Указ Президента України від 7 листопада 2005 р. № 1556/2005. Верховна Рада України. Законодавство України. URL: https://zakon.rada.gov.ua/laws/show/1556/2005#Text

132. Про доступ до публічної інформації: Закон України від 13.01.2011 № 2939-VI. Верховна Рада України. Законодавство України. URL: https://zakon.rada.gov.ua/laws/show/2939-17#Text

133. Про електронні документи та електронний документообіг: Закон України від 22.05.2003 № 851-IV. Верховна Рада України. Законодавство України. URL: https://zakon.rada.gov.ua/laws/show/851-15#Text

134. Про затвердження Вимог до авторизованої електронної системи: Рішення НКЦПФР від 30.12.2021 № 1310. Верховна Рада України. Законодавство України. URL:https://zakon.rada.gov.ua/laws/show/z0077-22/ed20230512#Text

135. Про затвердження Державного стандарту початкової загальної освіти: Постанова Кабінету Міністрів України від 20.04.2011 № 462. Верховна Рада України. Законодавство України. URL: https://zakon.rada.gov.ua/laws/show/462-2011-%D0%BF/ed20110510/find?text=%CA%EE%EC%EF%E5%F2%E5%ED%F6%B3%FF#Text

136. Про затвердження Інструкції з технічного забезпечення засобами технічного захисту інформації і комплексами технічного контролю Національної гвардії України: Наказ МВС України від 27.07.2015 № 906 Верховна Рада України. Законодавство України. URL: https://zakon.rada.gov.ua/laws/show/z0999-15#n13

137. Про затвердження Інструкції про порядок взаємодії між Державною службою спеціального зв'язку та захисту інформації України і Державною службою України з надзвичайних ситуацій з питань забезпечення урядовим зв'язком спеціальної Урядової комісії з ліквідації наслідків надзвичайної ситуації: Наказ Адміністрації Держспецзв'язку та МВС України від 10.11.2014 № 599/1198. Верховна Рада України. Законодавство України. URL: https://zakon.rada.gov.ua/laws/show/en-ro/z1493-14?lang=uk#Text

138. Про затвердження Інструкції про порядок здійснення Службою безпеки України контролю за додержанням порядку обліку, зберігання і використання документів та інших [...]: наказ Служби безпеки України від 18.08.2017 № 471 Верховна Рада України. Законодавство України. URL: https://zakon.rada.gov.ua/laws/main/z1127-17

139. Про затвердження Ліцензійних умов провадження господарської діяльності з надання послуг з охорони власності та громадян: Наказ МВС України від 14.12.2004 № 145/1501 (Втрата чинності від 11.01.2010). Верховна Рада України. Законодавство України. URL: https://zakon.rada.gov.ua/laws/show/en-ro/z1678-04/ed20100111/find?lang=uk#Text

140. Про затвердження Мінімальних вимог до захисту інформаційних, електронних комунікаційних, інформаційно-комунікаційних та технологічних систем: Постанова Кабінету Міністрів України від 29.03.2006 № 373. Верховна Рада України. Законодавство України. URL: https://zakon.rada.gov.ua/laws/show/373-2006-%D0%BF#Text

141. Про затвердження Положення про Адміністрацію Державної служби спеціального зв'язку та захисту інформації України: Постанова Кабінету Міністрів України від 03.09.2014 № 411. Верховна Рада України. Законодавство України. URL: https://zakon.rada.gov.ua/laws/show/411-2014-%D0%BF#n8

142. Про затвердження Положення про державний контроль за станом технічного захисту інформації: Наказ Адміністрації Держспецзв'язку від 16.05.2007 № 87. Верховна Рада України. Законодавство України. URL: https://zakon.rada.gov.ua/laws/show/z0785-07#Text

143. Про затвердження Положення про контроль за станом технічного захисту інформації в органах і підрозділах Національної поліції України: Наказ МВС України від 29.02.2016 № 139. Верховна Рада України. Законодавство України. URL: https://zakon.rada.gov.ua/laws/show/z0431-16#n13

144. Про затвердження Положення про організаційно-технічну модель кіберзахисту: Постанова Кабінету Міністрів України від 29.12.2021 № 1426. Верховна Рада України. Законодавство України. URL: https://zakon.rada.gov.ua/laws/show/1426-2021-%D0%BF#n9

145. Про затвердження Порядку оцінки стану захищеності державних інформаційних ресурсів в інформаційних, електронних комунікаційних та інформаційно-комунікаційних [...]: наказ Адміністрації Держспецзв'язку від 02.12.2014 № 660. Верховна Рада України. Законодавство України. URL: https://zakon.rada.gov.ua/laws/show/z0090-15#Text

146. Про затвердження Порядку та умов виплати надбавки за особливий характер роботи працівникам Державної служби спеціального зв'язку та захисту інформації України, які [...]: наказ Адміністрації Держспецзв’язку від 30.08.2018 № 527. Верховна Рада України. Законодавство України. URL: https://zakon.rada.gov.ua/laws/show/z1061-18#n14

147. Про затвердження Порядку формування програми робіт із стандартизації криптографічного та технічного захисту інформації, кіберзахисту, протидії технічним розвідкам, [...]: наказ Адміністрації Держспецзв’язку від 16.12.2025 № 832. Верховна Рада України. Законодавство України. URL: https://zakon.rada.gov.ua/laws/show/z0147-26#Text

148. Про захист економічної конкуренції: Закон України від 11.01.2001 № 2210-III. Верховна Рада України. Законодавство України. URL: https://zakon.rada.gov.ua/laws/show/2210-14/ed20220507#Text

149. Про захист інформації в інформаційно-комунікаційних системах: Закон України від 05.07.1994 № 80/94-ВР. Верховна Рада України. Законодавство України. URL: https://zakon.rada.gov.ua/laws/show/80/94-%D0%B2%D1%80#Text

150. Про захист персональних даних: Закон України від 01.06.2010 № 2297-VI. Верховна Рада України. Законодавство України. URL: https://zakon.rada.gov.ua/laws/show/2297-17#Text

151. Про інформацію: Закон України від 02.10.1992 № 2657-XII. Верховна Рада України. Законодавство України. URL: https://zakon.rada.gov.ua/laws/show/2657-12#Text

152. Про Кабінет Міністрів України: Закон України від 27.02.2014 № 794-VII. Верховна Рада України. Законодавство України. URL: https://zakon.rada.gov.ua/laws/show/794-18#Text

153. Про Національний координаційний центр кібербезпеки: Указ Президента України від 07.06.2016 № 242/2016. Верховна Рада України.

Законодавство України. URL: https://zakon.rada.gov.ua/laws/show/242/2016#Text

154. Про основні засади забезпечення кібербезпеки України: Закон України від 05.10.2017 № 2163-VIII. Верховна Рада України. Законодавство України. URL: https://zakon.rada.gov.ua/laws/show/2163-19#Text

155. Про Положення про проходження військової служби (навчання) військовослужбовцями Державної служби спеціального зв'язку та захисту інформації України: Указ Президента України від 31.07.2015 № 463/2015. Верховна Рада України. Законодавство України. URL: https://zakon.rada.gov.ua/laws/show/463/2015#n10

156. Про Положення про технічний захист інформації в Україні: Указ Президента України від 27.09.1999 № 1229/99. Верховна Рада України. Законодавство України. URL: https://zakon.rada.gov.ua/laws/show/uk-hu/1229/99/ed20080504/find?text=%C4%EE%F1%F2%F3%EF%ED%B3%F1%F2%FC#Text

157. 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. Верховна Рада України. Законодавство України. URL: https://zakon.rada.gov.ua/laws/show/685/2021#Text

158. Про Службу безпеки України: Закон України від 25.03.1992 № 2229-XII. Верховна Рада України. Законодавство України. URL: https://zakon.rada.gov.ua/laws/show/2229-12#Text

159. Про статус ветеранів війни, гарантії їх соціального захисту: Закон України від 22.10.1993 № 3551-XII. Верховна Рада України. Законодавство України. URL: https://zakon.rada.gov.ua/laws/show/3551-12#Text

160. Про центральні органи виконавчої влади: Закон України від 17.03.2011 № 3166-VI. Верховна Рада України. Законодавство України. URL: https://zakon.rada.gov.ua/laws/show/3166-17#Text

161. Публічна адміністрація (система урядування) в Україні. URL: https://pravo.org.ua/publichna-administratsiya-systema-uryaduvannya-v-ukrayini/

162. Пугачов О. Зарубіжний досвід забезпечення інформаційної безпеки держави. Problems of Modern Transformations. Series: Law, Public Management and Administration. DOI: https://doi.org/10.54929/2786-5746-2024-13-02-07

163. Пугачов О. І. Удосконалення державних механізмів забезпечення інформаційної безпеки України. Дис. на здобуття наукового ступеня доктора філософії з галузі знань «Публічне управління та адміністрування» за спеціальністю 281«Публічне управління та адміністрування», Київ, 2025. 242 с.

164. РБК-Україна. Глава Євроради розповів про прогрес українського питання в НАТО. 23 листопада 2024. URL: https://www.rbc.ua/rus/news/glava-evroradirozpoviv-progres-ukrayinskogo-1700764510.html

165. Рішення № 125202700, 17.02.2025, Київський окружний адміністративний суд. URL: https://youcontrol.com.ua/catalog/court-document/125202700/

166. Росляков О. В. Адміністративно-правові засади здійснення державного контролю за діяльністю органів і посадових осіб місцевого самоврядування: дис. ... канд. юрид. наук: 12.00.07. НДІПП. Київ, 2025. 206 с.

167. Ртищева Т. О. Адміністративно-правовий статус помічника-консультанта народного депутата України: дис. ... канд. юрид. наук: 12.00.07. Науково-дослідний інститут публічного права. Київ, 2018. 220 с.

168. Савосько Т.О. Зміст та функції поняття державної інформаційної політики. *Вчені записки ТНУ імені В.І. Вернадського.* Серія: Публічне управління та адміністрування. 2024. Том 35 (74) № 1. С. 28–32.

169. Садова А. Ю. Проблема визначення основних ознак сучасної держави. URL: https://elar.navs.edu.ua/bitstreams/112de8c2-3e0e-4e56-8c99-69099c674976/download

170. Санакуєв М. Філософія інформації та філософські основи інформатики. *Інтегровані комунікації.* 2016. № 2. С. 91–96.

171. Сікорський О.П. Поняття концепції органу виконавчої влади. Гуманіт. вісн. НУК. Миколаїв: НУК, 2012. Вип. 5. С. 52–54.

172. Скакун О.Ф. Теорія держави і права : підручник. Харків: Консум, 2005. 656 с.

173. Скочиляс-Павлів О.В. Сучасні загрози інформаційній безпеці України в умовах правового режиму воєнного стану. *Юридичний науковий електронний журнал.* 2023. № 9. С. 263–266.

174. Солонар А. В. Окремі аспекти розкриття змісту поняття «повноваження». *Порівняльно-аналітичне право.* 2014. № 2. С. 253–256.

175. Сорока Л.В., Куркова К.М., Даниленко А.О. Використання інструментів цифрового врядування як фактор зниження корупції: адміністративно-правовий аспект. *Науковий вісник публічного та приватного права.* 2025. Вип. 4. С. 256–261

176. Соснін О. В. Проблеми державного управління системою національних інформаційних ресурсів з наукового потенціалу України: монографія. К.: Інститут держави і права ім. В. М. Корецького НАН України, 2003. 572 с.

177. Стеценко С. Г. Адміністративне право України: навч. посіб. Київ: Атіка, 2007. 624 с.

178. Терещук В. В. Правовий статус суб’єктів публічного адміністрування. URL: http://dspace.wunu.edu.ua/bitstream/316497/38567/1/disertacja-tereschuk-v_-v_-na-sajt.pdf

179. Тимошенко В.І. Особиста безпека: сутність та загрози. *Актуальні проблеми освіти і науки в умовах війни:* матеріали першої

науково-практичної онлайн-конференції з міжнародною участю (м. Київ, 6–7 червня 2023 року). ДП «Експрес-об'ява» 2023. С. 64–73.

180. Токар О. Державна інформаційна політика: проблеми визначення концепту. *Політичний менеджмент*. 2009. № 5. С. 131–141.

181. Троцюк Н. В., Петрина Н. О. Адміністративно-правовий захист авторського права та суміжних прав: теоретико-правовий аспект. *Порівняльно-аналітичне право*. 2015. №2. С. 115–118.

182. Тугарова О. К. Інформація як основний об’єкт інформаційних правовідносин. *Юридичний науковий електронний журнал.* 2022. № 8. С. 358–361.

183. Турченко О.Г., Груценко Ю.І. Національна безпека і державна безпека: поліваріантність визначення та співвідношення. *Правничий часопис Донецького національного університету імені Василя Стуса.* 2024. № 1. С. 66–74.

184. Уряд затвердив єдиний порядок взаємодії у сфері кіберзахисту між CERT-UA, CSIRT та силовими структурами. URL: https://cip.gov.ua/ua/news/uryad-zatverdiv-yedinii-poryadok-vzayemodiyi-u-sferi-kiberzakhistu-mizh-cert-ua-csirt-ta-silovimi-strukturami

185. Ухвала Печерського районного суду міста Києва № 84757146 від 26.09.2019. URL: https://youcontrol.com.ua/catalog/court-document/84757146.

186. Фролова О., Теренник В. Співробітництво між Україною та НАТО у сфері інформаційної безпеки. *Геополітичні пріоритети України.* Збірник наукових праць. 2025. Вип. 1 (34). С. 69–79.

187. Халюк С.О. Повноваження Вищої ради правосуддя: теоретико-правова характеристика. *Прикарпатський юридичний вісник.* 2021. Вип. 3(38). С. 19–22.

188. Хартія про особливе партнерство між Україною та Організацією Північно-Атлантичного договору: Міжнародний документ від 09.07.1997. Верховна Рада України. Законодавство України. URL: https://zakon.rada.gov.ua/laws/show/994_002#Text

189. Хахановський В.Г. Інформаційне право: навч.-метод. комплекс. Національна академія внутрішніх справ. Київ, 2013.166 с.

190. Центр глобалістики «Стратегія XXI». Співробітництво Україна – ЄС – НАТО з протидії гібридним загрозам у кіберсфері. Київ: Центр глобалістики «Стратегія XXI», 2019. 64 с.

191. Чи був «злив» і наскільки насправді захищена «Дія». URL: https://dou.ua/lenta/articles/data-leak-and-diia/

192. Шарук О. Г. Механізм адміністративно-правового захисту об'єктів критичної інфраструктури фінансового сектору України: дис. ... канд. юрид. наук : 12.00.07. Київ, 2024. 244 с.

193. Шевчук М.О. Система управління інформаційною безпекою в контексті сучасних викликів. *Науковий вісник Херсонського державного університету*. 2024. № 1. С. 9–13.

194. Шиленко М. В. Поняття адміністративно-правової охорони малого підприємництва. *Форум права.* 2013. № 1. С. 1188–1193.

195. Шишка Р.Б. «Право інтелектуальної власності погляд на проблему». *Право України.* 1999. № 1. С. 38–41.

196. Шпарага Ю.І. Нормативні засади діяльності регіонального Департаменту соціального захисту населення: порівняльно-правовий аналіз. *Прикарпатський юридичний вісник*. 2019. Вип. 3(28). Т. 2. С. 134–138.

197. Юдін О. К, Богуш В. М. Інформаційна безпека держави. Харків: Консум, 2005. 506 с.

198. Які заходи боротьби з корупцією треба запровадити у наступні 5 років? Реанімаційний Пакет Реформ. URL: https://rpr.org.ua/news/yaki-zakhody-borot-by-z-koruptsiieiu-treba-zaprovadyty-u-nastupni-5-rokiv/

199. Яковлєв П.О. Функції державного регулювання у сфері забезпечення інформаційної безпеки. *Часопис Київського університету права*. 2020. №1. С. 155–159.

200. Avtorgov, A.M. Administrative and legal status of the state executive. Nation. Univer. of Intern. Affairs. 2008. 211 p.

201. Batishchev S. Peculiarities of interaction between public administration bodies and other subjects in the field of information protection. *Entrepreneurship, Economy and Law*. 2024. № 6. P. 257–262.

202. CISA. URL: https://www.cisa.gov/

203. Cybersecurity and Infrastructure Security Agency (CISA). Joint Cyber Defense Collaborative: Unifying Cyber Defense Planning and Operations. URL:https://nsarchive.gwu.edu/sites/default/files/documents/qytieo-agiyf/04.pdf

204. Danylenko, A., Sokiran M., Batishchev S., Slabko K. Space Debris: Legal Status and Liability Regime. *Advanced Space Law*. 2022. Vol. 10. P. 4–13.

205. Data Protection Authority & you. DATA PROTECTION GUIDE. URL: https://www.edpb.europa.eu/sme-data-protection-guide/data-protection-authority-and-you_en

206. Data Protection Laws and Regulations USA 2025-2026. ICLG. URL: https://iclg.com/practice-areas/data-protection-laws-and-regulations/usa

207. DHS.gov. URL: https://www.dhs.gov/

208. Directive (EU) 2022/2555 (NIS2) on measures for a high common level of cybersecurity across the Union. URL: https://eur-lex.europa.eu/eli/dir/2022/2555/oj

209. Directive 2002/58/EC of the European Parliament and of the Council of 12 July 2002 concerning the processing of personal data and the protection of privacy in the electronic communications sector (Directive on privacy and electronic communications). URL: https://eur-lex.europa.eu/legal-content/EN/TXT/HTML/?uri=CELEX:32002L0058

210. Directive on security of network and information systems (NIS Directive) EU cybersecurity policy. URL: https://www.europarl.europa.eu/RegData/etudes/BRIE/2020/654198/EPRS_BRI(2020)654198_EN.pdf

211. Directive on security of network and information systems (NIS Directive). URL: https://www.europarl.europa.eu/thinktank/en/document/EPRS_BRI(2020)654198

212. Document 62018CJ0311. EUR-Lex. URL: https://eur-lex.europa.eu/legal-content/ET/ALL/?uri=CELEX:62018CJ0311

213. EDPB. URL: https://www.edpb.europa.eu/edpb_en

214. ENISA. Public-Private Partnerships in Cyber Security: Recommendations and Best Practices. URL: https://www.enisa.europa.eu/topics/state-of-cybersecurity-in-the-eu/national-cybersecurity-strategies/public-private-partnerships-ppps

215. ENISA. URL:https://www.enisa.europa.eu/

216. EU Digital Markets Act та Digital Services Act. Нові можливості та вимоги. URL: https://loyer.com.ua/uk/eu-digital-markets-act-ta-digital-services-act-novi-mozhlyvosti-ta-vymogy/

217. FBI. URL:https://www.fbi.gov/investigate

218. FCA оштрафувало Equifax на £11 млн за виток даних у 2017 під час кібератаки. URL: https://iaa.international/publication/fca-oshtrafuvalo-equifax-na-11-mln-za-vitok-danikh-u-2017-pid-chas-kiberataki

219. Federal Information Security Modernization Act. An official website of the United States government. URL: https://www.cisa.gov/topics/cyber-threats-and-advisories/federal-information-security-modernization-act#:~:text=Other%20provisions%20of%20FISMA%202014%20include:%20*,reporting%20to%20eliminate%20inefficient%20or%20wasteful%20reporting

220. Floridi, L. (2004). Open problems in the philosophy of information. Metaphilosophy, 35 (4), 554–582.

221. Floridi, L. (2010). The philosophy of information: ten years later. Metaphilosophy, 41 (3), 420–442.

222. Floridi, L. (2011). The philosophy of information. Oxford University Press. Oxford, UK. URL: http://ukcatalogue.oup.com/product/ 9780199232383. do?keyword=floridi&sortby=bestMatches

223. FOR SMALL BUSINESS. URL: https://www.edpb.europa.eu/sme-data-protection-guide/data-protection-authority-and-you_en

224. FTC. URL:https://www.ftc.gov/

225. General Data Protection Regulation GDPR. URL: https://gdpr-info.eu/#:~:text=The%20GDPR%20includes%20the%20following%20articles:%20*,official%20PDF%20of%20the%20GDPR%20on%20gdpr%2Dinfo.eu.

226. German, Keith H. Interagency Interaction: Exploring the Facilitators and Inhibitors of Interagency Interaction in the U.S. National Security System. A Dissertation Submitted to the Graduate Faculty of George Mason University in Partial Fulfillment of The Requirements for the Degree of Doctor of Philosophy Public Policy. 2015. URL: https://mars.gmu.edu/server/api/core/bitstreams/ed4c8215-78f1-47a7-bd2f-94c431606d37/content

227. Komarova, Yu. M. (2018) Administrative and legal status of the National Anti-Corruption Bureau of Ukraine. Kyiv. URL: https://elar.navs.edu.ua/server/api/core/bitstreams/f15d9ae8-a90a-4578-af39-75a6c3d21d1f/content

228. Makarchuk, Vitaliy (2015) The concept of «legal status of a person» in theoretical and legal literature. Pravo.ua. No 3: 18–22. Available online: http://193.138.93.8/bitstream/ BNAU/1740/3/Poniattia_pravov.pdf

229. National Cybersecurity Strategy of the United States. Washington: White House, 2023. URL: https://www.whitehouse.gov/wp-content/uploads/2023/03/National-Cybersecurity-Strategy-2023. pdf

230. NATO Cyber Defence Strategy. Brussels: NATO, 2021. URL: https://www.nato.int/cps/en/ natohq/topics_78170.htm

231. NATO. NATO Industry Cyber Partnership Launched at the NATO Cyber Defence Conference. URL: https://www.nato.int/cps/en/natohq/news_113121.htm

232. NIST. URL:https://www.nist.gov/

233. North Atlantic Treaty Organization (NATO). NATO’s approach to countering hybrid threats URL: https://www.nato.int/cps/ru/natohq/topics_156338. htm?selectedLocale=en

234. Overview of the Privacy Act: 2020 Edition. An official website of the United States government. URL:https://www.justice.gov/opcl/overview-privacy-act-1974-2020-edition/introduction#LegHistory

235. Privacy & Cybersecurity Law Blog. URL: https://www.hunton.com/privacy-and-cybersecurity-law-blog/congress-extends-cybersecurity-information-sharing-act-of-2015

236. Privacy Act of 1974. An official website of the United States government. URL: https://www.justice.gov/opcl/privacy-act-1974#:~:text=The%20Privacy%20Act%20requires%20that%20agencies:%20*,Office%20of%20Privacy%20and%20Civil%20Liberties%20staff

237. S.754 - An act to improve cybersecurity in the United States through enhanced sharing of information about cybersecurity threats, and for other purposes. URL: https://www.congress.gov/bill/114th-congress/senate-bill/754

238. Status noun (2022) Merriam-webster. URL: https://www.merriam-webster.com/ dictionary/status

239. Supreme Court of Arkansas (2004) Ronald A. May, Susan E. May, and Gayle Bradford v. Charlie Daniels, in his official capacity as Secretary of State of the State of Arkansas. 359 Ark. 100, 194 S.W.3d 771. URL: https://casetext.com/case/may-vdaniels-1

240. The Attack on Colonial Pipeline: What We've Learned & What We've Done Over the Past Two Years. URL: https://www.cisa.gov/news-events/news/attack-colonial-pipeline-what-weve-learned-what-weve-done-over-past-two-years

241. The Cambridge Analytica Scandal and What It Teaches Us. Graduation. URL: https://greatermanchester.ac.uk/blogs/the-cambridge-analytica-scandal-and-what-it-teaches-us#:~:text=The%20Cambridge%20Analytica%20scandal%20involved%20the%20improper,liked%20*%20Information%20from%20their%20friends'%20profiles

242. The CNIL's restricted committee imposes a financial penalty of 50 Million euros against GOOGLE LLC.

URL: https://www.edpb.europa.eu/news/national-news/2019/cnils-restricted-committee-imposes-financial-penalty-50-million-euros_en

243. The European Data Protection Board. URL: https://www.edpb.europa.eu/about-edpb/who-we-are/european-data-protection-board_en

244. TITLE 5—GOVERNMENT ORGANIZATION AND EMPLOYEES. URL: https://www.govinfo.gov/content/pkg/USCODE-2018-title5/pdf/USCODE-2018-title5-partI-chap5-subchapII-sec552a.pdf

245. Vytruk, N.V. (1993) The status of a person in the political system of society. Politologiya. 1993. №. 3. P. 45–52.

246. What is the ePrivacy Directive? URL: https://www.cloudflare.com/learning/privacy/what-is-eprivacy-directive/

ДОДАТКИ

Додаток А

СПИСОК ПУБЛІКАЦІЙ ЗДОБУВАЧА ЗА ТЕМОЮ ДИСЕРТАЦІЇ

в яких опубліковані основні наукові результати дисертації:

1. Danylenko, A., Sokiran M., ***Batishchev S.***, Slabko K. Space Debris: Legal Status and Liability Regime. *Advanced Space Law*. 2022. Vol. 10. P. 4–13. DOI: https://doi.org/10.29202/asl/10/1

2. Батіщев С.О. Інформація як об’єкт правового захисту. *Право і суспільство*. 2023. № 3. С. 638–642. DOI: https://doi.org/10.32842/2078-3736/2023.3.96

3. Batishchev S. Peculiarities of interaction between public administration bodies and other subjects in the field of information protection. *Entrepreneurship, Economy and Law*. 2024. № 6. P. 257–262. DOI: https://doi.org/10.32849/2663-5313/2024.6.43

4. Батіщев С.О. Адміністративно-правовий захист інформації: теоретико-правовий аналіз. *Вісник Одеського національного університету. Правознавство*. 2025. Т. 27. №. 2(41). С. 12–16. DOI: https://doi.org/10.32782/2304-1587/2025-27-2(41)-2

які засвідчують апробацію матеріалів дисертації:

5. Батіщев С. О. Інформація та публічна адміністрація: точки перетину. *Інноваційні підходи до реформування сучасного законодавства*: матеріали міжнародної науково-практичної конференції (Київ, 20–21 квіт. 2023 р.). Київ: Науково-дослідний інститут публічного права, 2023. С. 44–46.

6. Батіщев С. О. Захист інформації через призму адміністративного законодавства України. *Актуальні проблеми імплементації наукових досягнень у практичну діяльність*: матеріали міжнародної науково-практичної конференції (Київ, 4–5 черв. 2024 р.). Київ: Науково-дослідний інститут публічного права, 2024. С. 98–100.

7. Батіщев С. О. Категорійно-понятєва визначеність правового концепту «адміністративно-правовий статус органів публічної адміністрації» на прикладі сфери захисту інформації. *Актуальні питання розвитку правової системи в сучасній Україні*: матеріали міжнародної науково-практичної конференції (Львів–Торунь, 4 лют. 2025 р.). Науково-дослідний інститут публічного права. Львів–Торунь: Liha-Pres, 2025. С. 26–28.

Додаток Б

ЗАТВЕРДЖУЮ
В.о. Президента Науково-дослідного
інституту публічного права,
доктор юридичних наук, професор
Сергій КОРОЄД
«28» січня 2026 р.

А К Т
впровадження результатів дисертаційного дослідження Батіщева Сергія Олександровича на тему «Адміністративно-правові засади діяльності органів публічної адміністрації у сфері захисту інформації», поданого на здобуття ступеня доктора філософії зі спеціальності 081«Право» у науково-дослідну діяльність Науково-дослідного інституту публічного права

Комісія в складі: головного наукового співробітника, доктора юридичних наук, професора Курило Інни Володимирівни, провідного наукового співробітника, доктора юридичних наук, професора Луценко-Миськів Лесі Ігорівни, провідного наукового співробітника, доктора юридичних наук, старшого дослідника Шкарупи Костянтина Вікторовича, склала цей акт про те, що матеріали дисертаційного дослідження Батіщева Сергія Олександровича на тему «Адміністративно-правові засади діяльності органів публічної адміністрації у сфері захисту інформації», мають необхідний теоретичний, методологічний рівень і практичну значимість та використовуються у науково-дослідній діяльності наукових відділів Науково-дослідного інституту публічного права під час проведення загальнотеоретичних і галузевих досліджень, спрямованих на вирішення теоретико-методологічних проблем адміністративно-правових засад діяльності органів публічної адміністрації у сфері захисту інформації та використовуються Інститутом в межах реалізації науково-дослідної теми «Правове забезпечення прав, свобод та законних інтересів суб'єктів публічно-правових відносин» (номер державної реєстрації № 0120U105390).

Використання результатів дисертації сприятиме активізації та підвищенню ефективності наукової роботи працівників відділів та аспірантів Науково-дослідного інституту публічного права.

ВИСНОВОК

Результати дисертаційного дослідження Батіщева Сергія Олександровича на тему «Адміністративно-правові засади діяльності органів публічної адміністрації у сфері захисту інформації» вважати впровадженими у науково-дослідну діяльність Науково-дослідного інституту публічного права, під час проведення загальнотеоретичних і галузевих досліджень, спрямованих на вирішення теоретико-методологічних проблем адміністративно-правових засад діяльності органів публічної адміністрації у сфері захисту інформації.

Голова комісії: **Інна КУРИЛО**

Члени комісії: **Леся ЛУЦЕНКО-МИСЬКІВ**

Костянтин ШКАРУПА

Додаток В

ЗАТВЕРДЖУЮ
В.о. Президента Науково-дослідного інституту публічного права, доктор юридичних наук, професор
Сергій КОРОЄД
«28» січня 2026 р.

АКТ
упровадження результатів дисертаційного дослідження Батіщева Сергія Олександровича на тему «Адміністративно-правові засади діяльності органів публічної адміністрації у сфері захисту інформації», поданого на здобуття ступеня доктора філософії зі спеціальності 081«Право» в освітній процес Науково-дослідного інституту публічного права

Комісія в складі: головного наукового співробітника, доктора юридичних наук, професора Курило Інни Володимирівни, провідного наукового співробітника, доктора юридичних наук, професора Луценко-Миськів Лесі Ігорівни, провідного наукового співробітника, доктора юридичних наук, старшого дослідника Шкарупи Костянтина Вікторовича, склала цей акт про те, що матеріали дисертації Батіщева Сергія Олександровича на тему «Адміністративно-правові засади діяльності органів публічної адміністрації у сфері захисту інформації» (на здобуття ступеня доктора філософії зі спеціальності 081«Право») мають необхідний теоретичний, методологічний рівень і практичну значимість та використовуються в освітньому процесі. Під час обговорення наданих матеріалів комісією було констатовано, що окремі положення дослідження було використано при розробленні лекційних курсів з дисципліни, яка викладається у Науково-дослідному інституті публічного права, а саме «Адміністративне право та процес: доктринальні та практичні проблеми», при підготовці відповідних підручників, навчальних посібників, а також у контексті інших дисциплін, які викладаються в Інституті. Лекційний курс окремих тем навчальних дисциплін увібрав положення цього дисертаційного дослідження.

ВИСНОВОК:
результати дисертаційного дослідження на тему: «Адміністративно-правові засади діяльності органів публічної адміністрації у сфері захисту інформації» Батіщева Сергія Олександровича вважати впровадженими в освітній процес Науково-дослідного інституту публічного права з дисципліни «Адміністративне право та процес: доктринальні та практичні проблеми».

Голова комісії: **Інна КУРИЛО**

Члени комісії: **Леся ЛУЦЕНКО-МИСЬКІВ**

Костянтин ШКАРУПА